ONLINE PRIVACY IN E-COMMERCE: PRIVACY PARADOX, SOURCES OF PRIVACY CONCERNS, AND ATTITUDINAL AMBIVALENCE

by

Jongtae Yu

A dissertation submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Business Administration

David Eccles School of Business

The University of Utah

May 2018

The University of Utah Graduate School

STATEMENT OF DISSERTATION APPROVAL

The dissertation of **Jongtae Yu**

has been approved by the following supervisory committee members:

Paul J. Hu	, Chair	**10/26/2017** Date Approved
Don Wardell	, Member	**10/26/2017** Date Approved
Shyam Gopinath	, Member	**10/26/2017** Date Approved
Vandana Ramachandran	, Member	**10/26/2017** Date Approved
Xiao Liu	, Member	**10/26/2017** Date Approved

and by **Taylor Randall** ,

Dean of **David Eccles School of Business**

and by David B. Kieda, Dean of The Graduate School.

ABSTRACT

This dissertation highlights two important issues with regard to online privacy concerns in e-commerce: (1) why can't privacy concerns explain online behavior? and (2) what are the essential sources of privacy concerns in e-commerce? In Chapter 2, we explain the discrepancy between people's privacy concerns and their willingness to provide personal information to an online vender, which is called the online privacy paradox. Drawing on construal level theory (CLT), we suggest that people form privacy concerns in a general situation by construing benefits of information disclosure and privacy risk. Due to high psychological distance, the evaluations of benefits and privacy risk become abstract and superficial (i.e., high-level construal). However, as people traverse to a particular situation, the evaluations of those factors become more specific, due to decreased psychological distance (i.e., low-level construal). When high- and low-level construals are consistent, privacy concerns significantly affect information disclosure in a particular situation. In contrast, when the construals are inconsistent, privacy concerns can't explain information disclosure in a particular situation (i.e., privacy paradox).

In Chapter 3, we attempt to identify essential antecedents of privacy concerns in e-commerce. Drawing on protection motivation theory, we select privacy risk, self-efficacy, and response efficacy as generic determinants of privacy concerns. We also identify notice and consent of information practice as privacy concerns' determinants specific to e-commerce. According to our results, while privacy risk and consent had direct effects on

privacy concerns, self-efficacy and notice indirectly impact privacy concerns through privacy risk.

In Chapter 4, we seek to explain the inconsistent direct and indirect effect of privacy concerns by examining attitudinal ambivalence. We develop two alternative models: direct ambivalence and indirect ambivalence model. The direct ambivalence model conceptualizes privacy concerns as attitude and assumes the direct effect of privacy concerns. The effect of privacy concerns is moderated by the ambivalence of privacy self-efficacy and privacy risk. On the other hand, indirect ambivalence model conceptualizes privacy concerns as individual characteristics and assumes indirect effect of privacy concerns via favorability of information disclosure. The relation between favorability and information disclosure is moderated by the ambivalence of benefits and privacy risk.

TABLE OF CONTENTS

LIST OF FIGURES

Figures

LIST OF TABLES

Tables

ACKNOWLEDGEMENTS

First and foremost, praise and thanks to the God, the Almighty, for His blessings and help throughout my Ph.D. study.

I would like to express my deep and sincere gratitude to my advisor Prof. Paul Hu for his continuous support and encouragement for my Ph.D. study and related research. His passion and creativity for research always inspire me. His advice on both research as well as on my career have been priceless. I could not have imagined having a better advisor for my Ph.D. study. Besides my advisor, I would like to thank my committee members: Prof. Don Wardell, Prof. Vandana Ramachandran, Prof. Shyam Gopinath, and Prof. Xiao Liu for their insightful comments for my dissertation.

A special thanks to my family. Words cannot express how grateful I am to my mother, my mother-in law, and father-in-law for all their sacrifices. Their prayer sustained me thus far. I owe a tremendous debt of gratitude to my beloved wife Hyunhee for her love, understanding, prayers, and continuing support for my study. Also, I express my love to my children, Kaylee and Phillip. They are the source of pleasure in my life.

I also would like to express the deepest appreciation to Prof. Dong-Yop Oh, Prof. Jong-Wook Ha, and Prof. Ki Soo Kim for their encouragement in time of need.

Finally, my thanks go to all the people who have supported me to complete my Ph.D. study directly or indirectly.

CHAPTER 1

INTRODUCTION

In the competitive online marketspace, online vendors attempt to maintain and develop their competitive advantages by offering personalized products or services to their customers (Rust & Huang, 2014; Zhou, 2013). Such practices, however, require the collection of a vast amount of personal information. With the collection of vast amounts of personal data, commonly observed online vendors' inappropriate management and use of the collected personal information inevitably create concerns about potential invasion to and loss of their information privacy (Hong &Thong, 2013; Malhotra et al., 2004; Smith et al., 2011; Xu et al., 2011). For example, according to identifyforce.com, data breaches increased by 40% in 2016, and got even more serious in 2017. The concerns about privacy loss are found to significantly affect people's online activities such as information sharing on social network sites or online shopping (Smith et al., 2011). In this light, the effect of privacy concerns on behavior such as online purchase or information disclosure has been of primary interest to information systems (IS) researchers (Awad & Krishnan, 2006; Brown & Muchira, 2004; Dinev & Hart, 2006; Li et al., 2011; Smit et al., 2014; Xu et al. 2009).

While previous studies have empirically examined direct or indirect effect of privacy concerns on behavior in different contexts, some important issues associated with privacy concerns seem to remain less explored. Especially, the reported inconsistent effect

of privacy concerns and lack of legitimacy in selecting antecedents of privacy concerns call for further investigation. In specific, accumulated results of previous studies suggest that the effect of privacy concerns is inconclusive (Bélanger & Crossler, 2011; Smith et al., 2011). For example, while Dinev and Hart (2006) found a significant, negative effect of privacy concerns on people's voluntary information disclosure to an online vendor, Hui et al. (2007) observed an insignificant relationship between privacy concerns and information disclosure in a similar online setting. The discrepancy between privacy concerns and behavior, which is coined as privacy paradox (Barnes, 2006), casts doubt on whether privacy concerns can effectively explain behavior, especially information disclosure. Although several plausible explanations have been proposed such as situational cues or biased evaluations of benefits or risk associated with information disclosure, some empirical findings are incongruent with the proposed explanations. For example, different from the biased evaluation approach, people disclose their personal information even for no rewards (Norberg et al., 2007). Further, the lack of attention to factors that moderate the relation between privacy concerns and behavior may offer a limited account of the condition in which privacy concerns can't explain online behavior in a reliable manner, which is believed essential for reconciling the mixed results of privacy concerns. In this light, there is a growing call for a better explanation of privacy paradox.

In addition, the essential sources of privacy concerns and the process underlying their formation seem to deserve more attention (Smith et al., 2011; Xu et al., 2008). Previous studies often selected key determinants of privacy concerns without a proper theory, such that the legitimacy and validity of chosen factors are questioned because justification of the selection is challenging. Further, the underlying mechanism of forming privacy concerns seems to remain unexplored. Especially, by exclusively focusing on either generic

or context-specific determinants and ignoring their indirect effects, previous studies offer an incomplete explanation of how privacy concerns are formed. The examination of the key sources of privacy concerns and the underlying mechanism of forming privacy concerns is important in that it helps online vendors to devise and implement effective measures to mitigate consumers' privacy concerns and thereby foster their transactions or services utilization online.

In this light, this dissertation aims at examining important but less explored issues regarding privacy concerns: privacy paradox, sources of privacy concerns, and inconsistent indirect effect of privacy concerns. In Chapter 2, we examine the "privacy paradox" in e-commerce. Although previous research has recognized the adverse effects of privacy concerns on people's willingness to provide personal information online (e.g., Bansal & Gefen, 2010; Benndorf et al., 2015; Dinev & Hart, 2006; Dinev et al., 2008; Zhao & Gupta, 2102), several studies report an intriguing discrepancy between individuals' expressed concerns and their voluntary disclosures (sharing) of personal information in online contexts that include e-commerce (Hui et al., 2007), social networking websites (Taddicken, 2014), and online communications (Baek, 2014). That is, although people are concerned about their privacy, they are willing to provide or share their personal information, even for small or no rewards (Norberg et al., 2007). The online privacy paradox has drawn growing attention from researchers and practitioners because it raises a fundamental question of whether privacy concerns can explain or predict behavior in a reliable or effective manner (Bélanger & Crossler, 2011; Dinev, 2014; Smith et al., 2011). We analyze the focal paradox through the lens of construal level theory (CLT, Trope & Liberman; 2010). According to the theory, the construal of an object is affected by perceived psychological distance toward the object. In

specific, when an object is perceived as psychologically distant, the construal of the object is abstract and context-free, i.e., a high-level construal. On the other hand, the construal becomes more context-specific and less abstract when an object is perceived to be psychologically near, i.e., a low-level construal. Our conceptual framework, premised in construal-level theory (CLT), suggests people's traversing different psychological distances influences their evaluations, predictions, and behaviors of disclosing (sharing) personal information online by adjusting the construal level of key factors of privacy concerns. While the absence of a specific situation increases psychological distance toward an object and motivates people to engage in high-level construals, the construal becomes low-level, context-specific in a specific situation as the psychological distance decreases. Drawing on the theory, we suggest that people form privacy concerns in a general setting by construing essential determinants of privacy concerns (e.g., privacy risk) in an abstract manner; when presented with a particular situation, people construe these determinants in a specific manner as the psychological distance toward these factors decreases. When the construals of key determinants remain consistent between a general context and a specific situation, people's information disclosure behaviors would coincide with their expressed (general) privacy concerns because the consistency tends to bolster confidence in an evaluation of key factors and enhances the effect of existing attitude (i.e., privacy concerns). When these construals are inconsistent between the situations, the expressed general privacy concerns may not explain individual behaviors effectively because, in the presence of inconsistent construals, the confidence in an evaluation gets decreased, which weakens the effect of attitude (Eagly & Chaiken, 1993; Jonas et al., 1997). Further, in the presence of inconsistent evaluations, connecting an object with an evaluation is challenging and the retrieval of attitude is prevented, which lessens the effect of attitude (Fazio et al., 1986).

Drawing on protection motivation theory (PMT) and previous studies (Dinev & Hart, 2006; Sheehan & Hoy, 2000; Xu et al., 2009), we highlight benefits of information disclosure and privacy risk as essential antecedents of privacy concerns. We conducted longitudinal experiments to test hypotheses developed in light of CLT, which consist of two phases. In phase 1, we measured participants' general privacy concerns, perceived benefits of information disclosure, privacy risk and information disclosure behavior. Then they were asked to indicate their willingness to provide personal information after reading a general description of online vendors' information collection practices. Drawing on their indicated values associated with benefits and privacy risk, we assigned participants into one of four groups: high benefits and high privacy risk (H_BH_R), high benefits and low privacy risk (H_BL_R), low benefits and high privacy risk (L_BH_R), and low benefits and low privacy risk (L_BL_R). In phase 2, we manipulated three experimental conditions (i.e., consistency, positive inconsistency, and negative inconsistency) associated with benefits and privacy risk by presenting different scenarios and examine the relationship between general privacy concerns and information disclosure in a particular situation for each condition. In specific, the consistency condition was manipulated by presenting a scenario that was congruent with their classified group determined by their indicated values in phase 1. For example, when a participant was classified as H_BH_R group based on their responses in phase 1, we assigned her into consistency condition by providing H_BH_R scenario. We manipulated a positive inconsistency condition by presenting H_BL_R scenario to participants who were classified as H_BH_R, L_BH_R, and L_BL_R based on their responses in phase 1 because the scenario provides higher benefits, lower privacy risk, or both than other scenarios. We manipulated a negative condition by providing L_BH_R scenario to participants who were classified as H_BH_R, H_BL_R, and L_BL_R based on their

indicated values in phase 1 because the scenario shows lower benefits, higher privacy risk, or both, compared to other scenarios. We collected data from students in a major university in the U.S. The analysis results demonstrate significant effect of general privacy concerns on information disclosure in a specific situation under a consistency condition. In contrast, in a positive and a negative inconsistency condition, privacy concerns had negligible effect on information disclosure in a particular situation. That is, in the inconsistency condition, privacy concerns can't explain information disclosure in an effective and reliable manner. We further extend our study for validating the results by using a different set of determinants suggested by PMT: self-efficacy and response efficacy. The analysis results fully supported the hypotheses as well. While the effect of privacy concerns remained significant under a consistency condition, the effect of privacy concerns was negligible in a positive and a negative inconsistency condition. We also collected data from MTurk workers to assure external validity of our findings. The results supported all proposed hypotheses. Overall, both students and MTurk workers' data support that privacy concerns have negligible effect on information disclosure in a particular situation when construals of privacy concerns' determinants are inconsistent between a general situation and a particular situation.

In Chapter 3, we identify key determinants of privacy concerns and examine their direct and indirect effects. While the effects of privacy concerns have been primarily examined, essential sources of online privacy concerns and the process underlying their formation have received relatively little attention (Smith et al., 2011; Xu et al., 2008). In this study, we seek to offer a theory-based explanation of how individuals form privacy concerns in e-commerce by identifying essential generic and e-commerce specific determinants of privacy concerns and examining their direct and indirect effects. We first

choose generic factors that shape privacy concerns based on protection motivation theory (PMT), which suggests people's protection behaviors to be motivated by their cognitive appraisals of several essential components of a fear appeal: cognitive appraisal of vulnerability, severity, self-efficacy, and response efficacy (Maddux & Rogers, 1983; Rogers, 1983). In the perspective of PMT, privacy concerns can be viewed as a mediating variable that explains the relationship between the cognitive appraisals and privacy protecting behaviors (Li et al., 2012; Youn, 2009). That is, customers form privacy concerns by cognitively appraising vulnerability, severity, self-efficacy, and response-efficacy and in turn decide their privacy protecting behaviors. We further consider perceived fairness in information collection process as an essential e-commerce specific determinant of privacy concerns. In information exchange, customers consider their personal information as an input of the exchange (Ashworth & Free, 2006). Fairness of the information collection process is a central element of fair information exchange and is often used for gauging opportunistic behavior of an online vendor (Culnan & Armstrong, 1999). Fairness in the information collection process leads customers to perceive an online vendor as ethical, which alleviates the fear of an online vendor's opportunistic behavior and diminishes customers' privacy concerns, thereby motivating information disclosure; in contrast, violations of fairness in information collection process escalate people's privacy concerns and discourage them from providing personal information to an online vendor (Ashworth & Free, 2006; Culnan & Bies, 2003). In specific, we focus on notice and consent, which are two core components of fairness in information collection process (Culnan & Armstrong, 1999). Drawing on protection motivation theory (PMT) and procedural fairness, we identify key determinants of privacy concerns: privacy risk (vulnerability and

severity), self-efficacy, response-efficacy, notice, and consent. In addition, we attempt to provide a fuller explanation of the forming process of privacy concerns by examining both direct and indirect effects of key privacy concerns' determinants. Although PMT helps identify essential sources of privacy concerns, there have been voices to highlight their indirect effects due to the associations among the distinctive cognitive appraisals (Maddux & Rogers, 1983; Neuwirth et al., 2000). Through the lens of self-efficacy theory (Bandura, 1989) and agency theory, we suggest indirect effects of coping and fairness appraisal on privacy concerns through threat appraisal. We also test the proposed model empirically using cross-cultural data. In line with Griffith et al. (2000) and Kim (2008), we identify two types of cultures by combining the national cultural dimensions from Hofstede's study (1994): individualistic-weak uncertainty avoidance-small power distance culture (type I) versus collectivistic-strong uncertainty avoidance-large power distance culture (type II). We collected data from two countries: the U.S. and South Korea (hereafter S. K.). While the U.S. can be categorized as type I culture, S.K. is a representative country that belongs to type II culture. We compare the effects of selected antecedents of privacy concerns at both construct and path coefficient levels between the countries. The comparison would shed light on the role of culture in forming privacy concerns in e-commerce. According to analysis results of U.S. data, privacy concerns were directly influenced by privacy risk and consent, whereas self-efficacy and notice indirectly influence privacy concerns via privacy risk. In addition, the comparison between two countries demonstrated the roles of culture in shaping privacy concerns. In specific, at the construct level, the two countries were significantly different in all constructs except notice. The S.K. participants perceived more privacy risk and more assurance that online vendors obtain permission before collecting and

using personal information than did their U.S. counterparts. In contrast, the U.S. participants showed more confidence in their ability to manage privacy risk (i.e., self-efficacy) and availability of effective response toward the risk (i.e., response efficacy). Further, the path coefficients derived from the two datasets significantly differed, with the exception of response efficacy. In specific, while the effects of privacy risk and consent were more prominent with the U.S. participants, the effects of self-efficacy and notice were greater among the Korean participants than with the U.S. participants. There was no significant difference in the effect of response-efficacy between the two countries.

In Chapter 4, we seek to offer an alternative explanation of the inconsistent direct and indirect effect of privacy concerns by highlighting the moderating roles of attitudinal ambivalence. In examining the effect of privacy concerns, some previous studies conceptualize privacy concerns as attitude or belief and examine their direct effect on online behaviors (e.g., Dinev & Hart, 2006; Pavlou et al., 2007; Son & Kim, 2008). However, accumulated results seem to suggest that direct effect of privacy concerns is inconclusive. In contrast, some other previous studies alternatively conceptualize privacy concerns as individual characteristics or value and suggest indirect effect of privacy concerns via attitude or belief such as risk or trust (Hong & Thong, 2013; Lowry et al., 2011; Malhotra et al., 2004). However, the indirect effect of privacy concerns seems mixed as well: fully mediated, partially mediated, or not mediated. While some studies observe that the effect of privacy concerns is fully mediated by an attitude or cognitive belief such as privacy attitude (e.g., Dienlin & Trepte, 2015; Van Slyke et al., 2006), others report partially mediated effect of privacy concerns (e.g., Li et al., 2011; Kehr et al.,2015). Some studies found negligible indirect effect of privacy concerns (Bansal et al., 2016; Lian & Lin, 2008; Xu & Gupta, 2009). Further, previous studies report mixed results

of indirect effect of privacy concerns with the same mediating factors such as risk or trust (e.g., Bansal et al., 2016; Li et al., 2011; Van Slyke et al., 2006), which suggests that the inconsistency may not stem from a different mediating variable or research context. However, the inconsistent indirect effect of privacy concerns seems overlooked and remained unexplained. Thus, we attempt to explain the inconsistent direct and indirect effects of privacy concerns through the window of the attitudinal ambivalence. Attitudinal ambivalence indicates a state in which an individual holds equivalently strong positive or negative evaluation toward a focal object at the same time (Thompson et al., 1995). Attitudinal ambivalence weakens the strength of the relation between attitude and behavior particularly by preventing accessibility to memory, averting attitude certainty, or hampering consistency between cognitive beliefs (Bargh et al., 1992; Maio et al., 1996). Drawing on attitudinal ambivalence, we developed research models to explain both inconsistent direct and indirect effects of privacy concerns: *direct ambivalence* and *indirect ambivalence model*. Drawing on protection motivation theory (PMT) (Rogers, 1983), we first determine important and relevant cognitive beliefs relevant to privacy concerns, a negative attitude associated with threat: privacy self-efficacy and privacy risk. In line with the privacy calculus model (Dinev & Hart, 2006), we select benefits of information disclosure and privacy risk as essential cognitive beliefs that constitute favorability of information disclosure, a positive attitude related to utility of information disclosure. Privacy risk is categorized as a negative cognitive belief because it augments threat but diminishes the utility of information disclosure. In contrast, privacy benefits and privacy self-efficacy are classified as positive cognitive beliefs because privacy self-efficacy decreases threat of information disclosure and benefits increase utility of disclosure behavior. The direct

ambivalence model conceptualizes privacy concerns as attitude and suggests a direct effect of privacy concerns on information disclosure to online vendors. In the model, the effect of privacy concerns on information disclosure is negatively moderated by the ambivalence of privacy risk and privacy self-efficacy. On the other hand, the indirect ambivalence model conceptualizes privacy concerns as individual characteristics or value and posits that indirect effect of privacy concerns via favorability of information disclosure. In the model, the ambivalence of benefits and privacy risk negatively moderates the relation between favorability and information disclosure behavior. Data analysis results supported our proposed hypotheses. While the ambivalence of privacy self-efficacy and privacy risk negatively moderates the effect of privacy concerns (i.e., negative attitude), the ambivalence of benefits and privacy risk moderates the effect of favorability (i.e., positive attitude).

Overall, our studies shed light on important issues of privacy concerns which are important but less explored. Chapter 2 and 4 offer alternative explanations of the inconsistent effects of privacy concerns on information disclosure in e-commerce. Chapter 3 identifies essential antecedents of privacy concerns and examines their direct and indirect effects for offering a better explanation of the formation process of privacy concerns.

CHAPTER 2

"WHY DON'T PEOPLE ACT AS THEY SAY?" AN EXPERIMENTAL STUDY OF ONLINE PRIVACY PARADOX IN E-COMMERCE

2.1 Introduction

A person's privacy concerns reflect his or her inherent worries about possible loss of information privacy (Xu et al., 2011). Although previous research has recognized the adverse effects of privacy concerns on people's willingness to provide personal information online (e.g., Bansal & Gefen, 2010; Benndorf et al., 2015; Dinev & Hart, 2006; Dinev et al., 2008; Zhao & Gupta, 2102), several studies report an intriguing discrepancy between individuals' expressed concerns and their voluntary disclosures (sharing) of personal information in online contexts that include e-commerce (Hui et al., 2007), social networking websites (Taddicken, 2014), and online communications (Baek, 2014). Barnes (2006) studies the uproar over privacy issues in social networks and coins the term "*privacy paradox*" to describe teenagers' tendency of freely giving up their personal information in online journals. Since then, online privacy paradox has drawn a growing attention from researchers and practitioners who question whether individual behaviors might differ from the expressed privacy preferences by asking "why people don't act as they say" (Bélanger & Crossler, 2011; Dinev, 2014; Smith et al., 2011).

As Dinev and Hart (2006) comment, people appear to disclose their personal information "as if they didn't care" (p. 76). This paradox is intriguing and warrants further scrutiny. Prior studies often consider privacy concerns as a proxy of privacy and thus use privacy concerns to indirectly examine the effects of privacy on individual behaviors (Bélanger & Crossler, 2011). The alignment between a person's expressed concerns and his or her disclosure behavior seems questionable, which reveals whether privacy concerns are indeed a valid proxy of privacy for explaining individual disclosure behaviors (Bélanger & Crossler, 2011; Dinev, 2014; Smith et al., 2011). We attempt to explain the online privacy paradox in e-commerce that represents crucial online context. In particular, we scrutinize the condition in which the privacy paradox may occur and thereby shed light on the mixed results concerning the effects of privacy concerns on information disclosures.

We analyze the focal paradox from the lens of construal level theory (CLT, Trope & Liberman, 2010) by exploring differential levels of construal in the relationship between general privacy concerns and disclosure behaviors in a specific situation. Overall, CLT describes how the perceived psychological distance could influence the construal levels of essential factors that jointly determine individual evaluations, predictions, and actions (Trope & Liberman, 2010). As Liberman et al. (2007) describe, psychologically distant objects or behaviors refer to "those that are not present in the direct experience of reality" (p. 353). When an object, factor, or behavior is perceived as psychologically distant, the corresponding construal is abstract and context-free, i.e., a high-level construal. The construal becomes more context-specific and less abstract when an object, factor, or behavior is perceived to be psychologically near, i.e., a low-level construal.

In line with CLT, we posit that people usually form their privacy concerns in a general

sense by construing key factors (such as privacy risk) in a rather abstract manner, due to the large psychological distance toward each factor, i.e., a high-level construal. As people traverse to a specific situation, the perceived psychological distance decreases, which prompts people to construe each factor in a more detailed and concrete manner, i.e., a low-level construal. Thus, the relationship between privacy concerns and disclosure behaviors can be moderated by the consistency (or the lack of thereof) of the high- and low-level construal of the respective factors. When the high- and low-level construals of key determinants are consistent, disclosure behaviors would coincide with the expressed privacy concerns, thus observing no paradox. However, when the different construal levels become inconsistent, the expressed concerns cannot sufficiently explain behaviors. The consistency of construals between a general and a particular situation tends to bolster confidence in an evaluation toward a focal object and enhances the effect of existing attitude (i.e., privacy concerns). In contrast, when construals of determinants are inconsistent between the situations, the confidence in an evaluation gets decreased, which weakens the effect of attitude (Eagly & Chaiken, 1993; Jonas et al., 1997). Further, in the presence of inconsistent evaluations, connecting an object with an evaluation is challenging and the retrieval of attitude is prevented, which lessens the effect of attitude (Fazio et al., 1986), i.e., the online privacy paradox.

Drawing on protection motivation theory (PMT, Maddux & Rogers, 1983) and previous studies, we determine benefits and privacy risk as essential antecedents of privacy concerns. Benefits refer to people's anticipated rewards from an online vendor in return for their information disclosures (Xu et al., 2009); privacy risk denotes people's estimated privacy loss associated with their information disclosures (Xu et al., 2011). The inconsistent construals of benefits and privacy risk between a general and a particular situation lessens the effect of

general privacy concerns on information disclosure in a particular situation. As a result, general privacy concerns can't explain disclosure behavior in a reliable manner.

Our study differs from most previous research in several ways. First, we propose a conceptual framework premised in CLT to analyze online privacy paradox in e-commerce, a crucial online context in which privacy paradox has received relatively limited attention (Bélanger & Crossler, 2011; Smith et al., 2011). Second, unlike many previous studies that examine factors that lead to the discrepancy of the expressed concerns and information disclosures, we seek to explain online privacy paradox by explicating the changes in the corresponding construals of key determinants between a general context and a specific situation. Third, we scrutinize the condition in which the effect of privacy concerns become neglectable and thereby offer a plausible explanation of the inconsistent results of privacy concerns' effects.

2.2 Literature Review

Several research streams are relevant to our study, including the effects of privacy concerns in e-commerce, and approaches to analyze online privacy paradox. Herein, we review representative studies of each stream to highlight the gaps that motivate our investigation.

2.2.1 Effects of Privacy Concerns in E-Commerce

Previous research has examined the effects of privacy concerns in e-commerce, e.g., online purchases (Brown & Muchira, 2004), personalization services, (Chellappa & Sin, 2005), privacy protection (Son & Kim, 2008), personal information disclosures and sharing (Malhotra et al., 2004). The overall results appear mixed. For example, Dinev and Hart

(2006) show that general privacy concerns negatively influence individuals' information disclosures to an online vendor but Hui et al. (2007) observe an insignificant effect of privacy concerns. Similarly, Brown and Muchira (2004) report a negative relationship of general privacy concerns and online purchase but Van Slyke et al. (2006) report an insignificant effect on online transactions. Similar inconsistent results are also noted in social network settings. Utz (2015) and Zlatolas et al. (2014) report a negative effect of privacy concerns on people's sharing personal information on Facebook, but Taddicken (2014) shows an insignificant effect of privacy concerns on voluntary information sharing on social network websites.

While these inconsistent results observed in different online contexts might suggest privacy paradox not a situation- or population-specific phenomenon, they indicate the need to examine the forces underlying the discrepancy between the expressed concerns and information disclosures. In Table 2.1, we summarize several representative previous studies that examine the effects of online privacy concerns.

2.2.2 Approaches and Views to Analyze Online Privacy Paradox

Previous research has investigated online privacy paradox, typically using behavioral intention to approximate disclosure behaviors (Acquisti & Grossklags, 2005; Kehr et al., 2015; Li et al., 2011). Several approaches have been taken, including bounded rationality, situational cues, weak awareness of privacy risk, and a genuine weak relationship. Acquisti and Grossklgas (2005) and Acquisti et al. (2012) follow the bounded rationality approach by considering people's irrational decisions about their information disclosures as an important source of privacy paradox. This approach is in sync with behavioral economics in that it

Table 2.1 Summary of Representative Previous Studies Examining Online Privacy Concerns

Study	Domain	Constructs	Effect of privacy concerns
Angst and Agarwal (2009)	Healthcare	• Independent variable: Privacy concerns • ME/MO variable: None • Dependent variable: Intent to adopt electronic healthcare records (HER)	• Privacy concerns → Intention to adopt (Supported)
Dienlin and Trepte (2015)	Social Network website (Facebook)	• Independent variable: General privacy concerns • ME/MO variable: Privacy attitude (ME) • Dependent variable: Information disclosure	• Privacy concerns → Information disclosure (Not supported) • Privacy concerns → Privacy attitude → Information disclosure (Supported)
Dinev and Hart (2006)	E-commerce	• Independent variable: General privacy concerns • ME/MO variable: None • Dependent variable: Willingness to provide personal information	• Privacy concerns → Information disclosure (Supported)
Hui et al. (2007)	E-commerce	• Independent variable: General privacy concerns • ME/MO variable: None • Dependent variable: Information disclosure	• Privacy concerns → Information disclosure (Not supported)
Kehr et al. (2015)	Mobile app	• Independent variable: General privacy concerns • ME/MO variable: Privacy risk (ME) • Dependent variable: Information disclosure	• Privacy concerns → Information disclosure (Not supported) • Privacy concerns → Privacy risk → Information disclosure (Supported)

Table 2.1 Continued

Study	Domain	Constructs	Effect of privacy concerns
Malhotra et al. (2004)	E-commerce	• Independent variable: General privacy concerns • ME/MO variable: Privacy risk (ME) • Dependent variable: Information disclosure	• Privacy concerns → Privacy risk → Information disclosure (Supported)
Norberg et al. (2007)	Commercial	• Independent variable: General privacy concerns • ME/MO variable: None • Dependent variable: Information disclosure	• Privacy concerns → Information disclosure (Not supported)
Van Slyke et al. (2006)	E-commerce	• Independent variable: General privacy concerns • ME/MO variable: • Risk perception (ME) • Trust (ME) • Dependent variable: Willingness to transact online	• Privacy concerns → WT (Not supported). • Privacy concerns → Risk perception → WT (AD: Supported; HD: Not supported) • Privacy concerns → Trust → WT (AD: Not supported; HD: Not supported)
Zlatolas et al. (2014)	Social network website	• Independent variable: Privacy concerns • ME/MO variable: None • Dependent variable: Information disclosure	• Privacy concerns → Information disclosure (Supported)

ME/MO: Mediating/moderating variable; AD: Amazon.com data; HD: Half.com data; WT: Willingness to transact.

anchors in an individual's tendency to make irrational information disclosure decisions, due to the bounded rationality coupled with incomplete information and a desire for immediate gratification (Acquisti & Grossklags, 2005; Acquisti et al., 2012; Wilson & Valacich, 2012).

Situational cues offer another approach; they distinguish general privacy concerns and situation-specific constructs. Overall, this approach suggests situational cues weaken the effects of privacy concerns and therefore lead to voluntary information disclosure (Hsu 2006; Kehr et al., 2014; Li et al., 2011; Wilson & Valacich, 2012). According to Li et al. (2011), as detailed information concerning disclosure behaviors becomes available in a specific situation, people could rely on key situational cues for evaluating the associated privacy risk, which may not be in sync with their expressed privacy concerns. That is, a person's assessment in a particular situation may be steered by situational cues that mask or even dominate the effect of the expressed concerns (Kehr et al., 2014).

Baek (2014) differentiates opinion- versus behavior-oriented view. The opinion-oriented view focuses on people's tendency to underestimate the associated privacy risk, probably due to their limited digital literacy or inability to understand and use information from various resources (Hargittai, 2009; Park, 2011). Despite the legitimacy of the expressed concerns, people tend to underestimate or even overlook the privacy risk of offering personal information in various online contexts, because they are not particularly knowledgeable of how online vendors gather, utilize, and manage the provided personal information. For example, low digital literacy restricts people's appreciation of probable privacy infringements and serious outcomes that could stem from their voluntary disclosures (sharing) of personal information with an online vendor (Baek, 2014; Park, 2011). The behavior-oriented view instead attributes the negligible or insignificant effects

of privacy concerns on disclosure behaviors to a genuine weak relationship between privacy concerns and disclosure behaviors. As Baek (2014) notes, individuals' opinions about online privacy concerns are superficial and dubious, and therefore cannot predict their actual disclosure behaviors in an effective, reliable manner. Dienlin and Trepte (2015) observe a weak relationship between privacy concerns and information disclosures, arguing the mediation of privacy attitudes on the effect of privacy concerns on information disclosures on social network websites. We summarize the different views on privacy paradox in Table 2.2.

A review of extant literature reveals several gaps. First, the prevalent approaches and views predominantly focus on either general factors or situation-specific constructs that influence the relationship of privacy concerns and disclosure behaviors. For example, both the bounded rationality approach and the opinion-oriented view stress general factors, such as the expected benefits, awareness of privacy risk, or their combinations. These approaches and views seem to overlook effects of situation-specific factors and thus provide a partial account of privacy paradox because people may also rely on situation-specific information for making privacy related decisions (Li et al., 2011). In contrast, the situational cue approach overlooks the roles of general attitudinal beliefs and only garners partial empirical support (e.g., Kehr et al., 2015; Li et al., 2011). Furthermore, this approach doesn't offer a proper explanation of how situation-specific factors override the effects of general belief or attitude which is reported to have a greater effect on behavior than situational factors do (e.g., Sitkin & Pablo, 1992; Terry, 1994). By considering both general and situation-specific factors and exploring how they interact and jointly affect information disclosure behavior, we could better explain the discrepancy between the expressed concerns and information disclosures. Second, while many previous studies focus on examining key factors that could lead to online privacy paradox, the

Table 2.2 Summary of Different Approaches on Privacy Paradox

Approach	Studies	Explanation of privacy paradox
Behavioral economics	Acquisti and Grossklags (2005) Acquisti (2009) Acquisti et al. (2012)	Bounded rationality Incomplete information Desire for immediate gratification
Situational Cues	Kehr et al. (2014) Kehr et al. (2015) Li et al. (2011) Wilson and Valacich (2012)	The effects of situational cues override the effect of privacy concerns on information disclosure
Opinion-oriented	Park (2011)	The underestimation of privacy risk associated with information disclosure due to digital illiteracy
Behavioral-oriented	Baek (2014) Dienlin and Trepte (2015)	A genuine weak relationship between privacy concerns and information disclosure due to superficial and dubious opinions about online privacy concerns.

condition in which privacy paradox occurs remains unclear. While the proposed explanations help figure out the neglectable effect of privacy concerns, they seem to shed little light on why previous studies observe different effects of privacy concerns in a similar context. For instance, while Dinev and Hart (2006) report a significant effect of privacy concerns on information disclosure in e-commerce, Hui et al. (2007) observe insignificant effect of privacy concerns in the same context. Explications of the condition leading to privacy paradox are crucial and can shed light on the mixed results of previous privacy research. Third, this paradoxical phenomenon is often studied in the context of individual communications on social network websites; relatively few efforts have been expended in e-commerce contexts. Compared with the personal communications that proceed on social network websites, online vendors might pose greater threats to individual privacy because of their ability to exploit the collected

customer data opportunistically. The online privacy paradox in e-commerce could differ from that in social network websites in terms of key factors and motivations. For example, institutional privacy concerns appear salient in e-commerce while social privacy concerns prevail on social network websites (Young & Quan-Haase, 2013).[1] In addition, information disclosures on a social network website are usually motivated by social rewards such as relationship development (Posey, et al., 2010), whereas the disclosure (sharing) of personal information to an online vendor is typically driven by economic benefits (Acquisti & Grossklags, 2005; Ashworth & Free, 2006).

2.3 Theoretical Foundation

We use construal-level theory (CLT) to conceptualize a framework that explains online privacy paradox. This theory is appropriate to our study in that it considers general and situational-specific construals in explaining behavior. According to CLT, the construal level of an object or behavior is determined by the perceived psychological distance formed by a person's perception of the temporal, spatial, social, or certainty space associated with the object (Trope & Liberman, 2010; Trope et al., 2007).

When an object is perceived as psychologically distant, people derive a mental construal of the object that is general, high-level, and abstract. A high-level construal leads to abstract interpretations of a psychologically distant object by focusing on its invariant, schematic features but transcending situational details, which leads to an oversimplified representation of the object (Trope & Liberman, 2010). Especially, a high-level construal is

[1] Institutional privacy concerns refer to individual concerns about a vendor's using the provided personal information for unwanted purposes, whereas social privacy concerns denote the fear of privacy intrusion by other people such as stalking (Young & Quan-Haase, 2013).

salient for understanding an object in a general situation when available information is limited and relevancy is low, i.e., large psychological distance (Trope & Liberman, 2010). In contrast, an object perceived as psychologically near facilitates a construal that is specific, concrete, and low-level. A low-level construal leads to the creation of a concrete interpretation by highlighting situation-specific features of a focal object or behavior, which are variant in nature (Liberman et al., 2007). Unlike their high-level counterparts, low-level construals entail situational details for developing context-specific interpretations. Low-level construals are prominent and determinant of an object or behavior in a particular situation in which detailed situation-specific information is available and relevancy is high, i.e., low psychological distance (Trope & Liberman, 2010).

CLT helps specify the condition in which the privacy paradox occurs by highlighting the relationship between a general and a situation-specific factor. According to the theory, a factor can be differently construed between a general and a particular situation due to the difference of perceived psychological distance between settings. In a general context with limited information available and low relevancy, a person forms his or her privacy concerns by construing relevant factors in an abstract way (i.e., high-level construal), due to the relatively large psychological distance perceived toward key factors.[2] However, the psychological distance toward the determinants decreases as people traverse from a general context to a specific situation, which prompts low-level construal for assessing the key factors. In a particular situation with situation-specific information available and high relevancy, a person

[2] We focus on the construals of privacy concerns' determinants. According to motivation protection theory (Rogers, 1975; Maddux & Rogers, 1983), anxiety or concerns are shaped as a result of construing the determinants rather than the concerns themselves are being construed.

tends to construe key determinants of privacy concerns in a detailed and specific way.[3] In this vein, the relationship between people's general privacy concerns and their information disclosures in a specific situation can be affected by whether the high- and low-level construals of key determinants remain consistent. A consistency of high- and low-level construals bolsters confidence in an evaluation toward information disclosure and thus underpins the existing attitude (Chaiken et al., 1995). Further, a consistency helps connect an evaluation with privacy concerns and facilitates convenient access to these concerns, which enforces the effect of the expressed concerns (attitudinal beliefs) (Fazio et al., 1986). In contrast, an inconsistency weakens the explanatory or predictive power of the expressed concerns for disclosure behaviors in that it decreases the confidence in an evaluation toward privacy concerns' determinants and restricts the access to the attitudinal beliefs (Bargh et al., 1992; Fazio et al., 1986; Jonas et al., 1997). The moderating effect of the consistency between high- and low-level construals helps reconcile the reported mixed results of privacy concerns' effect on information disclosure by specifying the condition in which privacy paradox occurs. The equivalently strong different evaluations toward a same object significantly diminish the effect of attitude which is formed by the evaluations (Armitage and Conner, 2000).

2.4 Conceptual Framework and Hypotheses

2.4.1 Conceptual Model

Using CLT as the theoretical premise, we conceptualize a framework to describe how the inconsistency of high- and low-level construals of privacy concern determinants

[3] We do not consider the relationship between high- and low-level construals between a general setting and a particular situation because people engage in low-level construals with situation-specific information which is not available in a general situation.

influence the relationship between general privacy concerns and information disclosure in a specific situation. According to the conceptual framework, general privacy concerns have a significant effect on people's willingness to disclose personal information in a general situation. The effect of general privacy concerns on information disclosure to online venders in a specific situation is affected by the degree to which the high- and low-level construals of the determinants are consistent. When they are consistent, general privacy concerns can effectively explain or predict information disclosure in a particular situation; the inconsistency between the construals leads to the discrepancy between the expressed privacy concerns and information disclosure. In the model, we further categorize the inconsistency as a positive versus a negative: while the former indicates that the low-level construals in a particular situation lead to the perceptions of higher benefits, lower privacy risk, or the combination, the latter denotes that the low-level construals suggest lower benefits, higher privacy risk, or both. In either a positive or negative inconsistency, the effect of privacy concerns would be neglectable which leads to privacy paradox. Overall, the effect of general privacy concerns on information disclosure in a particular situation is moderated by the level of inconsistency of construals pertain to benefits and privacy risk between a general and a particular situation. Drawing on PMT and previous studies, we identify essential antecedents of privacy concerns. PMT suggests benefits, risk (vulnerability and severity), self-efficacy, response efficacy, and cost of adopting a response as fundamental components of a fear appeal which jointly shape his or her anxiety or concerns (Floyd, 2000; Maddux & Rogers, 1983). Previous studies also highlighted benefits and privacy risk as essential cognitive beliefs that compose privacy concerns (Sheehan & Hoy, 2000; Dinev & Hart, 2006; Xu et al., 2009). In this light, we consider

benefits and privacy risk as essential and relevant antecedents of privacy concerns. We illustrate our conceptual frame in Figure 2.1.

2.4.2. Hypotheses

In a general situation, general privacy concerns have an adverse effect on information disclosure (Dinev & Hart, 2006; Xu et al., 2009). Concerns about negative consequences of information sharing such as privacy loss restrict people's information disclosure (Dinev & Hart, 2006; Xu et al., 2009). Consistent with previous studies, we posit that general privacy concerns are negatively associated with intention to information disclosure in a general setting.

- HYPOTHESIS 1 (H1). General privacy concerns have negative effect on information disclosures to online vendors in a general situation in (H1a) consistency, (H1b) a positive inconsistency, and (H1c) a negative inconsistency condition.

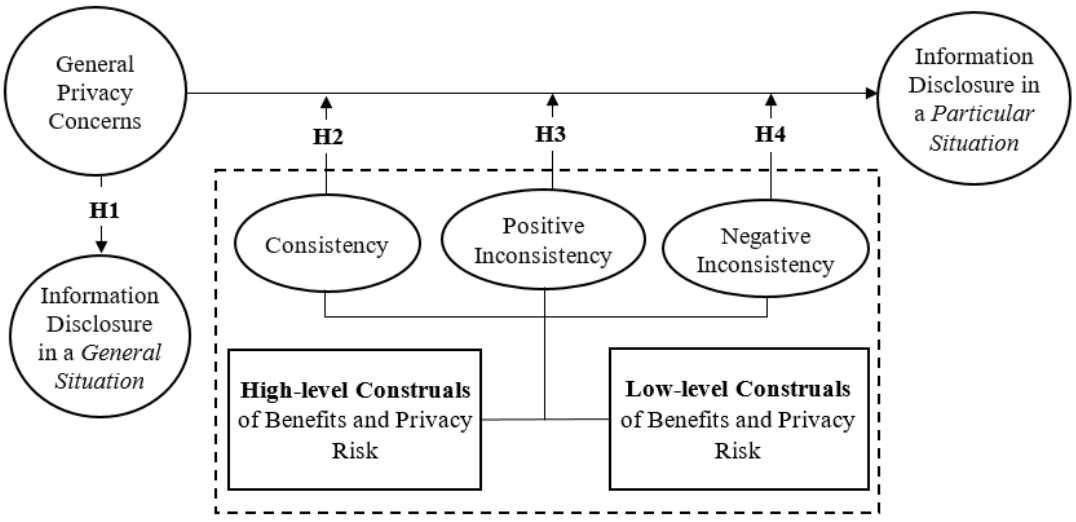


Figure 2.1 Conceptual Model

People, in a general sense, tend to shape general privacy concerns by construing factors associated with benefits and privacy risk in a rather abstract, superficial manner, due to the great psychological distance toward information disclosure. The traverse to a specific situation decreases psychological distance toward the key determinants of general privacy concerns and prompts low-level construals, which may be consistent or inconsistent with high-level construals of the determinants. We posit that the effect of general privacy concerns on information disclosure to online vendors in a specific situation remains significant when high- and low-level construals of privacy concern determinants are consistent. On the other hand, the effect of general privacy concerns remains significant when the construals of the key determinants are consistent. A consistency between construals of privacy concerns' determinants (i.e., benefits and privacy risk) reinforces the effect of general privacy concerns by increasing confidence in an evaluation of the determinants and helping to readily associate the evaluation with privacy concerns (Chaiken et al., 1995; Fazio et al., 1986; Jonas et al., 1997). Therefore, we hypothesize that general privacy concerns have adverse effect on information disclosure in a particular situation in the presence of consistency between the high- and low-level construals of privacy concerns determinants associated with threat appraisal (benefits and privacy risk) and coping appraisal (privacy self-efficacy and response efficacy) (i.e., no privacy paradox).

- HYPOTHESIS 2 (H2). General privacy concerns have negative effect on information disclosure to online vendors in a specific situation when high- and low-level construals of benefits and privacy risk are consistent.

The inconsistency between high- and low-level construals of privacy concerns' determinants leads to privacy paradox by weakening the effect of general privacy concerns

on information disclosure in a specific situation. We further categorize the inconsistency as positive versus negative, and examine their respective effects. In the presence of a positive inconsistency, the low-level construals of privacy concern determinants lead people to sense more positive about information disclosures in a specific situation than they would in a general sense: more benefits, lower privacy risk, or both. On the other hand, with a negative inconsistency, the low-level construals make people to feel less positive about disclosures in a specific situation than a general context: lower benefits, higher privacy risk, or their combination. The inconsistencies between construals of privacy concerns determinants between a general context and a particular situation weaken the effect of general privacy concerns on information disclosure in a particular situation because incongruent evaluations of alternative values tend to attenuate confidence in an evaluation of the determinants and prevent the access to privacy concerns in the decision making process (Chaiken et al., 1995; Fazio et al., 1986). Thus, people may decide whether to disclose their personal information in a particular situation, regardless of privacy concerns.

- HYPOTHESIS 3 (H3). The effect of general privacy concerns on information disclosure to online vendors in a specific situation becomes neglectable in the presence of a positive inconsistency between high- and low-level construals of benefits and privacy risk.
- HYPOTHESIS 4 (H4). The effect of general privacy concerns on information disclosure to online vendors in a specific situation becomes neglectable in the presence of a negative inconsistency between high- and low-level construals of benefits and privacy risk.

2.5 Experimental Design and Procedure

2.5.1 Measurements

We measured the investigated constructs with question items adapted from previously validated scales, with minor word changes that better fit our participants and context. General privacy concerns were operationalized with 4 items from Dinev and Hart (2006) and Malhotra et al. (2004). Benefits of information disclosure were measured by using 4 items from Xu et al. (2009); privacy risk was measured using 4 items from Xu et al. (2011). All question items employed a seven-point Likert scale, with 1 being "strongly disagree" and 7 being "strongly agree." We also consider age and gender for control. The detailed measurement items are presented in Appendix C.

2.5.2 Experimental Design

To test the moderating effects of consistency and inconsistency between the high- and low-level construals of privacy concern determinants, we designed a three-phase controlled lab experiment.

In phase 1, each participant was presented with a general description of online vendors' data collection practice, then was asked to indicate his or her privacy concerns, assess the key determinants (benefits and privacy risk), and specify the willingness to provide personal information to an online vendor in a general sense. To ensure large psychological distance, the general description offered very limited information regarding general practices of online vendors, without any direct relevance to participants. In this light, the measured key determinants reflect high-level construals of key determinants (i.e., benefits and privacy risk). We classified the participants by high vs. low group along with their perceived benefits and

privacy risk respectively and assigned them into one of the four dimensions: high benefits and high privacy risk (H_BH_R), high benefits and low privacy risk (H_BL_R), low benefits and high privacy risk (L_BH_R), and low benefits and low privacy risk (L_BL_R).

In phase 2, to test the moderating effects of consistency and inconsistency between high- and low-level construals of privacy concerns determinants associated benefits and privacy risk, we manipulated experimental conditions by providing participants with different scenarios: consistency, a positive inconsistency, and a negative inconsistency scenario. We present the scenarios in Appendix B. We attempt to solicit the low-level construals of key determinants by offering situation-specific information of data collection such as a vendor's name and highlighting 'You' for assuring relevancy with them in the scenarios. For the manipulations of consistency and inconsistency condition, we prepared four different scenarios: H_BH_R scenario, H_BL_R scenario, L_BH_R scenario, and L_BL_R scenario. While high benefits scenario suggested seven benefits of information disclosure including monetary rewards such as gift card, low benefits scenario informed two small nonmonetary benefits. High privacy risk scenario informed that a given online vendor had a record of violating Fair Information Practices Principles (FTPPs) of the U. S. Federal Trade Commission multiple times. On the other hand, low privacy risk scenario suggested that a given online vendor fully complies with FTPPs and invests resources for protecting customers' privacy.

For manipulating the consistency condition, participants were presented with a scenario that was congruent with their classified group determined by their indicated values in phase 1. For example, when a participant was classified as H_BH_R group in phase 1, we assigned her into consistency condition by providing H_BH_R scenario. We manipulated a positive inconsistency condition by presenting H_BL_R scenario to participants who were

classified as H_BH_R, L_BH_R, and L_BL_R based on their responses in phase 1 because the scenario provides higher benefits, lower privacy risk, or both to the groups of participants. Thus, the participants classified as H_BL_R in phase 1 were assigned to a consistency or a negative inconsistency condition only in phase 2. We manipulated a negative condition by providing L_BH_R scenario to participants who were classified as H_BH_R, H_BL_R, and L_BL_R based on their indicated values in phase 1 because the scenario shows lower benefits, higher privacy risk, or both to the groups of participants. The participants classified as L_BH_R group in phase 1 were assigned to a consistency or a negative inconsistency condition in phase 2.

2.5.3 Experimental Flow

In Phase 1, we solicited voluntary participants by sending them an invitation email that contains a direct link to the experimental website. In phase 1, we presented a general description about most online vendors' data collection practice. We then measured participants' perceived privacy concerns, benefits, privacy risk, and willingness to provide their personal information to an online vendor, based on the presented general description. We also collected the participants' gender and age for control purposes.

We first calculated z-scores of benefits and privacy risk, respectively. Then we sorted the participants by their z-scores of benefits and classified the top 40% as high benefit group and the bottom 40% as low benefit group. The remaining data points were removed to assure the classification (i.e., high vs. low). Next, all participants were sorted again by their z-scores of privacy risk, and the top 40% and bottom 40% of the participants were classified as high privacy risk and low privacy risk group, respectively. We organized four different groups by joining the classified groups of benefits and privacy risk: H_BH_R, H_BL_R, L_BH_R, and L_BL_R. In

organizing the groups, we removed a participant when he or she was classified as middle group either in benefits, privacy risk, or both.

In phase 2, we invited those who completed phase 1, with a one-week interval to prevent potential carryover effects and attenuate plausible association between high- and low-level construals of benefits and privacy risk, if any. In phase 2, we manipulated three experimental conditions by assigning different scenarios: consistency, a positive inconsistency, or a negative inconsistency. Specifically, participants classified as H_BH_R group in phase 1 were equally assigned to all three different conditions. That is, 1/3 of the participants of the group received H_BH_R scenario and were assigned to a consistency condition, 1/3 were presented with H_BL_R scenario and appointed to a positive inconsistency condition, and the remaining were given L_BH_R scenario and assigned to a negative inconsistency. Those classified as H_BL_R group in phase 1 were equally assigned to two experimental conditions: consistency and a negative inconsistency condition. Half of them were presented with H_BL_R scenario (a consistency condition) and the remaining half were given L_BH_R scenario (a negative inconsistency condition). Participants classified as L_BH_R group in phase 1 were equally assigned to consistency and a negative inconsistency condition. That is, half of them were given L_BH_R scenario (a consistency condition) and the remaining were presented with H_BL_R scenario (a positive inconsistency condition). Finally, participants classified as L_BL_R group in phase 1 were equally assigned to three different conditions: L_BL_R scenario (a consistency), H_BL_R scenario (a positive inconsistency), and L_BH_R scenario (a negative inconsistency). After completing the assignments, we measured their information disclosure to a vendor in the given scenario and examined the relationship between general privacy concerns and information disclosure in a particular situation in each group. The classifications in phase 2 are presented in Table 2.3.

Table 2.3 Assignments of Participants

Group in Phase1		Group in Phase2	Assigned condition
H_BH_R	1/3	H_BH_R	Consistent
	1/3	H_BL_R	A positive inconsistency
	1/3	L_BH_R	A negative inconsistency
H_BL_R	1/2	H_BL_R	Consistent
	1/2	L_BH_R	A negative inconsistency
L_BH_R	1/2	L_BH_R	Consistent
	1/2	H_BL_R	A positive inconsistency
L_BL_R	1/3	L_BL_R	Consistent
	1/3	H_BL_R	A positive inconsistency
	1/3	L_BH_R	A negative inconsistency

Note: H=high; L=low; B=benefits; R=privacy risk; S=privacy self-efficacy; E=response efficacy

For manipulation check for threat appraisal, subjects were asked to answer two questions: (1) how many benefits does a particular online vendor offer? and (2) does the online vendor have a good/notorious reputation regarding information collection and uses?

2.5.4 Pilot Tests

We conducted a pilot test for evaluating experimental design and ensuring clarity and validity of question items, using samples of students. For the student sample, we contacted 153 students enrolled in the business school at a major university located in western United states; among them, 93 students completed all three phases.

Analyses of the pilot data showed that the designed experiment was feasible and

exhibited adequate reliability of the question items as well as their convergent and discriminant validity. The pilot test results affirmed the overall feasibility of experimental design and clarity of the question items with some minor issues.

2.6 Data and Analysis Results

We collected data from students who are enrolled in a major university. We approached 466 U.S. students for their voluntary participation; among them, 376 agreed to take part. Specifically, 376 students participated in phase 1 and answered the questions associated with privacy concerns, benefits of information disclosure, privacy risk and information disclosure behavior. After measurements, we sorted participants based on their z-scores of the components of benefits and privacy risk respectively and classified top and bottom 40% as high versus low group. To assure the classification, we removed a participant when she was classified as middle group either in benefits, privacy risk, or both. In phase 2, 359 students participated in and answered the questions respectively after reading presented scenarios. In phase 2, we excluded the data of participants who provided incorrect answers to the questions for manipulation check. Finally, data of 171 participants were used for analysis. The total number of participants used for data analysis by group and descriptive statistics are presented in Table 2.4 and 2.5.

Table 2.4 The Number of Subjects Used for Data Analysis

	Consistency	Positive inconsistency	Negative inconsistency
Phase 1	376		
Phase 2	69	47	55

Table 2.5 Descriptive Statistics

		Frequency / Average (Std.)	Percent
Gender	Female	129	0.344
	Male	246	0.656
Age		23.8 (4.99)	
Year of university	1	4	0.011
	2	51	0.142
	3	124	0.346
	≥ 4	179	0.500

2.6.1 Measurement Testing Results

We assessed our measurements in terms of construct reliability, and convergent and discriminant validity. To establish indicator reliability, we first removed items with a loading value lower than .6 (Gefen & Straub, 2005). Then we examined construct reliability on the basis of composite reliability, using the common threshold of .7 (Bagozzi & Yi, 1988). As we summarize in Table 2.6, each construct indicated a composite reliability greater than the threshold, suggesting appropriate construct reliability.

Table 2.6. Analysis of Construct Reliability

Construct	Mean (Standard deviation)	Average Variance Extracted (AVE)	Composite Reliability	
			Composite Reliability	Cronbach's alpha
Privacy concerns	19.23 (5.05)	0.771	0.931	0.901
Benefits	17.33 (4.91)	0.780	0.934	0.906
Privacy risk	17.76 (4.88)	0.770	0.931	0.900
Privacy efficacy	17.59 (5.51)	0.768	0.930	0.899
Response efficacy	18.13 (4.17)	0.655	0.884	0.825

We evaluated convergent validity by examining average variance extracted (AVE), using the common threshold of .5 (Götz et al., 2010). We assessed discriminant validity by the square roots of AVEs and the pair-wise correlations between constructs (Fornell & Larcker, 1981). In general, discriminant validity is established when a construct's square root of AVE is significantly greater than the correlation between a pair of constructs. As we show in Tables 2.6 and 2.7, the AVE value of each construct exceeded .5 and was noticeably greater than the correlations between any pair of constructs. Together, our analysis results suggested the measurements possessing adequate convergent and discriminant validity. The measurement testing results suggest that all constructs had proper reliability and construct validity.

2.6.2 Hypothesis Test Results

We analyzed the data using partial least square (PLS). The analysis results are summarized in Table 2.8 and illustrated in Figure 2.2.

Table 2.7. Square Roots of AVE and Correlations between Constructs

	Privacy concerns	Benefits	Privacy risk	Privacy self-efficacy	Response efficacy
Privacy concerns	**0.878**				
Benefits	-0.181	**0.883**			
Privacy risk	0.784	-0.225	**0.878**		
Privacy self-efficacy	-0.016	0.152	-0.008	**0.876**	
Response efficacy	0.032	0.279	-0.070	0.528	**0.809**

Note: The square root value AVE of privacy risk and privacy concerns and their correlations with other constructs are not presented because they are conceptualized as second-order construct

Table 2.8. Summary of Analysis Results

Condition	Exogenous	Endogenous	Path coefficient	Hypothesis	Result
Consistency	GPC	GID	-0.499*** (0.086)	H1(a)	Supported
	GPC	PID	-0.646*** (0.070)	H2	Supported
Positive Inconsistency	GPC	GID	-0.374*** (0.103)	H1(b)	Supported
	GPC	PID	0.186 (n.s.) (0.247)	H3	Supported
Negative Inconsistency	GPC	GID	-0.303* (0.148)	H1(c)	Supported
	GPC	PID	-0.269 (n.s.) (0.262)	H4	Supported

Note: 1) GPC=General Privacy Concerns; GID=Information Disclosure in a general situation; PID=Information disclosure in a particular situation; n.s.=not significant.
2) The value in parenthesis indicates standard error.
*p<0.05, **p<0.01, ***p<0.001

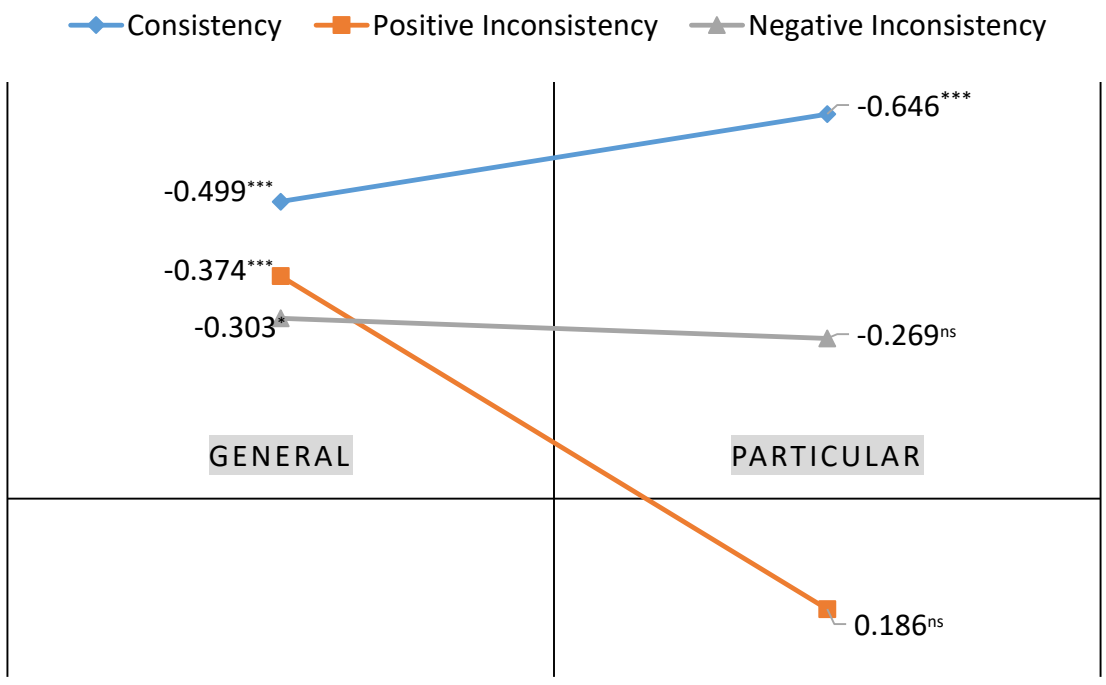


Figure 2.2 Analysis Results

The analysis results indicate that general privacy concerns had significant negative effect on information disclosure in a general situation in all three conditions associated with threat and coping appraisal. Therefore, our data supported H1(a), H1(b), and H1(c).

Under a consistency condition, general privacy concerns had a negative effect on information disclosure in a specific situation. Thus, our data supported H2. In the presence of a positive inconsistency associated with benefits and privacy risk, the effect of general privacy concerns on information disclosure in a particular situation was insignificant, in support of H3. Finally, under a negative inconsistency condition, the effect of general privacy concerns on information disclosure in a particular situation was also neglectable, which supported H4.

Figure 2.2 graphically illustrates the relation between general privacy concerns and information disclosure. The values on "GENERAL" dimension indicate the effects of general privacy concerns on information disclosure in a general situation by experimental conditions. On the other hand, the values on "PARTICULAR" dimension suggest the effects of general privacy concerns on information disclosure in a particular situation by experimental conditions.

We further extend our study for validating the results by using a different set of determinants. PMT suggests self-efficacy and response efficacy as important cognitive appraisals that shape concerns (Maddux & Rogers, 1983). In our context, self-efficacy indicates a person's confidence in his or her ability to effectively protect privacy from a privacy threat (Youn, 2009); response efficacy reveals the person's perceived availability of an effective coping response to protect privacy (Johnston & Warkentin, 2010). We examine whether the effect of general privacy concerns on information disclosure in a particular situation becomes insignificant in a positive and a negative inconsistency condition. We invited those who completed phase 1 of the experiment, with a one-week interval from phase 2 to

prevent potential carryover effects. Among the contacted students, 344 participated in and answered the questions. As in phase 2, we manipulated three different conditions associated with self-efficacy and response efficacy. For a positive inconsistency condition, we presented a high self-efficacy and high response efficacy scenario. In contrast, a low self-efficacy and low response efficacy scenario was presented to manipulate a negative inconsistency condition. As shown in Table 2.9 and Figure 2.3, while the effect of privacy concerns remained significant under a consistency condition, the effect of privacy concerns was neglectable in a positive and a negative inconsistency condition, which fully supported our hypotheses. That is, the privacy paradox occurs when the high- and low-level construals of privacy self-efficacy and response efficacy are inconsistent between a general setting and a particular situation.

Table 2.9. Summary of Analysis Results (Self-efficacy and Response Efficacy)

Condition	Exogenous	Endogenous	Path coefficient
Consistency	GPC	GID	-0.433*** (0.097)
	GPC	PID	-0.253* (0.124)
Positive Inconsistency	GPC	GID	-0.394** (0.135)
	GPC	PID	-0.203 (n.s.) (0.208)
Negative Inconsistency	GPC	GID	-0.362*** (0.112)
	GPC	PID	-0.237 (n.s.) (0.177)

Note: 1) GPC=general privacy concerns; GID=information disclosure in a general situation; PID=information disclosure in a particular situation; n.s.=not significant.
2) The value in parenthesis indicates standard error.
*p<0.05, **p<0.01, ***p<0.001

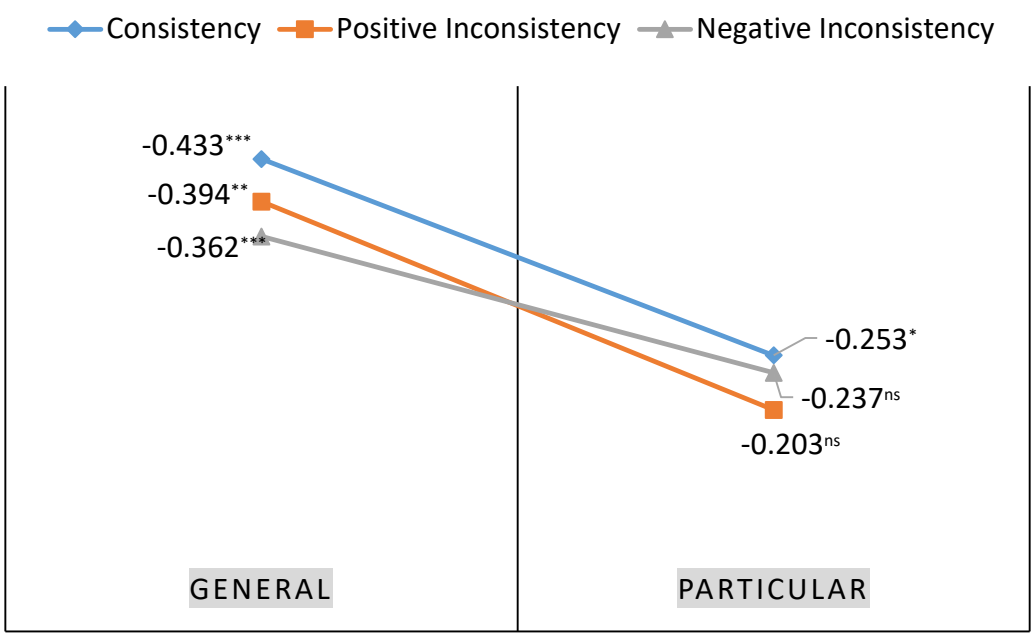


Figure 2.3 Analysis Results Using Self-efficacy and Response Efficacy

To assure the external validity of our findings, we also collected data from MTurk workers. The analysis results demonstrate that the data fully supported hypotheses. Detailed data collection process and data analysis results are presented in Appendix A.

2.6.3 Ex Post Analyses

We empirically examine some essential assumptions of our proposed conceptual model *ex post* to increase the validity of the proposed model. Although the assumptions are essential for the research model, they weren't hypothesized and empirically examined. Further, we compare information disclosure between a general and a particular situation across experimental conditions to offer a plausible explanation of why inconsistency weakens the effect of general privacy concerns on information disclosure in a specific situation.

2.6.3.1 High- and Low-level Construal

Drawing on CLT, we assumed that high-level construals are salient in a general situation while the decreased psychological distance makes low-level construals become more important in a specific situation (Liberman et al., 2007). Thus, we attempted to examine whether the low-level construals are salient in a particular situation by analyzing average time being taken for answering the questions associated with benefits and privacy risk. According to CLT, a psychological distant entity requires people to construe the entity quickly by classifying it into fewer, broader categories (Liberman et al., 2002). In contrast, rich or complex context requires elaborate judgment or evaluation which entails more time and effort for processing associated information (Bhattacherjee & Sanford, 2006; Petty & Cacioppo, 1986). In this light, the low-level construals capture many features of an entity and require more effort and time for processing information associated with the features than high-level construals (Trope & Liberman, 2010). Thus, we expect that participants would take longer time in responding questions in phase 2 than in phase 1. That is, participants spend more time for construing information carefully associated with the key determinants of privacy concerns in a specific situation.

To compare response time between phase 1 and 2, we measured time for answering the questions about benefits and privacy risk in phase 1 in phase 2, respectively. Next, we calculated average responding time of the questions for each phase and then compared the times to examine whether participants spent more time to process information in phase 2. However, we removed a participant whose response time was over 30 minutes in total because all participants in our pilot test completed each survey in 15 minutes on average with standard deviation of ±5.02. The analysis result is presented in Table 2.10.

Table 2.10 Comparison of Response Time between a General and Particular Situation

Response time (second)		F-statistic
Phase 1	Phase 2	
9.71	12.90	28.751***

Note: Response time is the average time taken for responding a question, ***p<0.001

The analysis results demonstrated that participants took longer time in phase 2 than in phase 1, suggesting that high (low)-level construals are salient in a general (particular) situation: people construe determinants of privacy concerns more specifically in a specific situation (i.e., low-level construals).

2.6.3.2 Test of Classification

We assumed that scenarios properly manipulated experimental conditions. To test the assumption, situation-specific determinants of privacy concerns were measured at the end of phase 2. Then we compared the scores of benefits and privacy risk between a general and a particular situation respectively across different experimental conditions.

As shown in Table 2.11, the results demonstrate that our classifications overall worked properly. For a consistency condition, perceived benefits and privacy risk in a particular situation were not significantly different from those in a general situation respectively. Participants in a consistency condition experienced marginal change in their perceived benefits and privacy risk during the traverse to a particular situation. For a positive inconsistency condition, participants perceived higher benefits and lower privacy in a particular situation than in a general situation, in support of our expectation in the condition. Finally, for a negative inconsistency condition, participants perceived lower benefits and higher privacy risk in a particular situation, which supports our classification.

Table 2.11 Results of Classification Test

Condition	Determinants	General	Particular	F-statistic	Classification
Consistency	Benefits	18.81	17.43	1.98 n.s.	Supported
	Privacy risk	17.07	18.82	1.29 n.s.	Supported
Positive Inconsistency	Benefits	15.83	18.36	5.81**	Supported
	Privacy risk	19.40	13.13	56.31***	Supported
Negative Inconsistency	Benefits	19.84	14.47	26.89***	Supported
	Privacy risk	13.40	15.18	61.62***	Supported

Note: n.s.=not significant,
*p<0.05, **p<0.01, ***p<0.001

2.6.3.4 Comparison of Information Disclosure

Our results show the neglectable effect of general privacy concerns when the high- and low-level construals of privacy concerns determinants are inconsistent. A plausible explanation is: when the evaluations of alternative values are inconsistent and thus the confidence in existing attitude is low, people tend to engage in more systematic information processing to attain sufficient confidence (Jonas et al., 1997). In this light, when the construals of privacy concerns determinant are inconsistent (i.e., either a positive or negative inconsistency), people are less confident in their evaluations of the determinants and attempt to more systematically process information associated with the factors in a specific situation. In the process, they put more weight on situation-specific information because it is more detailed and relevant. As a result, information disclosure is more likely to be driven by the processed situation specific information, regardless of existing privacy concerns. Thus, information disclosure in a particular situation would be significantly higher (lower) than that in a general situation under a positive (negative) inconsistency condition. On the other hand, information disclosures between a general and particular

situation would be not significantly different under a consistency condition. Thus, we compared information disclosure between a general and particular situation across different experimental conditions. Table 2.12 summarizes the analysis results. The results fully supported our expectations, suggesting that people decide information disclosure based on situation specific information when the construals of benefits and privacy risk are inconsistent.

2.7 Discussion

Our paper contributes to IS research by providing a logical explanation of why people willingly disclose their personal information to online vendors or firms, not in sync with their privacy concerns. Especially, our longitudinal approach theoretically contributes to literature by considering construals of both general and situational factors and examining the effects of their inconsistency on the relation between general privacy concerns and information disclosure in a particular situation. We suggest that information disclosure in a particular situation is not in sync with general privacy concerns when people's construed determinants of privacy concerns are inconsistent between a general setting and a particular

Table 2.12 Comparison of Information Disclosure between the Situations

Condition	Average of GID	Average of PID	F-statistic
Consistency	2.812	2.928	0.203 (n.s.)
Positive Inconsistency	3.021	3.447	2.866*
Negative Inconsistency	2.582	1.618	25.451***

Note: GID=information disclosure in a general situation; PID=information disclosure in a particular situation; n.s.= not significant.

*p<0.05, **p<0.01, ***p<0.001

situation (i.e., the privacy paradox). In contrast, when the construed determinants are consistent, privacy concerns have significant effect on information disclosure in a particular situation.

Our findings provide several implications. First, the results highlight the importance of a dynamic or longitudinal approach for explaining the inconsistent effect of privacy concerns. While previous studies commonly examine the respective effects of either generic or situational factors, the interaction or joint effect of generic and situation specific factors has received relatively little attention. However, the examination of joint effect seems essential for a better understanding of inconsistent effect of privacy concerns because people tend to adjust their attitude or belief such as privacy concerns by referring to situational cues (Li et al., 2011). That is, the effect of privacy concerns can differ by how much a person significantly consider situational information and adjust her existing attitude (i.e., privacy concerns). In this light, a longitudinal approach is imperative for tracking how individuals refer to situational information and change their attitude and scrutinizing the joint effect of generic and situational factors on behavior. Further, previous studies seem inconclusive whether situational cues override the effect of generic factors such as attitude. For example, while Li et al. (2011) observe greater effect of situational cues on behavior, Terry (1994) suggests that general attitude or belief is not changed in a short time and considered to have a greater effect on behavior than a situational factor does. Thus, it is important to capture how a person changes her attitude by referring to situational information for a better understanding of unstable effect of generic factors, which requires a longitudinal approach, instead of exclusive consideration of generic or situational factors.

Second, our study highlights the effect of psychological distance toward a focal

object on attitude or behavior. Although previous studies empirically examine the effects of situational factors on behavior (e.g., Kehr et al., 2015; Li et al., 2011), little is known about how situational information changes an existing attitude or belief which is stable and resists changes (Ajzen, 1991). Psychological distance offers a plausible explanation. In a particular situation, people tend to systematically process situation specific information associated with a focal object due to the significant psychological distance toward that object. More careful and thorough information processing increases the confidence in and reliability of the processed information, which have greater effects on behavior than information processed abstractly. This calls for the necessary of examining 'how' people perceive an object, instead of analyzing perception itself. Previous IS studies have often captured a perception of an object and analyzed its effect on behavior (e.g., perceived usefulness of a technology). However, our study suggests that behavior is explained not only by the perception of an object but also by how an object is perceived (e.g., abstractly or systematically). Further, our finding reveals the association between the presence of a specific situation and psychological distance. People seem to perceive an object as psychologically near especially when specific situation associated with the object is given, which offers more detailed information of and higher relevance with the object. In this light, our findings highlight the association between the specificity of a situation and the way of perceiving an object

Third, previous studies examine the effect of psychological distance on the level of construal commonly from a static view (e.g., Alter & Oppenheimer, 2008; Bornemann & Homburg, 2011; Liberman & Förster, 2009). However, our results suggest the necessity of examining how the decrease or increase of psychological distance of a focal object affects

the level of construal and accordingly changes associated attitude or belief. When perceived psychological distance toward a focal object changes, the corresponding construals are affected and changed. When the results of changed construals toward an object confirm pre-existing construals, the evaluation or interpretation of the object remains unchanged. On the other hand, when the changed construals contradict pre-existing construals, the evaluation of the object can be changed. Thus, our approach helps to reconcile the mixed results of privacy concerns' effect by specifying the condition in which privacy paradox occurs. Our finding Privacy concerns can't explain or predict information disclosure when the construals of privacy concerns determinants between a general setting and a particular situation are inconsistent. The examination of psychological distance change sheds light on the attitude-behavior gap. The effect of existing attitude on behavior is moderated by the degree to changed construals are congruent with pre-existing construals. While the consistency of construals strengthens the effect of attitude, the inconsistency of the construals weakens the stability of the relation and attenuates the effect of attitude.

Finally, our results seem to support heuristic-systematic model (HSM) (Bohner et al., 1995; Chaiken et al., 1989). According to the model, when confidence in evaluations of a focal object is insufficient, people tend to systematically process information for attaining confidence in their evaluations. In contrast, when a certain level of confidence in their evaluations is attained, people tend to process information heuristically. Our *ex post* analysis results demonstrate that individuals were more (less) likely to disclose personal information in a positive (negative) inconsistency condition, whereas their information disclosure is not significantly different in a consistency condition. The findings suggest that people may engage in heuristic information processing when the construals between a general setting

and a particular situation are consistent, which offers consistent evaluations and thus provides a certain confidence in the evaluations. On the other hand, the inconsistency of construals weakens the confidence in the construals and requires processing relevant information more systematically. When people engage in systematic information processing, they are expected to more consider situation specific information because it is more detailed and relevant. As a result, people tend to decide whether to disclose personal information solely based on the result of situation specific information processing, regardless of privacy concerns.

CHAPTER 3

THE KEY DETERMINANTS OF ONLINE PRIVACY CONCERNS IN E-COMMERCE: A CROSS-COUNTRY STUDY

3.1 Introduction

With the help of information technology, online vendors can collect massive personal information at low costs (Ashworth & Free, 2006; Dinev & Hart, 2006). The prodigious collections and detailed analyses of personal information by online vendors or firms, however, raises privacy concerns which refer to individuals' concerns of an online vendor's practices associated with collection and use of provided personal information (Son & Kim, 2008). Privacy concerns indeed have significant impacts on individuals' behaviors in e-commerce and accordingly become crucial to online vendors and consumers (Awad & Krishnan, 2006; Smith et al., 2011; Xu et al. 2009). In this light, the effects of privacy concerns have been of primary interest to information system (IS) researchers, particularly in e-commerce (Dinev & Hart, 2006; Malhotra et al., 2004; Smith et al., 2011).

While the effects of privacy concerns have been primarily examined, essential sources of online privacy concerns and the process underlying their formation have received relatively little attention, despite their importance to IS research and practice (Smith et al., 2011; Xu et al., 2008). For example, by better understanding key concern determinants and the underlying process, online vendors can devise and implement

effective measures to mitigate consumers' privacy concerns and thereby foster their transactions or services utilization online. In this study, we seek to offer a theory-based explanation of how individuals form privacy concerns in e-commerce by identifying essential generic and e-commerce specific determinants of privacy concerns and examining their direct and indirect effects. We first choose generic factors that shape privacy concerns based on protection motivation theory (PMT), which suggests people's protection behaviors are motivated by their cognitive appraisals of several essential components of a fear appeal: cognitive appraisal of vulnerability, severity, self-efficacy, and response efficacy (Maddux & Rogers, 1983; Rogers, 1983). Vulnerability refers to the conditional probability that a threatened event would occur; severity denotes the magnitude of noxiousness of a threatened event. While self-efficacy indicates a person's confidence in his or her ability to successfully adopt a recommended coping strategy, response efficacy denotes the availability and effectiveness of a coping strategy. In the perspective of PMT, privacy concerns can be viewed as a mediating variable that explains the relationship between the cognitive appraisals and privacy protecting behaviors (Li et al., 2012; Youn, 2009). That is, customers form privacy concerns by cognitively appraising vulnerability, severity, self-efficacy, and response-efficacy and in turn decide their privacy protecting behaviors.

Perceived fairness in the information collection process is considered an essential e-commerce specific determinant of privacy concerns. In information exchange, customers consider their personal information as an input of the exchange (Ashworth & Free, 2006). Online information exchanges are perilous to information providers due to the likelihood of online vendors' opportunistic behaviors: they could pursue their profits at the expense of information providers' benefits by hiding a key piece of information pertaining to the

use of collected information (Pavlou et al., 2007). Fairness of the information collection process is a central element of fair information exchange and often used for gauging opportunistic behavior of an online vendor (Ashworth & Free, 2006). Fairness in the information collection process leads customers to perceive an online vendor as ethical, which alleviates the fear of an online vendor's opportunistic behavior and accordingly diminishes customers' privacy concerns, thereby motivating information disclosure; in contrast, violations of fairness in the information collection process escalate people's privacy concerns and discourage them from providing personal information to an online vendor (Ashworth & Free, 2006; Culnan & Bies, 2003;). In specific, we focus on notice and consent, which are two core components of fairness in information collection process (Culnan & Armstrong, 1999). While notice refers to an online vendor's practices of revealing information relevant to data collection and use to information providers, consent indicates the practice of securing information providers' authorization for information collection and use (Ashwarth & Free, 2006). Fairness in information collection process is established when relevant information is provided, direct control over personal information is allowed through consent procedure, or both (Culnan & Armstrong, 1999; Xu et al., 2012).

In addition, we attempt to provide a fuller explanation of the forming process of privacy concerns by examining both direct and indirect effects of key privacy concerns' determinants. Although PMT helps identify essential sources of privacy concerns, there have been voices to highlight their indirect effects due to the associations among the distinctive cognitive appraisals (Maddux & Rogers, 1983; Neuwirth et al., 2000). For example, perceived risk of engaging in a situation is affected by perceived capability of managing a threatening situation (i.e., self-efficacy) (Bandura, 1989). In this light,

examining indirect effects of key determinants offers a better depiction of the process underlying the formation of privacy concerns. Further, the consideration of indirect effects helps explain why some empirical findings are not in sync with the corresponding theory-based propositions or hypotheses. For instance, Youn (2009) observed insignificant effect of self-efficacy on privacy concerns. Overall, anchored on PMT and fairness in information collection process, we develop a research model in which privacy concerns are directly influenced by threat appraisal (vulnerability and severity), coping appraisal (self-efficacy and response-efficacy), and fairness appraisal (notice and consent). Further, we model that coping and fairness appraisal indirectly affect privacy concerns through formed threat appraisals of information disclosure. To test whether the consideration of indirect effects of the antecedents offer better explanation, we compare our model with a direct effect model that considers direct effects of privacy concerns' determinants.

We also test the proposed model empirically using cross-cultural data. In line with Griffith et al. (2000) and Kim (2008), we identify two types of cultures by combining the national cultural dimensions from Hofstede's study (1994): individualistic-weak uncertainty avoidance-small power distance culture (type I) versus collectivistic-strong uncertainty avoidance-large power distance culture (type II). We collected data from two countries: the U.S. and South Korea (hereafter S. K.). While the U.S. can be categorized as a type I culture, S.K. is a representative country that belongs to type II culture. [4] We compare the effects of selected antecedents of privacy concerns at both construct and path coefficient levels between the countries. The comparison sheds light on the role of culture

[4] Hofstede's scores of the U.S. and S.K. by three cultural dimensions are: individualism (U.S.=91, S. S.K.=18), uncertainty avoidance (U.S.=46, S. S.K.=85), and power distance (U.S.=40, S.K.=60) (The Hofstede Center [http://geert-hofstede.com/]).

in forming privacy concerns in e-commerce. In specific, while the comparison at construct demonstrates the direct effect of culture on privacy concerns' determinants, the comparison at path coefficient level helps figure out the moderating effects of culture. We discuss the comparison results and offer plausible explanations of such direct and indirect effects of culture, which may help reconcile the mixed results of a culture's effects on privacy concerns (e.g, Bellman, et al., 2004; Cho et al., 2009; Krasnova et al., 2014; Milberg et al., 1995).

3.2 Literature Review

3.2.1 Theoretical Foundation in Selecting Antecedents of Privacy Concerns

We summarize the theoretical foundations adopted in representative previous studies for choosing antecedents of privacy concerns in Table 3.1. As shown in the table, most representative previous studies determine antecedents of privacy concerns without a proper theoretical foundation.

3.2.2 Determinants of Privacy Concerns

Smith et al. (2011) and Li (2011) propose a macro model of privacy concerns, which suggests integrative perspective of antecedents and consequences of privacy concerns. In the model, Smith et al. (2011) categorize antecedents of privacy concerns as privacy experience, privacy awareness, personality differences, demographic differences, and culture. On the other hand, Li (2011) classifies determinants of privacy concerns as knowledge and experience, computer anxiety, need for privacy, computer self-efficacy, demographic factors, and personality traits. As shown in Table 3.2, an extensive literature review suggests further categorization of the antecedents: individual perception (belief), experience, individual

Table 3.1 Theoretical Foundations of Representative Previous Studies

Research	Antecedents	Theory Employed to Select Antecedents	Theory Employed to Explain Focal Behavior
Culnan and Armstrong (1999)	• Procedural fairness	No[a)]	No
Dinev and Hart (2005)	• Internet literacy • Social awareness	No	No
Dinev and Hart (2006)	• Perceived Internet privacy risk	No	• Privacy calculus model
Hann et al. (2007)	• Positive valence (incentive)	No	• Information-processing theory of motivation
Jiang et al. (2013)	• Perceived anonymity of self • Perceived anonymity of others • Perceived intrusiveness	No	• Hyper personal framework • Privacy calculus model
Pavlou et al. (2007)	• Trust • Website informativeness • Social presence	• Social presence theory[b)]	• Principal-agent perspective
Smith et al. (1996)	• Privacy invasion experience • Knowledge of media coverage • Personality ○ Cynical distrust ○ Paranoia ○ Social criticism	No	No
Stewart and Segars (2002)	• Computer anxiety	No	No
Xu et al. (2011)	• Privacy control • Privacy risk • Disposition to value privacy	• Communication Privacy Management Theory	
Xu et al. (2012)	• Perceived control over personal information	No[c)]	No

Note: a) We do not consider procedural fairness as a theory because of the longstanding debate and lack of a consensus on whether procedure fairness constitutes a theory.
b) Social presence theory is used as the foundation for explaining the relationship between social presence and privacy concerns only.
c) Control agency theory is employed to explain amplifications of personal controls as well as preferences toward direct personal controls, but not for identifying essential sources of privacy concerns.

Table 3.2 Classification of Key Determinants of Privacy Concerns Examined by Previous Studies

Category		Exemplar Determinants	Studies	Hypothetical Effect on Privacy Concerns	Context
Perception (belief)	Risk-specific	Perceived privacy risk	Dinev and Hart (2006)	Positive direct effect (significant)	E-commerce
			Xu et al. (2011)		Electronics Social networking Finance Healthcare
		Information sensitivity	Gu et al. (2017)	Positive direct effect (significant)	Mobile app download
	Ability-specific	Privacy control	Xu et al. (2011)	Negative direct effect (significant)	Electronics Social networking Finance Healthcare
			Xu et al. (2012)		A location tracking service (location-aware mobile-coupon service)
			Gu et al. (2017)	Negative direct effect (significant)	Mobile app download

Table 3.2 Continued

Category		Exemplar Determinants	Studies	Hypothetical Effect on Privacy Concerns	Context
Perception (belief)	Ability-specific	Self-efficacy	Youn (2009)	Negative direct effect (insignificant)	Internet use
			Yao et al. (2007)	Indirect effect through internet use diversity and experience (insignificant)	Internet use
	Exchange-specific	Fair information practice	Culnan and Armstrong (1999)	Negatively moderating the effect of privacy concerns on information disclosure (significant)	Commerce
	Social-specific	Social awareness	Dinev and Hart (2005)	Positive direct effect (significant)	E-commerce
	Website-specific	Social presence	Pavlou et al. (2007)	Negative direct effect (significant)	E-commerce
		Web-informativeness			

Table 3.2 Continued

Category		Exemplar Determinants	Studies	Hypothetical Effect on Privacy Concerns	Context
Perception (belief)	Website-specific	Third party certificate	Nam et al. (2006)	Negative direct effect (significant)	E-commerce
		Reputation	Eastlick et al. (2006)	Negative direct effect (significant)	E-commerce
			Nam et al. (2006)	Negative direct effect (insignificant)	E-commerce
Experience			Smith et al. (1996)	Positive direct effect (significant)	Organizational information practice
			Okazaki et al. (2009)	Positive direct effect (significant)	Mobile phone use
			Gu et al. (2017)	Positive direct effect (significant)	Mobile app download

Table 3.2 Continued

Category	Exemplar Determinants	Studies	Hypothetical Effect on Privacy Concerns	Context
Individual characteristics	Personality	Korzaan and Boswell (2008)	Extroversion: positive direct effect (insignificant) Agreeableness: positive direct effect (Significant) Conscientiousness: positive direct effect (insignificant)	Commerce
		Bansal et al. (2016)	Extroversion: negative direct effect (e-commerce) Agreeableness: positive direct effect in all settings. Emotional instability: positive direct effect in all settings.	E-commerce Finance Health
	Demographic factors (e.g., gender, age)	Youn and Hall (2008)	Gender (male): direct positive effect (significant)	Internet use
		Sheehan (1999)	Gender (male): direct positive effect (significant)	E-commerce
		Campbell (1997)	Age: direct positive effect (significant)	Commerce

Table 3.2 Continued

Category	Exemplar Determinants	Studies	Hypothetical Effect on Privacy Concerns	Context
Culture	Cultural dimensions	Milberg et al. (1995)	UAI and PDI: positive direct effect (insignificant)	E-commerce
		Bellman et al. (2004)	PDI, IDV, MAS: negative direct effect (significant)	E-commerce
		Lowry et al. (2011)	IDV and PDI: negative direct effect (significant) UAI: positive direct effect (significant) MAS: negative direct effect (insignificant)	Instant messenger

Note: IDV=individualism, PDI=power distant index, UAI=uncertainty avoidance index, and MAS=masculinity

characteristics (e.g., personality or demographics), and culture.

Privacy risk has been regarded as an important source of privacy concerns in previous studies (Dinev & Hart, 2004; Dinev et al, 2013; Xu et al., 2011). Privacy risk generally denotes the expectation of a potential loss associated with the release of personal information (Malhotra et al., 2004; Xu et al., 2011). In e-commerce, privacy risk is closely related to online vendors' opportunistic behaviors that may cause the loss of privacy (Pavlou et al., 2007). In particular, the illiteracy of who accesses the provided information and how it is used leads people to sense a greater risk associated with information disclosure and thereby increases privacy concerns (Baek, 2014; Dinev & Hart, 2006).

Perceived privacy control is also presented as a key determinant of privacy concerns. According to Xu et al. (2011, p. 804), privacy control indicates "a perceptual construct reflecting an individual's beliefs in his or her ability to manage the release and dissemination of personal information." The perceived ability to control provided personal information attenuates privacy concerns and thus motivates information disclosure (Dinev & Hart, 2004). Drawing on Communication Privacy Management (CPM) theory, Xu et al. (2011) also suggest privacy risk and control as essential determinants of privacy concerns because concerns about privacy stem from the perceived boundary of the information space consisting of perceived risk and privacy control. Similarly, self-efficacy, confidence in ability to protect privacy, is argued to affect privacy concerns (Youn, 2009; Yao et al., 2007). While Youn (2009) argues direct effect of self-efficacy on privacy concerns, Yao et al. (2007) examine its indirect effect through Internet use diversity and experience. However, their analysis results didn't support the hypothesized effect of self-efficacy on privacy concerns.

Alternatively, some previous research emphasizes the role of context-specific factors such as website informativeness, social presence, or reputation (Eastlick et al. 2006; Pavlou et al., 2007). Pavlou et al. (2007) examine the effect of website informativeness, social presence, and trust on privacy concerns. Website informativeness relieves information asymmetry between sellers and buyers and decreases the likelihood of sellers' opportunistic behaviors, which, in turn, attenuate privacy concerns. Social presence, which indicates the degree to which a website conveys the presence of sellers behind the website, also mitigates privacy concerns by shortening the psychological distance between sellers and buyers. Nam et al. (2006) scrutinize the effects a website reputation and third-party certificate on privacy concerns.

Individual characteristics such as personal traits are also identified to affect privacy concerns. For example, Junglas et al. (2008) examine the relationship between personality trait measured by Big Five scales and privacy concerns in a location-based service context. They found that people tend to be less concerned about privacy as their personality is more agreeable, conscientious, and open to experience. Korzaan and Boswell (2008) also scrutinize the effect of individual personality but find agreeableness as a meaningful antecedent of privacy concerns. According to Pedersen (1987), introverted people are more concerned about privacy and therefore have a stronger urge for anonymity than extraverted counterparts. Smith et al. (2006) report significant positive effects of individual personality factors including cynical distrust, paranoia, and social criticism. Demographic factors such as gender or age affect privacy concerns as well. In general, men, younger, less educated, or poorer people appear to have less privacy concerns than women, older, more educated, or more wealthy people (Culnan, 1993; Sheehan, 1999).

3.2.3 Gap Analysis

Although previous studies examine a number of antecedents of privacy concerns such as experience, privacy awareness, demographic factors, or personality traits (Li, 2012; Smith et al., 2011), a review of extant literature reveals several gaps that deserve to receive more research attention and motivate our investigation of key sources of online privacy concerns. Many previous studies tend to rely on previous studies for choosing important antecedents to examine, such that the legitimacy and validity of chosen factors are not sufficiently assured. Choosing key determinants without a proper theory does not assure that a chosen factor is important and all essential determinants are considered. A proper theory renders legitimacy of the antecedent choices by providing established premises for explaining why particular antecedents should be emphasized and how they may lead to the creation of online privacy concerns. Furthermore, many previous studies seem to offer incomplete explanation of privacy concerns' antecedents by exclusively focusing on generic (e.g., perceived privacy risk) or context-specific factors (e.g., website reputation), which are both essential in shaping privacy concerns. Especially, in e-commerce, individual perceive their personal information as an input into an exchange with online vendors and expect rewards (such as monetary compensation) as an output of the exchange, which is an important feature of information exchange (Acquisti & Grossklags, 2005; Ashworth & Free, 2006). In this light, considering both generic and information exchange specific factors would provide a better explanation of the formation of privacy concerns in e-commerce. Third, with regard to the underlying process of forming privacy concerns, previous studies seem to ignore the indirect effects of privacy concerns determinants, which offers limited explanation of why some empirical findings are not in sync with the

corresponding theory-based propositions or hypotheses. For example, Youn (2009) and Yao et al. (2007) report an insignificant effect of self-efficacy on privacy concerns, in opposition to their hypothesis. The examination of indirect effects of self-efficacy on privacy concerns could shed light on this observed discrepancy.

Overall, our literature review reveals several privacy concerns determinants, mostly associated with individual perceptions or belief. However, as Smith et al. (2011) note, an integrative approach is required to have a more cohesive and systematic understanding of essential sources of privacy concerns. In addition, the exclusive focus on either generic factors such as privacy risk or context-specific factors such as website informativeness may offer incomplete explanation of key determinants of privacy concerns. Our literature review also indicates the need for an appropriate theoretical foundation for identifying important concern determinants to examine, which allows a logical justification for the determinant choices and offers a legitimate perspective on how they affect privacy concerns.

3.3 Theoretical Foundation

Drawing on protection motivation theory (PMT) (Rogers, 1975, 1983), we identify generic key determinants of privacy concerns. The central premise of PMT is that a person's protection behaviors are motivated by his or her cognitive appraisals of vulnerability, severity, response efficacy, and self-efficacy (Maddux & Rogers, 1983; Rogers, 1983). Such cognitions can be organized along two distinct mediating appraisals: threat and coping appraisal (Floyd et al. 2000). While the threat appraisal focuses on the benefits of maladaptive response, vulnerability, and severity, the coping appraisal centers

self-efficacy, response-efficacy, and the costs of an adaptive coping response. The perceived benefits of maladaptive response would diminish the probability of adopting a protective behavior against privacy risk. In contrast, the threat would augment the probability of engaging in protective behavior. In light of this theory, online privacy concerns can be viewed as a variable mediating the effects of the respective cognitive appraisals on a person's privacy protection behavior (Youn, 2009).

We apply several appropriate adjustments for the use of PMT to identify key determinants of privacy concerns to fit our context. For example, we consider privacy risk which encompasses both vulnerability and severity. Privacy risk denotes the potential loss of privacy and incorporates both the likelihood of experiencing negative outcomes (vulnerability) and the magnitude of such negative outcomes (severity) (Xu et al., 2011). Privacy risk is a validated measure of the cost of information disclosure by many previous studies, e.g., Dinev and Hart (2006); Hong and Thong (2013); Malhotra et al. (2004). The costs of adaptive response are not considered because customers may choose from multiple (alternative) adaptive responses that differ in their adopting costs, which makes it difficult to accurately measure a general cost of adaptive response. Furthermore, privacy self-efficacy appears more relevant and adequate to individual privacy in e-commerce than general self-efficacy of successfully adopting effective response. Privacy self-efficacy refers to a person's confidence in his or her ability to protect privacy from a threat (Youn, 2009).

We also emphasize perceived fairness of information collection process as an antecedent of privacy concerns, specific to e-commerce. The perceived fairness of information collection process decreases privacy concerns by escalating customers' perceived trustfulness of an online vendor and leading to believe their direct control over provided personal

information (Xu et al., 2012). Thus, fairness tends to alleviate the fear of an online vendor's opportunistic behavior (Ashworth & Free, 2006; Culnan & Armstrong, 1999). In contrast, a violation of fairness in information collection process amplifies privacy concerns due to the likelihood of an online vendor's opportunistic behavior (Ashworth & Free, 2006; Culnan & Bias, 2003; Pavlou et al., 2007). This particular fairness highlights the importance of an online vendor's notice about what information is collected and how it is used and direct control over personal information through consent procedure (Ashwarth & Free, 2006). That is, in e-commerce, customers tend to sense an information collection process as fair when essential and relevant information about data collection and use is provided or direct control over personal information allows through consent procedure (Ashworth & Free, 2006; Culnan & Bias 2003).

Overall, drawing on PMT and fairness in information collection process, we finalize key determinants of privacy concerns in e-commerce: vulnerability and severity (threat appraisal), self-efficacy and response-efficacy (coping appraisal), and notice and consent (fairness appraisal). However, we conceptualize privacy risk as a second-order construct that embraces vulnerability and severity, consistent with Xu et al. (2011), which suggest that privacy risk encompasses both the likelihood of experiencing negative outcomes (i.e., vulnerability) and the magnitude of such negative outcomes (i.e., severity). We also employ privacy self-efficacy, instead of self-efficacy, which refers to confidence in one's ability to protect privacy from a threat to fit our context (Youn, 2009). As a result, we consider privacy risk, self-efficacy, response-efficacy, notice, and consent as key determinants of online privacy concerns in e-commerce settings.

3.4 Research Model and Hypothesis

Our research model suggests that coping and fairness appraisals determine privacy concerns directly as well as indirectly through privacy risk. Both PMT and fairness of information collection process posit direct effects of cognitive appraisals of threat, coping, and fairness appraisals on privacy concerns. In addition to their direct effects, coping and fairness appraisals would also indirectly determine privacy concerns through privacy risk. People confident in their ability to control a threatening situation tend to perceive a lower risk than otherwise (Bandura, 1977). Furthermore, the fairness of information collection process, as perceived by customers, would mitigate their fear of an online vendor's opportunistic behavior and lead to perceive risk to be low. Response efficacy is assumed to have a positive effect on privacy self-efficacy because available effective protections increase a person's confidence in her ability to handle a threatening situation. Consent affects notice information practice because offering relevant information is inevitable for getting permission of data collection and use from information providers.

We also compare our proposed research model with direct effect model as a benchmark. In the model, the antecedents of privacy concerns directly affect privacy concerns of information disclosure to online vendors. The comparison would demonstrate whether the inclusion of indirect effects can provide more explanatory power. We illustrate the research model and benchmark model in Figures 3.1 and 3.2.

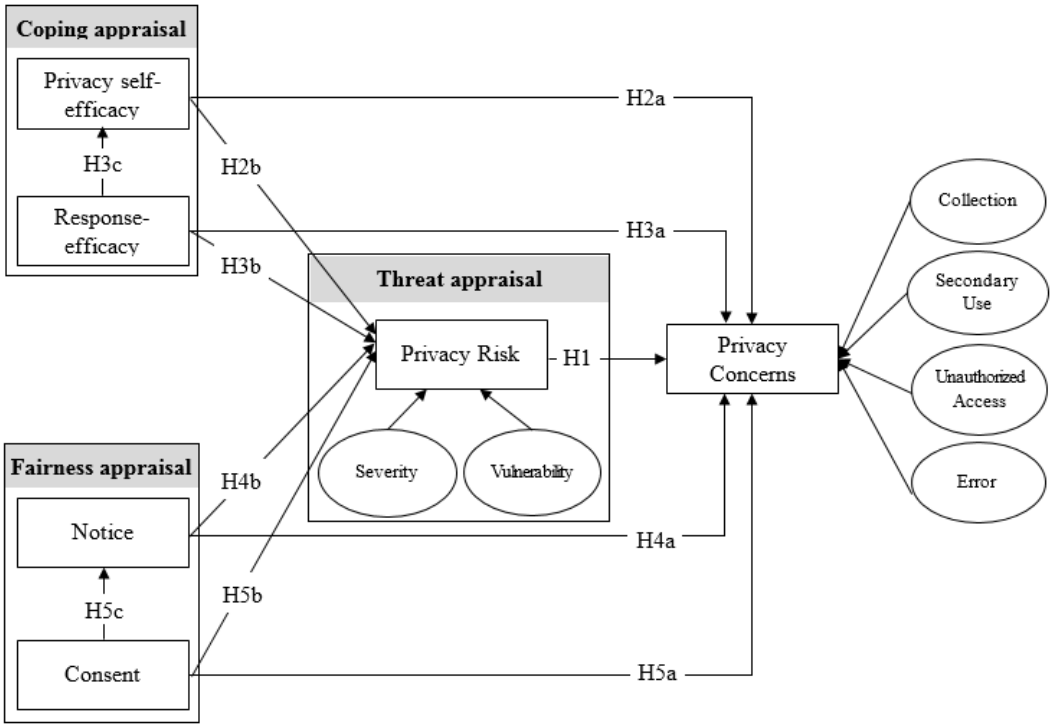


Figure 3.1 Research Model

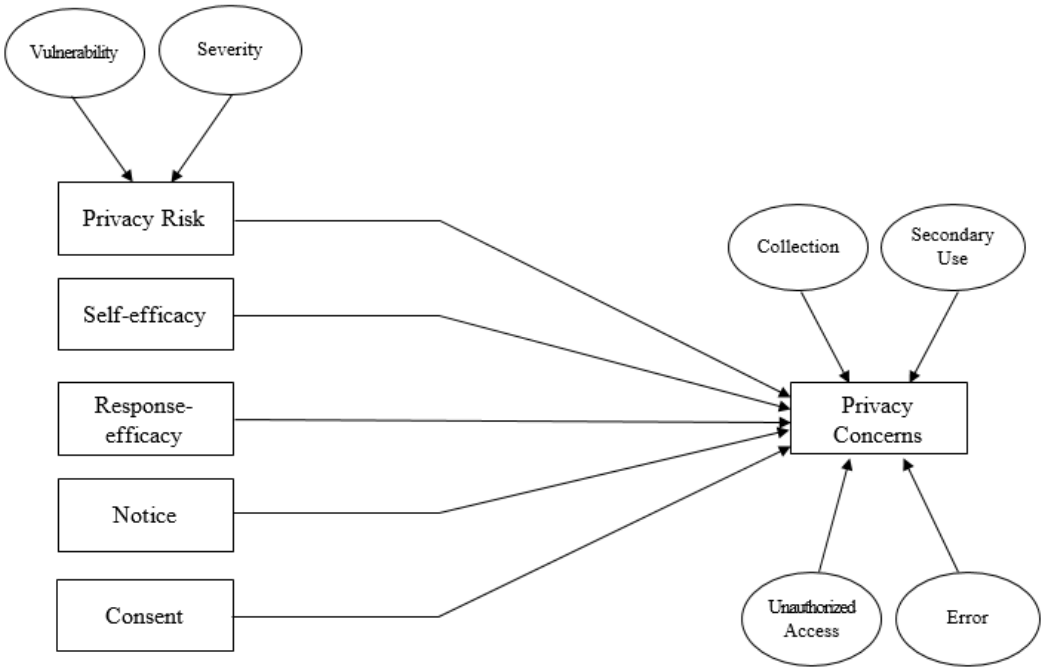


Figure 3.2 Direct Effect Model (Benchmark)

3.4.1 Privacy Risk (Threat Appraisal)

PMT states perceived vulnerability and severity of negative consequence as important sources of a fear (Maddux & Rogers, 1983; Rogers, 1975). The potential loss of privacy and the associated negative consequences of providing personal information to online vendors increase people's concerns about privacy and thus restrict such behaviors to protect their privacy (Youn, 2009). Consequently, privacy risk positively associates with privacy concerns: people become more concerned about their privacy, as they perceive more privacy risk associated with their information disclosure to an online vendor (Dinev & Hart, 2006; Xu et al., 2011). Therefore, we hypothesize:

- HYPOTHESIS 1 (H1). Privacy risk is positively associated with privacy concerns.

3.4.2 Coping Appraisal

According to PMT, self-efficacy and response-efficacy mitigate anxiety about negative consequences because ability to manage a threat and successful adoption of a coping strategy can prevent the occurrence of adverse consequences (Maddux & Rogers, 1983; Rogers, 1975). In this light, customers' confidence in their ability to protect privacy and the available effective means for protecting privacy mitigate privacy concerns, thereby encouraging information disclosure to an online vendor.

Self-efficacy theory (Bandura, 1977) can help explain indirect effect of privacy self-efficacy on privacy concerns through privacy risk. According to the theory, customers who perceive self-efficacy (personal mastery) exceeding a threatening situation tend to engage in the situation because they believe their capability to handle the situation. In contrast, when perceiving their self-efficacy insufficient for a threatening situation, customers tend

to lack the conviction of handling the situation and therefore choose to avoid it. Such perceived manageability of a threatening situation significantly affects risk assessment: customers convinced of their capability of handling a threatening situation tend to assess the associated risk to be low (Beck, 1984). In addition, the assured controllability over a potential threat often leads people to perceive a situation in an excessively optimistic manner and unduly assess the risk to be low (Bandura, 1989). As a result, customers' confidence in protecting their privacy reduces their awareness of privacy risk associated with a vendor's collecting personal information and thus increases the willingness to provide personal information. Therefore, privacy self-efficacy is negatively associated with privacy risk. In the same way, an available effective coping strategy to a threatening situation is believed to prevent the occurrence of adverse consequences and therefore lead customers to perceive privacy risk to be low (Maddux & Rogers, 1983). We also posit indirect effect of response efficacy on privacy concerns through privacy self-efficacy. When an effective coping response is perceived, customers may believe they can more control over threat stimuli. In other words, the presence of an effective coping response would increase customers' belief that they can exercise control over risky situation and thus augment their confidence in ability to protect privacy from a threat. Therefore, we hypothesize:

- HYPOTHESIS 2 (H2). Privacy self-efficacy affects privacy concerns.
- HYPOTHESIS 2a (H2a). Privacy self-efficacy is negatively associated with privacy concerns.
- HYPOTHESIS 2b (H2b). Privacy self-efficacy is negatively associated with privacy risk which, in turn, affects privacy concerns.
- HYPOTHESIS 3 (H3). Response efficacy affects privacy concerns.

- HYPOTHESIS 3a (H3a). Response efficacy is negatively associated with privacy concerns.
- HYPOTHESIS 3b (H3b). Response efficacy is negatively associated with privacy risk which, in turn, affects privacy concerns.
- HYPOTHESIS 3c (H3c). Response efficacy is positively associated with privacy self-efficacy which, in turn, affects privacy concerns.

3.4.3 Fairness Appraisal

Anxiety or concerns about transaction arise due to the potential of opportunistic behavior of an entity (Williamson, 1988). People are willing to provide their personal information to an online vendor in return for economic or social benefits; such willingness however diminishes when a vendor's information collection process is perceived as unfair (Culnan & Armstrong, 1999). Fairness of information collection process mitigates customers' privacy concerns by alleviating the fear of an online vendor's such opportunistic behavior (Asworth & Free, 2006; Pavlou et al., 2007; Xu et al., 2012). Culnan and Armstrong (1999) argue that information collection process is perceived as fair when an online vendor offers relevant information about what information is collected and used and allows information providers to have direct controls over personal information. Similarly, Ashworth and Free (2006) highlight the norm of openness and permission in collecting individual's personal information as a foundation of fairness in information exchange. The norm of openness stipulates that an information collector should notify customers of the specific information to be collected as well as how it will be used. The norm of permission requires an information collector to seek an explicit consent from customers before collecting their

information. In this vein, privacy concerns arise when an online vendor fails to clearly notify customers about the information it collects and uses (i.e., notice and norm of openness), when customers lack controls of the vendor's subsequent use of the collected information (i.e., control and norm of permission), or both. Thus, we postulate negative relationship between fairness appraisal and privacy concerns: customers are more likely to concerns of their privacy as they perceive a vendor's information practices associated with notice and consent as unfair.

Agency theory helps explain how perceived fairness indirectly influences privacy concerns through privacy risk. The locus of this theory is determining efficient ways to govern the principal-agent relationship (Jensen & Meckling, 1972). According to the theory, self-interest is a key motivation for guiding acts of both principals and agents in an exchange relationship. Problems arise when lacking proper monitoring of an agent's acts or enforcing compliance tempts the agent to act opportunistically for its own profits even at the expense of the principal's interests (Eisenhardt, 1989). A fear of opportunistic behaviors by an agent increases perceived risk of engaging in an exchange relationship with the agent (Pavlou et al., 2007). In this vein, violations of fairness in a vender's collecting personal information lead customers to perceive the likelihood that an online vendor pursues its profits at the expense of customers' privacy. In contrast, established procedural fairness lessens the risk of a vendor's opportunistic behaviors and alleviates privacy concerns associated with providing personal information to the vendor. Further, consent may affect notice because, in many practices, online vendors offer information regarding data collection and use for obtaining consent from information providers. Therefore, when customers believe that online vendors collect information after getting agreement, they would expect that online vendors provide detailed information about data

collection.

- HYPOTHESIS 4 (H4). Notice practice affects privacy concerns.
- HYPOTHESIS 4a (H4a). Notice is negatively associated with privacy concerns.
- HYPOTHESIS 4b (H4b). Notice is negatively associated with privacy risk which, in turn, affects privacy concerns.
- HYPOTHESIS 5 (H5). Consent practice affects privacy concerns.
- HYPOTHESIS 5a (H5a). Consent is negatively associated with privacy concerns.
- HYPOTHESIS 5b (H5b). Consent is negatively associated with privacy risk which, in turn, affects privacy concerns.
- HYPOTHESIS 5c (H5c). Consent is positively associated with notice which, in turn, affects privacy concerns.

3.5 Study Design

To test the hypotheses, we performed a survey study that involved more than 300 and 200 undergraduate students who enrolled in a major university in the U.S. and S.K, respectively. We administered the survey at the beginning of regular class meetings. We used a script to clearly explain the study's objectives and our intended data analyses to participants, and addressed any concerns related to privacy.

3.5.1 Participants

We targeted business students enrolled at each university. Our participant selection criteria included prior experiences of providing personal information to online vendors and made purchases online. Several faculty members teaching business classes at each university

assisted with participant recruitment. All participation was voluntary and had no impacts on class performance and grade.

3.5.2 Measurements

We measured the investigated constructs with question items adapted from previously validated scales, with minor word changes that better fit our participants and context. In Table 3.3, we provide the definition of each investigated construct, together with their respective source(s). Following Smith et al. (1996), we modeled online privacy concerns as a second-order construct consisted of four subdimensions: collection, secondary use, unauthorized access, and error. Privacy risk was also measured as a second-order construct consisted of vulnerability and severity. We measured vulnerability with items from Cox et al. (2004) and Eppright et al. (1994); the severity items were adapted from Cox et al. (2004) and Melamed et al. (1996). Response efficacy was measured with items from Son and Kim (2008); the privacy self-efficacy items were from Herath and Rao (2009) and Youn (2009). Notice and consent were measured with items from Malhotra et al. (2004); and items for subdimensions of online privacy concerns were from Malhotra et al. (2004) and Smith et al. (1996). All question items employed a seven-point Likert scale, with 1 being “strongly disagree” and 7 being “strongly agree.” The detailed measurement items are presented in Appendix D. We also consider age, gender, and experience of privacy invasion as control variables, consistent with previous studies (Malhotra et al., 2004; Smith et al., 1996).

Table 3.3 Definition of Each Construct and Sources of Measurement Items

Constructs		Definition and Source(s)	Sources of Measurement Items
Threat appraisal	Vulnerability	An individual's perceived conditional probability that invasion to his or her privacy will occur (Rogers, 1983).	Eppright et al. (1994), Cox et al. (2004)
	Severity	An individual's perceived magnitude of noxiousness of privacy invasion (Rogers, 1983).	Cox et al. (2004), Melamed et al. (1996)
Coping appraisal	Response efficacy	An individual's perceived availability and effectiveness of a coping strategy for privacy invasion (Rogers, 1983).	Son and Kim (2008)
	Privacy self-efficacy	An individual's confidence in his or her ability to protect privacy (Youn, 2009).	Herath and Rao (2009), Youn (2009)
Fairness appraisal	Notice	An individual's belief that firms inform the collection and use of personal information (Malhotra et al., 2004).	Malhotra et al. (2004)
	Consent	An individual's belief that firms don't collect, process, and use his or her personal information without permission or consent (Malhotra et al., 2004).	
Online privacy concerns	Collection	The degree to which an individual is concerned about the extensive amount of personal information that firms can collect online and store in their database (Smith et al., 1996).	Malhotra et al. (2004), Smith et al. (1996)
	Secondary use	The degree to which a person is concerned about that the firm's collecting personal information for one purpose and then uses the information for another (Smith et al., 1996).	
	Unauthorized access	The degree to which an individual is concerned about his or her personal information readily available to people and firms not authorized to access or use the information (Smith et al., 1996).	
	Error	The degree to which an individual is concerned about online firms' inadequate protections against deliberate or accidental errors in the personal data stored in databases (Smith et al., 1996).	

3.5.3 Translation

We conducted the survey in English and Korean. Because the original items were available in English, we employed a translation and back-translation method (Brislin et al. 1973). A professional translator translated all the items in English into Korean. To ensure consistent semantics, two experienced researchers, fluent in both English and Korean and not involved in this study, reviewed the translated items individually. Their reviews indicated satisfactory and consistent semantics in the translation. The question items in Korean were then translated back to English by another professional translator, and individually reviewed by the same researchers who again indicated satisfactory semantic preservation and consistency. Our survey also included a concise description of our objective and provided explicit definitions of important factors to properly anchor their responses.

3.6 Data and Analysis Results

We approached 402 U.S. students for their voluntary participation; among them, 307 agreed to take part. Six participants only partially completed the survey and were removed from our sample, which has 301 participants and shows a 74.9% effective response rate. On the other hand, 517 S.K. students were contacted, and 268 agreed to participate, of whom 18 responses were excluded due to partial completion. The effective response rate is 48.4%. We provide descriptive statistics in Table 3.4. For the U.S. (S.K.) participants, approximately 66.0% (54.9%) of the participants were females, 65% (74.3%) were younger than 25 years in age, 57% (74%) spent less than $100 for online shopping, and 71% (69.3%) were using social network media less than 2 hours a day. As a group, the respondents spent 4.3 (2.8) hours on the Internet on average each day.

Table 3.4 Descriptive Statistics

Measure	Value	U.S.	S.K.
Gender	Male	102 (34.0%)	110 (45.1%)
	Female	198 (66.0%)	134 (54.9%)
Age	< 20	10 (3.4%)	1 (0.4%)
	20-24	182 (61.5%)	184 (73.9%)
	25-29	67 (22.6%)	63 (25.3%)
	> 30	37 (12.5%)	1 (0.4%)
Years in university	1-2 year	48 (16.1%)	105 (43.0%)
	3-4 year	197 (66.1%)	139 (57.0%)
	5-6 year	41 (13.8%)	0 (0.0%)
	> 7 year	12 (4.0%)	0 (0.0%)
Average amount spent for shopping online in the past three months	Less than $50	85 (28.3%)	104 (43.7%)
	$51 ~ $ 100	86 (28.7%)	72 (30.3%)
	$101 ~$150	39 (13.0%)	32 (13.4%)
	$151~$200	26 (8.7%)	19 (8.0%)
	$201~$300	26 (8.7%)	11 (4.6%)
	> $ 300	38 (12.7%)	0 (0.0%)
Time spent for the Internet		4.3 hours / a day	2.8 hours / a day

3.6.1 Measurement Testing Results

We assessed our measurements in terms of construct reliability, and convergent and discriminant validity. To establish indicator reliability, we first removed items with a loading value lower than .6 (Gefen & Straub, 2005). Then we examined construct reliability on the basis of composite reliability, using the common threshold of .7 (Bagozzi & Yi, 1988). As we summarize in Table 3.5, each construct indicated a composite reliability greater than the threshold, suggesting appropriate construct reliability.

Table 3.5 Analysis of Construct Reliability

	Mean (Standard deviation)		AVE		Composite Reliability	
	U.S.	S.K.	U.S.	S.K.	U.S.	S.K.
Collection	2.95 (0.04)	2.84 (0.04)	0.708	0.701	0.906	0.875
Secondary use	2.38 (0.03)	2.51 (0.03)	0.772	0.906	0.910	0.951
Unauthorized access	2.35 (0.02)	2.63 (0.02)	0.653	0.833	0.785	0.909
Error	2.51 (0.03)	2.91 (0.04)	0.536	0.828	0.774	0.951
Vulnerability	2.61 (0.03)	2.89 (0.02)	0.729	0.728	0.890	0.914
Severity	3.21 (0.04)	3.41 (0.03)	0.591	0.554	0.850	0.859
Privacy self-efficacy	2.84 (0.04)	2.55 (0.03)	0.578	0.643	0.871	0.900
Response efficacy	3.13 (0.03)	2.99 (0.03)	0.786	0.756	0.880	0.860
Notice	1.91 (0.03)	1.85 (0.03)	0.735	0.683	0.893	0.865
Consent	2.09 (0.03)	2.23 (0.04)	0.636	0.722	0.838	0.834

We evaluated convergent validity by examining average variance extracted (AVE), using the common threshold of .5 (Götz et al., 2010). We assessed discriminant validity in terms of the square roots of AVEs and the pair-wise correlations between constructs (Fornell & Larcker, 1981). In general, discriminant validity is established when a construct's square root of AVE is significantly greater than the correlation between a pair of constructs. As we show in Tables 3.5 and 3.6, the AVE value of each construct exceeded .5 and was noticeably greater than the correlations between any pair of constructs. Together, our analysis results suggested the measurements possessing adequate convergent and discriminant validity.

We also assessed multicollinearity of measurement items by examining variance inflation factor (VIF), using the threshold of 3.3 (Cenfetelli & Bassellier, 2009) which is recommended in the context of variance-based structural equation model (SEM) (Kock & Lynn, 2012).

Table 3.6 Square Roots of AVE and Correlations between Constructs

U.S.				
	Consent	Notice	Response efficacy	Privacy self-efficacy
Consent	**0.798**			
Notice	0.724	**0.857**		
Response efficacy	0.298	0.332	**0.881**	
Privacy self-efficacy	0.227	0.238	0.246	**0.799**
S.K.				
	Consent	Notice	Response efficacy	Privacy self-efficacy
Consent	**0.700**			
Notice	0.545	**0.827**		
Response efficacy	0.244	0.312	**0.731**	
Self-efficacy	0.110	0.109	0.229	**0.836**

Note: The square root value AVE of privacy risk and privacy concerns and their correlations with other constructs are not presented because they are conceptualized as second-order construct.

As we show in Table 3.7, VIF values are under the threshold and multicollinearity does not appear as serious problem in our data. Overall our data showed appropriate reliability, convergent validity, discriminant validity, and multicollinearity.

3.6.2 Model Fit of Research Model

We assessed model fit based on Chi-square/*df,* GFI, AGFI, CFI, RMSEA, and SRMR, consistent with Chau and Hu (2001), Hu and Bentler (1988), and Ullman (2006). The test results are presented in Table 3.8. Although RMSEA of S.K. data were slightly over the threshold, the research models seemed to show overall adequate fit to the data.

Table 3.7. Collinearity Statistics (VIF)

Construct		Privacy risk	Privacy concerns
Privacy self-efficacy	U.S.	1.102	1.175
	S.K.	1.059	1.264
Response-efficacy	U.S.	1.169	1.183
	S.K.	1.165	1.228
Notice	U.S.	2.180	2.367
	S.K.	1.496	1.736
Consent	U.S.	2.215	2.159
	S.K.	1.438	1.526

Table 3.8 Overall Model Fit

Fit index	Recommended value	U.S.	S.K.	Source
Chi-square/*df*	≤ 3.0	2.181	2.746	Chau and Hu (2001)
GFI	≥ 9.0	0.917	0.947	
AGFI	≥ 8.0	0.874	0.886	
CFI	≥ 9.0	0.923	0.958	
RMSEA	≤ 0.08	0.079	0.093	Ulman (2006)
SRMR	≤ 0.08	0.042	0.068	Hu and Bentler (1998)

3.6.3 Hypothesis Test

We used partial least square (PLS) to test the proposed model and summarize our hypothesis test results in Table 3.9. As shown, the model accounted for 38.4% (U.S.) and 54.4% (S.K.) of the variances in online privacy concerns. According to our results, privacy risk was positively associated with privacy concerns in both countries, in support of H1. Privacy self-efficacy was negatively associated with privacy risk, but its direct effect on privacy concerns was significant in S.K. data only; thus, our data supported H2b but partially

Table 3.9 Model Test Results

Exogenous construct	Endogenous construct	U.S.	S.K.	Hypothesis	Result
Privacy risk	Privacy concerns	0.478***	0.345***	H1	Supported
Privacy self-efficacy	Privacy concerns	0.032	-0.235**	H2(a)	Partially supported (S.K.)
	Privacy risk	-0.133*	-0.333***	H2(b)	Supported
Response-efficacy	Privacy concerns	0.061	-0.047	H3(a)	Not supported
	Privacy risk	-0.050	0.293***	H3(b)	Not supported
	Privacy self-efficacy	0.250***	0.260***	H3(c)	Supported
Notice	Privacy concerns	-0.076	-0.297***	H4(a)	Partially supported (S.K.)
	Privacy risk	-0.197*	-0.218*	H4(b)	Supported
Consent	Privacy concerns	-0.162*	0.044	5(a)	Partially supported (US)
	Privacy risk	-0.038	-0.145+	5(b)	Partially supported (S.K.)
	Notice	0.723***	0.567***	5(c)	Supported
Controls					
Controls	Age	0.041	0.047		
	Gender	-0.044	-0.006		
	Experience	-0.055	0.207***		
R^2	Privacy self-efficacy	0.062	0.068		
	Notice	0.523	0.322		
	Privacy risk	0.096	0.246		
	Privacy concerns	0.326	0.480		

+p<0.1, *p<0.05, **p<0.01, ***p<0.001

support H2a. Our data did not support hypothesized association of response efficacy and privacy concerns as well as that between response efficacy and privacy risk. That is, our data did not support H3a and H3b. The effect of notice on privacy concerns was statistically significant in S.K. data, partially supporting H4a. However, notice was negatively associated with privacy risk, in support of H4b. Consent had a significant negative association with privacy concerns in U.S. data, but its relationship with privacy risk was significant in S.K. data; thus, our data partially supported H5a and H5b.

3.6.4 Model Comparison

We compared our proposed research model with direct effect model using model fit statistics and chi-square difference test. As shown in Table 3.10, the direct effect model didn't fit to the data, suggesting the discrepancy between observed values and the expected values of direct effect model. Next, we compared the two models by examining chi-square difference which indicates whether the fuller model that includes extra paths helps more to explain the data (Ullman, 2006). As shown in Table 3.11, The test results showed that the research model considering indirect paths provides a better explanation of the data.

3.6.5 Cross-Country Comparison Results

We compared our results from the respective datasets at both overall individual construct and path levels. Because of our intent to examine privacy concerns, we focused on the direct effects of cognitive appraisals. The comparisons at the construct and path-coefficient level may shed light on main and moderating effect of culture on privacy concerns, respectively. Thus, the comparisons at the both levels offer a better understanding of the roles of culture.

Table 3.10 Analysis Results of the Direct Effect Model

Exogenous variable	Endogenous variable	Path coefficient		Model Fit	
		U.S.	S.K.	U.S.	S.K.
Privacy risk	Privacy concerns	0.488***	0.262***	Chi-square/*df*: 4.573 GFI: 0.808 AGFI: 0.639 CFI: 0.916 RMSEA: 0.109 SRMR: 0.152	Chi-square/*df*: 4.028 GFI: 0.779 AGFI: 0.721 CFI: 0.793 RMSEA: 0.110 SRMR: 0.189
Privacy self-efficacy		0.036	-0.186***		
Response-efficacy		0.081	-0.002		
Notice		-0.105	-0.434***		
Consent		-0.254***	0.007		
Age		0.004	0.015		
Gender		-0.005	-0.004		
Experience		-0.004	0.150***		

Table 3.11 Chi-square Difference Test

Model		Chi-square	*df*	Difference (*df*)
U.S.	Direct effect model	759.11	166	455.94 (27)***
	Research model	303.17	139	
S.K.	Direct effect model	668.71	166	259.55 (17)***
	Research model	409.16	149	

***p <0.001

3.6.4.1 Comparison at Construct Level

We performed a *t*-test to examine whether there existed significant differences in our selected determinants of privacy concerns between the datasets. As we show in Table 3.12, all the antecedents of privacy concerns significantly differed between the countries at the .01 level, with the exception of notice. The results suggest that the S.K. participants perceived more privacy risk than did their U.S. counterparts. In addition, the S.K. participants demonstrated more assurance that online vendors obtain permission before collecting and using personal

Table 3.12 Comparison of Antecedents of Privacy Concerns between the Two Countries

Constructs		U.S. (mean)	S.K. (mean)	t-value
Threat appraisal	Vulnerability	2.61	2.89	-7.089**
	Severity	3.21	3.41	-4.036**
Coping appraisal	Response efficacy	2.84	2.55	3.178**
	Privacy self-efficacy	3.13	2.99	5.942**
Fairness appraisal	Notice	1.91	1.85	1.012
	Consent	2.09	2.23	-3.022**

*p<0.05, **p<0.01

information. In contrast, the U.S. participants showed more confidence in their ability to manage privacy risk and availability of effective response toward the risk.

3.6.4.2 Comparison at the Coefficient Level

We compared the structural path coefficients of the key determinants of privacy concerns. This comparison sheds light on the moderating role of culture on the relationship between privacy concerns and their determinants. Consistent with Steelman et al. (2014), our comparative results were obtained from a two-tailed *t*-test below.

$$t = \frac{Path_{sample\_1} - Path_{sample\_2}}{\left[\sqrt{\frac{(m-1)^2}{(m+n-2)} \times S.E._{sample_1}^2 + \frac{(m-1)^2}{(m+n-2)} \times S.E._{sample_2}^2}\right] \times \left[\sqrt{\frac{1}{m} + \frac{1}{n}}\right]}$$

As shown in Table 3.13, the path coefficients derived from the two datasets significantly differed, with the exception of response efficacy. In specific, while the effects of privacy risk and consent were more prominent with the U.S. participants, the effects of self-efficacy, notice, and affect were greater among the Korean participants than the U.S. participants. However, there was no significant difference in the effect of response-efficacy.

Table 3.13 Comparisons of Coefficient of Determinants

Construct	Path coefficient		t-value
	U.S.	S.K.	
Privacy risk → Privacy concerns	0.478	0.345	23.332***
Privacy self-efficacy → Privacy concerns	0.032	-0.235	46.973***
Response efficacy → Privacy concerns	0.061	-0.047	0.000a)
Notice → Privacy concerns	-0.076	-0.297	32.423***
Consent → Privacy concerns	-0.162	0.044	-29.040***

Note: although the path coefficients of response-efficacy between the two countries were significantly different, we set the t-value as 0 because they were insignificant in both datasets.
*p<0.05, **p<0.01, ***p<0.001

3.7 Discussion

3.7.1 Key Determinants of Privacy Concerns

This study identifies key determinants of privacy concerns through a theoretical lens and examines their direct and indirect effects. On the basis of the findings of the U.S. dataset, we provide several implications. First, our results highlight the necessity of scrutinizing the indirect effects of key determinants of privacy concerns for a better understanding of the process underlying the formation of privacy concerns in e-commerce. While previous studies exclusively focus on direct effects of examined antecedents of privacy concerns, indirect effects of or interactions among them have received little attention. For example, despite possible relationship between personality and perception of risk (Bouyer et al., 2001), the indirect effects of personality via privacy risk have not been scrutinized. In addition, the consideration of indirect effects helps to figure out the insignificant effect of an important antecedent such as self-efficacy (e.g., Yao et al., 2007;

Youn, 2009). In this light, our findings suggest the reconsideration of exclusive focus on direct effects in examining privacy concerns' determinants to offer a better depiction of the process underlying the formation of privacy concerns.

Second, privacy self-efficacy indirectly influenced privacy concerns through privacy risk. This result suggests that customers refer to their ability to protect privacy in assessing the risk of providing their personal information to an online vendor. That is, a person's perceived capability of protecting privacy in information exchange is essential when assessing whether he or she could prevent the occurrence of negative consequences of information disclosure. However, the insignificant direct effect of privacy self-efficacy on privacy concerns may demonstrate the doubt in customers' minds about the effectiveness of their capability in controlling opportunistic behavior of an online vendor. For example, while customers could decrease privacy risk by assessing the likelihood that an online vendor behaves opportunistically using their knowledge or skills, they couldn't monitor an online vendor's information management or prevent it from sharing personal information with a third-party without permission. Our results also suggest an insignificant effect of response efficacy, different from our expectation. A plausible explanation is that an effective privacy protection is a source of privacy self-efficacy. That is, the confidence in ability to protect privacy may be derived from the available effective protection to cope with privacy risk. The significant and positive relationship between response-efficacy and privacy self-efficacy may support this plausible explanation (β=0.250, p=0.000). Alternatively, the insignificant effect of response efficacy on privacy concerns may reveal the uncertainty of the effectiveness of an available privacy protection. Customers seldom have a proper way of accurately evaluating the effectiveness of a privacy protection, largely

due to the lack of knowledge of how data are collected, processed, analyzed, and used by online vendors (Baek, 2014). Accordingly, the illiteracy of data collection and use leads customers to be unsure about the effectiveness of a privacy protection: whether a privacy protection can protect privacy or a protection is available in time of need. Instead, those protections may be referred when assessing ability to protect privacy.

Last but not least, our results indicate that fair practice of information collection influences privacy concerns in different manners. While consent practice directly mitigates privacy concerns, notice practice alleviates the concerns by offering information relevant to data collection and use, which decreases privacy risk. Consent practice has a direct effect on privacy concerns because it allows people to exert controls over their provided personal information; after all, they have total freedom to either accept or reject an information exchange (Alge, 2001). Thus, whether customers exercise controls over their providing personal information to a vendor significantly matters to privacy concerns, a manifestation of their rights to accept or reject an exchange with the vendor (Malhora et al., 2004). In contrast, notice practice indirectly decreases privacy concerns. Notice practice alleviates information asymmetry between customers and online vendors and leads customers to have a feeling of being respected; as a result, online vendors seem trustworthy, and the risk of engaging in an information exchange is perceived to be low (Pavlou et al., 2007). However, the effect of notice practice on privacy concerns was insignificant. A plausible explanation is that customers may sense that they are limited in controlling opportunistic behavior of an online vendor if relevant information is offered.

3.7.2 The Differentials between the Two Countries

According to Hofstede's culture model (Hofstede, 1983), the U.S. and S.K. significantly differ in the cultural dimensions of individualistic-collectivistic, power distance dimensions, and uncertainty avoidance. These differentials provide plausible explanations for the observed comparative results. In specific, the comparison at construct level reveals direct effects of culture on privacy concerns' determinants, whereas the comparison at path coefficient level sheds light on moderating effects of culture on the relation between the determinants and privacy concerns in e-commerce.

3.7.2.1 Construct Level

For privacy risk, S.K. participants perceived higher vulnerability and severity than did their U.S. counterparts. In general, people in an individualistic culture, such as that of the U.S., have a tendency of viewing risks as opportunities and have more acceptance or tolerance of risk than those in a collectivistic culture (Lowary et al., 2011; Palmer, 1996). In addition, due to a greater faith in their ability or skills, people in an individualistic culture usually consider that many behaviors are under their direct control and perceive them as less risky (Palmer, 1996).

Regarding coping appraisals, the U.S. participants perceived more assurance of their capability to reduce privacy risks and greater efficacy for privacy protection. The higher assurance of capability of protecting privacy may stem from individualistic culture that emphasizes individual achievement and competitiveness over collective social relationships and thus puts a higher value on individuals' ability to act and control (Schoorman et al., 2007). On the other hand, people in a collectivistic culture typically emphasize collective good and

interpersonal cooperation rather than individual achievement or competitiveness (Hofstede, 1983). In this light, people in an individualistic culture may have more opportunities to develop their abilities for increased competitiveness or observe the success of others, thus showing a higher self-efficacy than those in a collectivistic culture (Bandura, 1997). Furthermore, people in a culture of great power distance tend to accept unequal distributions of power and readily conform to those in higher positions to make unilateral decisions on their behalf. Thus, people in cultures of great power distance are less willing to proactively take part in goal settings or dispute established performance norms, which subsequently leads to lower self-efficacy (Latham et al., 1994; Sue-chan & Ong, 2002).

For fairness appraisal, our result showed that S.K. participants seemed to believe that online vendors should obtain explicit consent for collecting and using personal information, more so than their U.S. counterparts. This finding is different from our expectation because people in an individualistic culture prefer to exercise control over the procedure of data collection through formal legal procedure. High uncertainty avoidance may offer a plausible explanation of this unexpected finding. Due to the tendency of avoiding a risk related to data collection and use, online vendors in S.K. seem to try to go through a formal procedure of data collection including consent, which helps them to feel immune from obligation to compensate possible privacy loss.

3.7.2.2 Path Coefficient Level

The effect of privacy risk on privacy concerns was greater among the U.S. participants than the S.K. participants. Cushion hypothesis (Weber & Hsee, 1998) offers a plausible explanation, suggesting that people in a collectivistic culture, such as S.K., expect help from

family and other in-group members when they encounter a major difficulty or loss. In contrast, people in an individualistic culture, such as the U.S., expect to personally bear the negative consequences of their decision. Accordingly, given the same level of risk, the effect of the risk would be greater to people in an individualistic culture.

For coping appraisal, the effects of self-efficacy were more prominent with S.K. participants. In general, effective privacy protections are offered by government (e.g., Fair Information Practices by the Federal Trade Commission) or online vendors (e.g., privacy policy or statement). However, individuals in high power distance culture may also put lower faith in the protections provided for government or organizations because of the likelihood of opportunistic behavior of authorities (Fukuyama, 1995), That is, the asymmetric distribution of resources tends to tempt authorities to take opportunistic behavior to maximize their utility, and the presence of opportunistic behavior may decrease trust toward authorities (Fukuyama, 1995). Accordingly, the relatively lower trust in the authorities commonly observed in cultures of high power distance leads people to suspect the efficacy of the protection measures by authorities. Thus, the absence of faith in effective protections by authorities such as government or online vendors leads customers to more focus on individuals' ability and accordingly rely more on their own ability to manage an uncertain or risky situation.

With respect to fairness appraisal, the effect of notice was greater with S.K. than with the U.S. participants. Procedural fairness has two distinct aspects: structural and social aspect (Tata, 2005). While the former deals with formal policies and procedures, the latter focuses on interpersonal treatment. Structural aspect suggests *voice* as an important procedural fairness principle (Thibaut & Walker, 1975). People in an individualistic culture tend to evaluate procedural fairness based on the degree to which they could exercise control over personal

information disclosure, which is closely connected to structural aspect of procedural fairness (Leung & Tong, 2004). In contrast, a collectivistic culture appeals more to the value of harmony, cooperation, supporting others' faces which are more likely to be associated with the social aspect of procedural fairness (Tata, 2005). In dispute, collectivists tend to show strong preference for mediation and bargaining rather than adversary procedures because of their desire for maintaining a harmonious relationship after the dispute is settled (i.e., interpersonal harmony) (Leung, 1987). Overall, individualists perceive a decision or process as fairer when they exert control over the decision or process, whereas collectivists more focus on the provision of relevant information and respectful treatment in assessing procedural fairness. As a result, people in a collectivistic culture such as S.K. tend to put more weight on notice practice in shaping privacy concerns.

CHAPTER 4

THE INCONSISTENT EFFECT OF PRIVACY CONCERNS: ATTITUDINAL AMBIVALENCE APPROACH

4.1 Introduction

In the hypercompetitive online marketspace, firms seek competitive advantages through product recommendations and personalized services to customers (Rust & Huang, 2014; Zhou, 2013). To be effective, these practices require collection and analysis of a vast amount of individuals' information, demographic and behavioral, which inevitably create concerns about potential invasion to and loss of their information privacy (Malhotra et al., 2004; Smith et al., 2011; Xu et al., 2011). For example, an online vendor could behave opportunistically and share its collected personal information with other parties, without explicit notice to or consent from people who provide the information (Pavlou et al., 2007; Son & Kim, 2008).

Online privacy has earned a lot of attention from information systems (IS) researchers and practitioners because of its explicit and implicit effects on behavior online (Bélanger & Crossler, 2011; Smith et al., 2011). Previous studies often use privacy concerns as a proxy of privacy and indirectly examine the effect of privacy by analyzing the relation between privacy concerns and behaviors (Awad & Krishnan, 2006; Brown & Muchira, 2004; Dinev & Hart, 2006; Li et al., 2011; Smit et al., 2014; Xu et al. 2009). In examining the

effect of privacy concerns, some previous studies conceptualize privacy concerns as attitude or belief and examine their direct effect on online behaviors (e.g., Dinev & Hart, 2006; Pavlou et al., 2007; Son & Kim, 2008). However, accumulated results seem to suggest that direct effect of privacy concerns is inconclusive. While some studies observe a significant effect of privacy concerns, others report negligible effect of privacy concerns (Bélanger & Crossler, 2011; Smith et al., 2011). For example, while Dinev and Hart (2006) found a significant, negative effect of privacy concerns on people's voluntary information disclosure to an online vendor, Hui et al. (2007) observed an insignificant relationship in a similar online setting. This inconsistency between privacy concerns and behavior have drawn the attention of IS researchers (Smith et al., 2011). Several alternative explanations of the discrepancy have been proposed, largely from the perspectives of behavioral economics or situational cues (Kehr et al., 2014; Wilson & Valacich, 2012). While the behavioral economics approach highlights biased evaluations of benefits and risk of information disclosure by incomplete information or bounded rationality as a source of the discrepancy (Acquisti, 2004; Acquisti & Grossklags, 2006; Flender & Müller, 2012), the situational cues approach attributes the inconsistency to the overriding effects of situational factors such as positive mood (Kehr et al., 2014; Li et al., 2011). However, empirical findings incongruent with the proposed explanations seem to call for an alternative explanation. For example, different from behavioral economics approach, people actually disclose their personal information even when there are no rewards or benefits (Norberg et al., 2007). Further, the proposed explanations are limited in explaining the condition in which the direct effect of privacy concerns becomes negligible.

Some other previous studies alternatively conceptualize privacy concerns as individual characteristics or value and suggest an indirect effect of privacy concerns via attitude or belief such as risk or trust (Hong & Thong, 2013; Lowry et al., 2011; Malhotra et al., 2004). However,

the results of privacy concerns' indirect effect seem mixed as well: fully mediated, partially mediated, or not mediated. While some studies observed that the effect of privacy concerns is fully mediated by an attitude or cognitive belief such as privacy attitude (e.g., Dienlin & Trepte, 2015; Van Slyke et al., 2006), others reported a partially mediated effect of privacy concerns (e.g., Kehr et al., 2015; Li et al., 2011). Some studies found no indirect effect of privacy concerns (Bansal et al., 2016; Lian & Lin, 2008; Xu & Gupta, 2009). Further, the inconsistent indirect effect of privacy concerns may not be attributed to different mediating factors. Previous studies demonstrate mixed results when mediating factors are the same (e.g., Bansal et al., 2016; Li et al., 2011; Van Slyke et al., 2006).[5] However, the inconsistency of the indirect effect of privacy concerns seems overlooked and remains unexplained.

In this light, we attempt to offer an alternative explanation of the inconsistent direct and indirect effects of privacy concerns by highlighting the roles of moderating factors. Specifically, we examine the effect of moderating factors through the lens of attitudinal ambivalence. Attitudinal ambivalence indicates a state in which an individual holds equivalently strong positive or negative evaluation toward a focal object at the same time (Thompson et al., 1995). Attitudinal ambivalence weakens the strength of the relation between attitude and behavior particularly by preventing accessibility to memory, averting attitude certainty, or hampering consistency between cognitive beliefs (Bargh et al., 1992; Maio et al., 1996). In the presence of attitudinal ambivalence, the effect of attitude becomes unstable and weak because equivalent strong opposite evaluations restrict the access to the attitude, and salience of evaluations fluctuates. As a result, connecting a focal object with

[5] In some cases, previous studies examine indirect effect of privacy concerns only such that it is unknown whether the effect of privacy concerns is fully or partially mediated (e.g., Hong & Thong, 2013; Malhotra et al., 2004).

an evaluation is challenging and predictability of attitude becomes poor (Sparks et al., 2001; Fazio et al., 1986).

Drawing on attitudinal ambivalence, we developed research models to explain both inconsistent direct and indirect effect of privacy concerns: *direct ambivalence* and *indirect ambivalence model*. In our direct ambivalence model, privacy concerns are conceptualized as attitude, and the effect of privacy concerns is moderated by the ambivalence of positive and negative cognitive beliefs which constitute privacy concerns. On the other hand, the indirect ambivalence model conceptualizes privacy concerns as individual characteristics or value and suggests indirect effect of privacy concerns through favorability of information disclosure. In the model, the effect of favorability toward information disclosure is moderated by the ambivalence of positive and negative cognitive beliefs that compose favorability of information disclosure.

We further distinguish between positive and negative attitude and specify cognitive beliefs that exclusively engage in attitudinal ambivalence for each attitude. Positive and negative attitudes are shaped by different cognitive beliefs because they are claimed to be different in their sources and consequences (Cenfetelli, 2004). We suggest that negative attitude (i.e., privacy concerns) is mainly constituted by cognitive beliefs associated with threat, whereas positive attitude (i.e., favorability) is greatly affected by cognitive beliefs associated with utility. Specifically, privacy concerns (i.e., negative attitude) are affected by positive cognitive belief which decreases risk and negative cognitive belief that increases threat. In contrast, favorability of information disclosure (i.e., positive attitude) is shaped by positive cognitive belief that augments utility and negative cognitive belief that attenuates utility.

Our study differs from previous research in several ways. First, different from most previous studies that commonly examine factors that mitigate the effect of privacy concerns

for explaining the discrepancy between privacy concerns and behavior, we focus on the roles of moderating factors through the lens of attitudinal ambivalence. Scrutinizing moderating factors is believed essential for explaining the condition in which privacy concerns can't explain behavior in a reliable manner and thus reconciling the mixed results of privacy concerns' effect. Second, we examine moderating effect of the ambivalence of positive and negative cognitive beliefs for both cases of direct and indirect effect of privacy concerns, thereby offering a fuller explanation of the discrepancy. Third, different from previous studies that capture positive and negative aspects of a focal object, we differentiate positive attitude (i.e., privacy concerns) from negative attitude (i.e., favorability of information disclosure) and examine the moderating effect of the ambivalence of different cognitive beliefs for each attitude.

4.2 Literature Review

Several streams of research are relevant to our study, including privacy concerns and their effects, and inconsistency between privacy concerns and disclosure behavior. We review representative studies of each stream to highlight the gaps that motivate our study.

4.2.1 Conceptualization of Privacy Concerns

Privacy concerns are commonly defined as concerns about the loss of privacy or control over personal information (Algae et al., 2006; Brown & Muchira, 2004; Eastlick et al., 2006; Milne & Culnan, 2004). However, the conceptualization of privacy has monikered from individual characteristics, belief, or attitude (Xu et al., 2009). Drawing on theory of reasoned action (TRA, Ajzen, 1991), some studies conceptualize privacy

concerns as individual characteristics or value and hypothesize indirect effect of privacy concerns through a cognitive belief such as trust or attitude (Awad & Krishnan, 2006; Hong & Thong, 2013; Lowry et al., 2011; Malhotra et al., 2004).[6] On the other hand, some other studies conceptualize privacy concerns as attitude or belief and scrutinize their direct effect on behavior (Dinev & Hart, 2006; Pavlou et al., 2007; Son & Kim, 2008). That is, the conceptualization of privacy concerns is closely related to the way privacy concerns influence behavior, i.e., directly or indirectly.

4.2.2 Effects of Privacy Concerns

In Table 4.1, we summarize representative studies that examine the effect of privacy concerns. Previous research has examined the direct and indirect effects of privacy concerns on behaviors largely in e-commerce or social network context (Brown & Muchira, 2004; Malhotra et al., 2004; Phelps et al., 2000; Son & Kim, 2008). However, the effect of privacy concerns on behavior, particularly information disclosure, is mixed and inconclusive. For example, while Hui et al. (2007) observe an insignificant effect of privacy concerns on willingness to disclose personal information in e-commerce, Li et al. (2011) report significant effect of privacy concerns in the similar context. On social network site, Taddicken (2014) reports that privacy concerns can't explain self-disclosure behavior, whereas Utz (2015) observes that privacy concerns effectively explain personal information sharing. Further, Norberg et al. (2007) found that people actually provide their sensitive personal information even for no rewards, despite their concerns about privacy. However, Kehr et al. (2015) report that privacy concerns in fact restrict people's information provision to a mobile apps.

[6] Although cognitive belief and attitude are conceptually different, many researchers often use them interchangeably (Lowry et al., 2011).

Table 4.1 Summary of Previous Research Examining Effects of Online Privacy Concerns

Research	Context	Independent Variable	Mediator(ME)/Moderator (MO)	Dependent Variable	Effect of Privacy Concerns
Acquisti and Grossklags (2005)	General	Privacy concerns		Information disclosure	Not supported
Alge et al. (2006)	Work organization	Privacy concerns (+)	Psychological empowerment (+) (ME)	Discretionary behavior	Supported
Angst and Agarwal (2009)	Healthcare	Argument frame (+) Issue involvement (+) Privacy concerns Intention (-)	Attitude (+) Privacy (+) (MO) Argument frame and attitude (+) Argument frame ×involvement and attitude (+)	Intent to adopt electronic healthcare records (HER)	Supported
Awad and Krishnan (2006)	E-commerce	Privacy concerns (+)	Information transparency (-) (ME)	Personalized service Personalized advertising	Supported
Bansal et al. (2016)	E-commerce Finance Healthcare	Privacy concerns E-commerce: n.s. Finance (-) Health: n.s. Trust Intention to disclosure	Trust (+)	Intention to disclosure	Supported

Table 4.1 Continued

Research	Context	Independent Variable	Mediator(ME)/Moderator (MO)	Dependent Variable	Effect of Privacy Concerns
Berestford et al. (2012)*	E-commerce	Information sensitivity		Purchase of DVD	Not supported
Brown and Muchira (2004)	E-commerce	Privacy concerns Unauthorized use (ns) Invasion (-) Errors (-)		Online purchase behavior	Partially supported
Carrascal et al. (2013)*	Online service	Online service improvement		Personal information disclosure	Not supported
Chellappa and Sin (2005)	E-commerce	Privacy concerns (-) Value for personalization (+) Trust (+)		Likelihood of using personalization services	Supported
Dinev and Hart (2006)	E-commerce	Privacy concerns (-) Internet trust (+)		Personal information disclosure	Supported

Note: * Research indirectly examines the effect of privacy concerns.

Table 4.1 Continued

Research	Context	Independent Variable	Mediator(ME)/Moderator (MO)	Dependent Variable	Effect of Privacy Concerns
Eastlick et al. (2006)	E-commerce	Privacy concerns Trust (-) Intention (-)	Trust (+) (ME)	Trust Purchase intention	Supported
Hui et al. (2007)	E-commerce	Privacy concerns (ns)		Information disclosure	Not supported
Keith et al. (2013)	Mobile app	Privacy concerns (+) Privacy risk (+) Information disclosure (-)	Privacy risk (-) (ME)	Information disclosure	Supported
Kehr et al. (2015)	Mobile app	Privacy concerns Privacy risk (+) Intention (-)	Privacy risk (-) (ME)	Intention to use smartphone app	Supported
Li et al. (2011)	E-commerce	General privacy concerns Privacy risk belief (+) Information disclosure (-)	Privacy protection belief (+) (ME) Privacy risk belief (-) (ME)	Information disclosure	Supported
Lian and Lin (2008)	E-commerce	Privacy concerns Books (-) TV (-) Games (-) Magazines (ns) Computer games (ns)		Attitude toward purchasing books, TV games, magazines, and computer games	Partially supported

Table 4.1 Continued

Research	Context	Independent Variable	Mediator(ME)/Moderator (MO)	Dependent Variable	Effect of Privacy Concerns
Malhotra et al. (2004)	E-commerce	Privacy concerns Trusting belief (-) Risk belief (+) Type of information Trusting belief (-) Risk belief (+)	Trusting belief (+) (ME) Risk belief **(-)** (ME)	Information disclosure	Supported
Milne and Culnan (2004)	E-commerce	Privacy concerns Read notices (+) Trust notices (-) Notice comprehension (+)	Trust of privacy notices (ME)	Read online privacy notices Trust of privacy notices	Not supported
Norberg et al. (2007)	Commerce	Privacy concerns (ns)		Information disclosure	Not supported
Son and Kim (2008)	Privacy concerns (+)			Refusal Removal Negative word-of-mouth Complaining to sellers	Supported
Taddei and Contena (2013)	Social network website	Privacy concerns		Privacy control Self-disclosure	Not supported

Table 4.1 Continued

Research	Context	Independent Variable	Mediator(ME)/Moderator (MO)	Dependent Variable	Effect of Privacy Concerns
Taddicken (2014)	Social network website	Privacy concerns Social relevance (+) Number of application (-) Information disclosure (ns)	Social relevance (+) (ME) Number of social web applications used (-) (ME)	Information disclosure	Not supported
Tufekci (2008)	Social network website	Privacy concerns		Information disclosure	Not supported
Utz (2015)	Social network website	Privacy concerns		Information disclosure (the frequency of	Supported
Van Slyke et al. (2006)	E-commerce	Privacy concerns Perceived risk (+) Trust (-) Willingness to transact (ns)	Perceived risk (-) (ME) Trust (+) (ME)	Willingness to transact	Not supported
Xu and Gupta (2009)	Location based service	Privacy concerns Expectancy: (-) Intention: n.s.	Performance expectancy	Intention to use LBS	Not supported
Zlatolas et al. (2014)	Social network website	Privacy concerns		Information disclosure	Supported

Some previous studies scrutinize the indirect effect of privacy concerns via cognitive beliefs such as psychological empowerment (Alge et al., 2006), privacy risk (Malhotra et al., 2004; Li et al., 2011), information transparency (Awad & Krishnan, 2006), trust (Eastlick et al., 2006; Van Slyke et al., 2006), or attitude (Dienlin & Trepte, 2015; Lowry et al., 2011). However, the results of the indirect effect of privacy concerns are inconclusive as well. For example, while Li et al. (2011) and Eastlick et al. (2006) found significant direct and indirect effects of privacy concerns via privacy risk (i.e., partial mediation), Van Slyke et al. (2006) observed substantial indirect effect of privacy concerns through privacy risk (i.e., full mediation). Dienlin and Trepte (2015) observed the effect of privacy concerns on information disclosure on a social network site was fully mediated by privacy attitude. Further, some studies found insignificant indirect effect of privacy concerns (Bansal et al., 2016; Lian & Lin, 2008; Xu & Gupta, 2009). Overall, the collective results are marked with noticeable differences and variations in the direct and indirect effects of privacy concerns on behaviors, which suggest the need to further scrutinize why the direct and indirect effects of privacy concerns are mixed.

4.2.3 Alternative Explanations of the Inconsistency

While several plausible explanations of the weak relationship between privacy concerns and behavior are proposed, the inconsistent results of indirect effect of privacy concerns seem to remain unexplored.

From the extensive literature review, Barth and de Jong (2017) and Kokolakis (2017) categorize proposed explanations of the discrepancy between the expressed privacy concerns and behavior. Barth and de Jong (2017) organize proposed explanations as (a) privacy calculation, (b) biased assessment of risk, (c) overriding effect of perceived

benefits, (d) biased privacy valuation, and (e) digital illiteracy. On the other hand, Kokolakis (2017) classifies plausible explanations as (a) perceived benefits, (b) contextual factors such as social norms or trust, (c) cognitive biases and heuristics, and (d) bounded rationality and incomplete information.

Both studies commonly identify the benefits of information disclosure and underestimated risk associated with disclosure as important sources of the discrepancy between expressed privacy concerns and behavior. The former highlights the overriding effect of benefit over privacy concerns. Although people concern about their privacy due to possible risk associated with information disclosure, the immediate benefits motivate them to reveal their personal information because people tend to overrate present benefits over future risk (Acquisti & Grossklags, 2005) or perceive benefits as compensation for potential loss of privacy (Sheehan & Hoy, 2000). For example, Jupiter Research study reports that 82% of online shoppers are willing to offer their personal data to an unknown shopping site for the chance of winning $100 (Tedeschi, 2002). Further, individuals are found to willingly give their personal information to receive small rewards such as purchase recommendations and discounts (Spiekermann et al., 2001). Alternatively, revealing personal information is provoked by underestimated risk of the behavior. People tend to underestimate or be unaware of risk associated with information disclosure due to incomplete information, digital illiteracy, or heuristics (Acquisti & Grossklags, 2005; Baek, 2014; Forgas, 2011). The lack of information or illiteracy of how personal information is processed and used by online vendors disturbs the awareness of risk associated with information disclosure and thus leads to underestimation of risk.

Researchers in information systems (IS) often seek a source of the inconsistency

from the effects of situational factors (Hui et al., 2007; Kehr et al., 2015; Li et al., 2011; Wilson & Valacich, 2012). Situational cues approach attributes the neglectable effect of privacy concerns to the overriding effect of situational factors such as positive mood or benefit immediacy over that of general privacy concerns (Wilson & Valacich, 2012; Kehr et al., 2014). The underlying assumption is that situational cues have a greater effect on behavior in a specific context than a general attitude or belief (Li et al., 2011). When situational cues and general privacy concerns are incongruent, behavior is more driven by situational cues. Alternatively, some researchers claim a genuine weak association between general privacy concerns and behavior as a source of the inconsistency (Baek, 2014; Park, 2011). Baek (2014) contends that people's understanding of privacy threat is superficial and dubious such that they easily change by a counter argument or evidence. In this light, some previous studies examine the indirect effect of privacy concerns via attitude based on theory of planned behavior or theory of reasoned action, instead of direct effect (Dienlin & Trepte, 2015; Lowery et al., 2011).

4.2.4 Gap Analysis

Overall, previous studies report mixed results of direct or indirect effect of privacy concerns. Researchers have proposed several alternative explanations of negligible effect of privacy concerns for reconciling the mixed results of privacy concerns' effect. However, we identify some gaps to deserve more attention. First, proposed explanations seem incongruent with some empirical findings. For example, different from behavioral economics approach, which attributes the discrepancy to overestimated benefits and/or underestimated risk, previous studies report mixed results of privacy concerns' effect in a

similar context in which perceived benefits and risk of information disclosure are similar (e.g., Van Slyke et al., 2006; Xu et al., 2011). Especially, Bansal et al. (2016) report significant effect of privacy concerns across different contexts, where information sensitivity and perceived risk are different (e-commerce, fiancne, and healthcare). Incongruent with situational cues approach, Li et al. (2011) and Kehr et al. (2015) found significant effect of privacy concerns even in the presence of situational factors, which question the overriding effect of situational cues over privacy concerns' effect. Further, different from a genuine weak approach, many studies report substantial direct effect of privacy concerns on behaviors (Dinev & Hart, 2006; Li et al.,2011; Xu et al., 2011). These inconsistencies of empirical findings may suggest the necessity for an alternative theory based approach (Dienlin & Trepte, 2015). Second, while previous studies commonly examine factors that weaken the effect of privacy concerns, scant studies focus on factors that moderate the relation between privacy concerns and behavior for explaining the inconsistent effect of privacy concerns. The lack of attention to moderating factors may offer a limited account of the condition in which privacy concerns can't be explained in a reliable manner, which is believed essential for reconciling the mixed results of privacy concerns. Third, while the discrepancy between privacy concerns and behavior has been of primary interest, previous studies seem to overlook the inconsistent indirect effect of privacy concerns. Previous studies report mixed results of indirect effect of privacy concerns in a similar context with same mediating factors such as risk or trust, which suggests that the inconsistency may not stem from a different mediating variable or research context. To fill the gaps, we attempt to explain the inconsistency of privacy concerns' effect through the lens of attitudinal ambivalence, especially with focus on the moderating effect of the ambivalence of positive

and negative cognitive beliefs that constitute attitude.

4.3 Theoretical Foundation

Attitude has been known as a good predictor of behavior (Ajzen, 1991; Ajzen & Fishbein, 1975). In this vein, social psychologists have attempted to elicit behaviors by changing or impacting corresponding attitudes (Glasman & Albarrancín, 2006). However, previous studies often observe considerable variability in the strength of the relationship between attitude and its corresponding behavior (Ajzen, 1991; Glasman & Albarrancín, 2006). That is, some attitudes have firm effect on behavior whereas others have flexible or negligible effect on action, which is coined as attitude-behavior inconsistency (Krosnick et al., 1993; Raden, 1985). The strength of attitude-behavior relation is significantly affected by stability of the relation which indicates the degree to which the formed attitude can resist change (Glassman & Albrracín, 2006). The relation between attitudes and behavior is more likely to be consistent and firm as they are more stable over time.

According to attitudinal ambivalence, individuals can hold equivalently strong positive and negative evaluations toward a focal object simultaneously (Conner et al., 2002). The coexistance of equivalently strong different evaluations of a focal object attenuate the stability of the relation between attitude and behavior (Armitage & Conner, 2000; DeMarree et al., 2014; Luttrell et al., 2016; Maio et al., 1996). For example, Armitage and Conner (2000) observe that attitudes are more predictive of behavior as attitudinal ambivalence decreases. Attitudinal ambivalence weakens the stability and strength of the relation between attitude and behavior by preventing accessibility to memory, averting attitude certainty, or hampering consistency between cognitive beliefs (Bargh et al., 1992;

Maio et al., 1996). In specific, attitudinal ambivalence weakens the effect of attitude by restricting access to attitude, which diminishes certainty of attitude. In the presence of attitudinal ambivalence, the access to attitude is confined because equivalently strong opposite evaluations make it hard to connect attitude to a positive or a negative evaluation (Fazio et al., 1986). The difficulty of associating between an attitude and an evaluation attenuates certainty of the attitude, thereby restricting access to the attitude when a person encounters a situation. Further, under attitudinal ambivalence, salience of cognitive beliefs fluctuates (Sparks et al., 2001). That is, salience of a positive or a negative cognitive belief readily changes such that the shaped attitude from the belief is unstable and can't resist changes.

Drawing on attitudinal ambivalence, we suggest that the effect of privacy concerns would be significant if the ambivalence of positive and negative cognitive beliefs is negligible (i.e., low attitudinal ambivalence). On the other hand, when the ambivalence is apparent (i.e., high attitudinal ambivalence), privacy concerns would have no effect on behavior and couldn't explain or predict behavior in a reliable manner. Overall, attitudinal ambivalence negatively moderates the relation between privacy concerns and information disclosure.

4.4 Model and Hypotheses

4.4.1 Research Model

We develop research models that offer alternative explanations of the inconsistency between privacy concerns and information disclosure: *direct ambivalence* and *indirect ambivalence model*. Drawing on protection motivation theory (PMT) (Rogers, 1983), we first determine important and relevant cognitive beliefs that affect privacy concerns, which

are associated with threat: privacy self-efficacy and privacy risk. In line with privacy calculus model (Dinev & Hart, 2006), we select benefits of information disclosure and privacy risk as essential cognitive beliefs that constitute favorability of information disclosure, which are related to utility of information disclosure. Privacy risk is categorized as a negative cognitive belief because it augments threat but diminishes utility of information disclosure. In contrast, privacy benefits and privacy self-efficacy are classified as positive cognitive beliefs because privacy self-efficacy decreases threat of information disclosure and privacy benefits increase utility of disclosure behavior. The direct ambivalence model conceptualizes privacy concerns as attitude and suggests direct effect of privacy concerns on information disclosure to online vendors. In the model, people form privacy concerns by appraising a positive and negative cognitive beliefs associated with threat (i.e., privacy risk and privacy self-efficacy). The effect of privacy concerns on information disclosure is negatively moderated by the ambivalence of privacy risk and privacy self-efficacy. The ambivalence of benefits and privacy risk is considered for control. On the other hand, the indirect ambivalence model conceptualizes privacy concerns as individual characteristics or value and posits that indirect effect of privacy concerns via favorability of information disclosure. Since favorability of information disclosure is a positive attitude, we suggest that the attitude is driven by cognitive belief associated utility (i.e., benefits and privacy risk). The ambivalence of benefits and privacy risk negatively moderates the relation between favorability and information disclosure behavior. The ambivalence of self-efficacy and privacy risk is also considered for control. Our research models are illustrated in Figures 4.1 and 4.2.

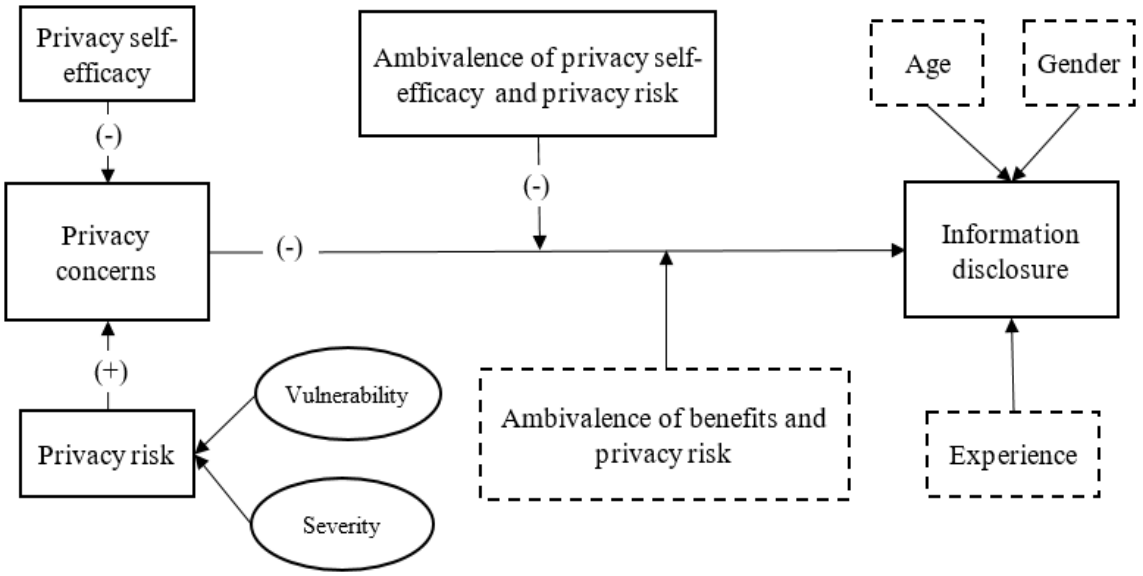


Figure 4.1 Direct Ambivalence Model

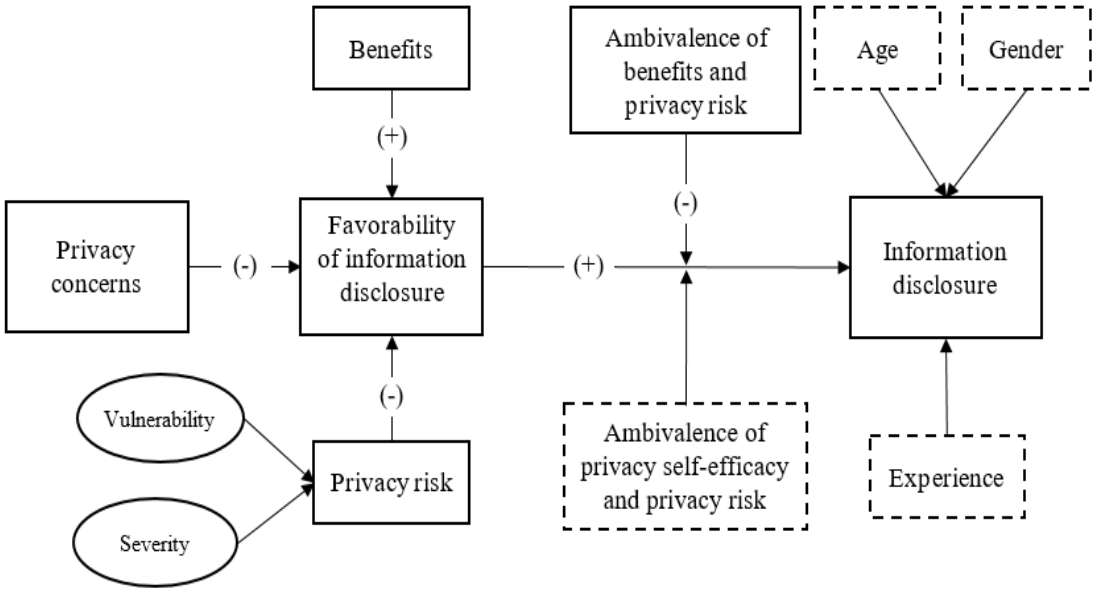


Figure 4.2 Indirect Ambivalence Model

4.4.2 Hypotheses

4.4.2.1 Direct Ambivalence Model

Privacy concerns have an adverse effect on information disclosure (Dinev & Hart, 2006; Xu et al., 2009). The expected negative outcomes associated with information disclosure such as receiving spam emails or calls raise concerns about privacy and thus restrict the disclosure of personal information (Dinev & Hart, 2006; Xu et al., 2009). Previous studies report a significant effect of privacy concerns on information disclosure in different contexts such as healthcare (Angst & Agarwal, 2009), e-commerce (Dinev & Hart, 2006; Li et al., 2011), mobile app (Keith et al., 2013; Kehr et al., 2015), and social network (Utz, 2015; Zlatolas et al., 2014). In line with previous studies, we posit that privacy concerns are negatively associated with information disclosure to online vendor.

- HYPOTHESIS 1 (H1). Privacy concerns are negatively associated with information disclosure to online vendor.

Attitude is formed by associating beliefs linked to a focal object or behavior with subjective evaluation of the belief's attribute (Ajzen, 1991; Fishbein & Azjen, 1975). Attitude is escorted by the cognitive beliefs about the possibility of obtaining positive outcomes or blocking negative outcomes (Rosenberg, 1960). While individuals are commonly argued to have either positive or negative attitude toward an object, attitudinal ambivalence suggests the coexistance of positive and negative evaluations or attitudes toward an object at the same time. According to PMT, a person's cognitive appraisals of several fundamental components of a fear appeal jointly shape his or her anxiety or concerns, which affect his or her protection behavior (Maddux & Rogers, 1983). In line with the theory, previous studies suggest that cognitive appraisals associated with fear shape privacy concerns, which motivate a coping response to deal with risk associated with information disclosure

(Lwin et al., 2007; Youn, 2009). The theory specifically suggests vulnerability, severity, self-efficacy, and response efficacy as important cognitive appraisals of forming a person's anxiety or concerns which affect protection behavior (Rogers, 1983). In this study, we focus on two cognitive appraisal components associated with the formation of privacy concerns: privacy risk and privacy self-efficacy. Privacy risk encompasses vulnerability and severity (Xu et al., 2011) and has been validated by many previous studies (Dinev & Hart, 2006; Hong & Thong, 2013; Malhotra et al., 2004). We do not consider response efficacy because there are multiple responses to protect privacy, of which effectiveness is substantially different. Further, people are often incapable of evaluating the effectiveness of a taken coping response because they are illiterate on how personal information is collected, processed, and used by online vendors, which prevents them from accurately evaluating the effectiveness of a coping response (Back, 2014; Youn, 2009).

The potential loss of privacy and negative consequences of providing personal information to online vendors increase privacy concerns, which restrict information disclosure to protect privacy (Youn, 2009). Thus, perceived privacy risk of information disclosure to online vendors increases concerns about privacy and restricts information disclosure behavior (Dinev & Hart, 2006; Xu et al., 2009). Privacy self-efficacy, the degree to which a person is confident in his or her ability to effectively protect privacy, is also an important predictor of protection behavior (Rifon et al., 2005; Youn, 2009). People who perceive themselves to be highly effective for protecting their privacy believe they can properly manage risks associated with information disclosure (Beck, 1984). The confidence in capability of controlling a potential threat often leads people to perceive a situation in an excessively optimistic manner and mitigates concern about privacy loss (Bandura, 1989).

Thus, we suggest that privacy self-efficacy lessens concern about privacy loss, whereas perceived privacy risk increases privacy concerns.

- HYPOTHESIS 2 (H2). Privacy concerns are (H2a) positively associated with privacy risk but (H2b) negatively associated with privacy self-efficacy of information disclosure.

The strength of the relation between attitude and behavior is largely determined by stability of the relation (Glasman & Albarrancín, 2006). However, attitudinal ambivalence attenuates the stability and strength of the relationship between privacy concerns and information disclosure due to the fluctuations in the salience of different cognitive beliefs. Attitudinal ambivalence reflects mixed evaluations of cognitive beliefs toward a focal object or behavior such that expressed attitude is constructed from different evaluations. In the presence of such mixed evaluations, salience of cognitive beliefs fluctuates; there are no dominant cognitive beliefs that shape and determine attitude, either positive or negative (Sparks et al., 2001). Thus, the mixed evaluations lead to weak attitude that has poor predictability on behavior. Further, the equivalently strong conflicting evaluations or cognitive beliefs restrict the accessibility to attitude (Fazio et al., 1986). Accessibility to attitude is determined by how easily a person can associate an evaluation with attitude toward an object (Bargh et al., 1992). Consequently, when positive and negative evaluations of a focal object are equivalently salient, connecting the object with an evaluation is challenging and the retrieve of attitude is prevented, such that the relation between attitude and behavior becomes weak and unstable (Fazio et al., 1986). Perceived uncertainty of expected outcomes by attitudinal ambivalence also makes the relation between attitude and behavior unstable. Equivalently strong values associated with alternatives lead to a great response uncertainty which refers

to inability to predict possible consequences of behavior (Milliken, 1987). High uncertainty by attitudinal ambivalence diminishes confidence in existing attitude and subsequently hinders accurate prediction of the consequences of information disclosure (Thompson et al., 1995). Through experiments, Armitage and Conner (2000) observed a negative effect of attitudinal ambivalence on the relation and behavior intention. Therefore, we suggest that the relation between privacy concerns and information disclosure becomes more stable as the ambivalence of positive and negative cognitive beliefs decreases.

In this study, we categorize privacy self-efficacy as positive cognitive beliefs, due to its negative effects on privacy concerns, whereas privacy risk is categorized as a negative cognitive belief of information disclosure because of its positive effect on privacy concerns. The stability and strength of the relation between privacy concerns and information disclosure decreases as the ambivalence of privacy self-efficacy and privacy risk enlarges.

- HYPOTHESIS 3 (H3). The effect of privacy concerns on information disclosure is negatively moderated by the ambivalence of privacy risk and privacy self-efficacy.

4.4.2.2 Indirect Ambivalence Model

Drawing on the theory of planned behavior (TPB, Ajzen, 1991) or theory of reasoned action (TRA, Fishbein & Ajen, 1975), previous studies suggest an indirect effect of privacy concerns on behavior through attitude (Dienlin & Trepte, 2015; Lian & Lin, 2008; Lowry et al., 2011). People concerned about privacy tend to shape negative attitude toward a technology (e.g., messenger) or communication platform (e.g., Facebook) by focusing on negative values of possible outcomes associated with information disclosure (Lowry et al., 2011). In this light, the model suggests that privacy concerns have adverse

effects on the favorability of information disclosure which, in turn, impact on information disclosure behavior.

In this model, we consider benefits of information disclosure and privacy risk as relevant cognitive beliefs that constitute attitude (i.e., favorability of information disclosure). Individuals' information disclosure closely related to the assessments of benefits and risk (Norberg et al., 2007). The privacy calculus model also suggests privacy benefits and costs as relevant cognitive beliefs associated with information disclosure in e-commerce (Culnan & Armstrong, 1999; Dinev & Hart, 2006). In this light, we posit that favorability of information disclosure is affected by perceived benefits and privacy risk of information disclosure. While privacy benefits have a positive effect on attitude toward information disclosure, perceived privacy risk negatively affect attitude because it reflects the costs of information disclosure. Since attitude is a good predictor of behavior (Ajzen, 1991), we posit the positive relationship between favorability of information disclosure and disclosure behavior. Thus, we hypothesize:

- HYPOTHESIS 4 (H4). Privacy concerns have an adverse effect on favorability of information disclosure.
- HYPOTHESIS 5 (H5). Favorability of information disclosure is influenced by cognitive beliefs of (H5a) benefits of information disclosure and (H5b) privacy risk.
- HYPOTHESIS 6 (H6). Favorability of information disclosure is positively associated with information disclosure behavior.

Attitudinal ambivalence weakens the effect of favorability of information disclosure on behavior by preventing accessibility to attitude (Fazio et al., 1986). Thus, we posit that the effect of favorability of information disclosure is negatively moderated by the

ambivalence of benefits and privacy risk. That is, the effect of the favorability on information disclosure increases, as either benefits of information disclosure or privacy risk becomes a dominate evaluation of disclosure behavior. On the other hand, the effect of the favorability diminishes when benefits and privacy risk are equivalently strong and thus no dominant evaluation exists.

- HYPOTHESIS 7 (H7). The relation between favorability of information disclosure and information disclosure is negatively moderated by the ambivalence of benefits and privacy risk.

4.5 Study Design and Data

To test the models and hypotheses, we performed a survey study that involved more than 300 undergraduate students who enrolled in a major U.S. university. We used a script to clearly explain to participants the study's objectives and our intended data analyses, and addressed any concerns related to privacy. In our survey, participants provided some demographic information and indicated their privacy concerns. Then a business scenario was presented in which an online vendor sought to collect personal information by providing some rewards in return. Participants were asked to indicate their perceived benefits, privacy risk, self-efficacy, favorability of information disclosure. Finally, they indicated their willingness to provide the personal information to the vendor.

4.5.1 Participants.

We targeted undergraduate students enrolled IS courses at the business school. Our participant selection criteria included previous experience with providing personal

information to online vendors and making purchases online. Several faculty members teaching different sessions of an IS course assisted with participant recruitment. All participation was voluntary and had no impacts on class performance and grade.

4.5.2 Measurements

We measured each investigated construct with question items adapted from previously developed and validated scales, with minor word changes that better fit our participants and context. We measured privacy concerns with items adapted from Dinev and Hart (2006) and Malhotra et al. (2004). Privacy risk belief was conceptualized as a second-order construct, consisting of privacy vulnerability and severity, consistent with Xu et al. (2011). Vulnerability, or an individual's perceived conditional probability that invasion of his or her privacy will occur (Rogers, 1983), was measured with items from Cox et al. (2004) and Eppright et al. (1994); severity, which refers to an individual's perceived magnitude of noxiousness of privacy invasion (Rogers, 1983), was measured with items from Cox et al. (2004), and Melamed et al. (1996). Benefits of information disclosure were calculated by multiplying benefit belief with values of the outcomes, in consistent with Ajzen (1991). Favorability of information disclosure was measured by using items from Chaiken and Baldwin (1981). All question items except favorability employed a seven-point Likert scale, with 1 being "strongly disagree" and 7 being "strongly agree." Question items for favorability employed an eleven-point Likert scale, with 1 being "Unfavorable" and 11 being "favorable", consistent with Chaiken and Baldwin (1981). We also collected information about participants' gender, age, experience of privacy invasion that we used as control variables in subsequent analyses.

We captured attitudinal ambivalence using the equation proposed by Thompson et

al. (1995). The equation is designed to measure similarity and intensity of two opposite evaluations toward a focal object (Armitage & Conner, 2000).

$$\text{Ambivalence} = (\text{positive} + \text{negative})/2 - |\ \text{positive} - \text{negative}\ |$$

The formula captures average intensity and level of similarity between positive and negative cognitive beliefs (Jonas et al., 1997). Attitudinal ambivalence decreases as the similarity of positive and negative cognitive beliefs increases. Since a cognitive belief was measured with multiple items, we first summed the items of a cognitive belief construct after removing an item of which loading value was below 0.7 and calculated ambivalence using the proposed equation. For calculating ambivalence associated with privacy risk which is a second-order measurement, we created a new variable by multiplying vulnerability scores to severity scores. In Table 4.2, we summarize the definition of each construct, together with its source(s) of measurement items. The measurement items are presented in Appendix E.

4.5.3 Nonresponse Bias

To examine potential nonrespondent bias, we compared the participants with the overall student pool we targeted (Fowler, 1993). We found no significant between-group differences in age, gender composition, or the number of years at the university. We also assessed nonrespondent bias by comparing early respondents (i.e., first 25% of completions) with late respondents (i.e., last 25%); again, we observed no significant between-group differences in age, gender composition, number of years at the university, or responses to various question items. These results suggested that nonrespondent bias was not a serious threat.

Table 4.2 Definition of Each Construct and Sources of Measurement Items

Constructs		Definition and Source(s)	Sources of Measurement Items
Privacy risk	Vulnerability	An individual's perceived conditional probability that invasion to his or her privacy will occur (Rogers, 1983).	Cox et al. (2004) and Eppright et al. (1994)
	Severity	An individual's perceived magnitude of noxiousness of privacy invasion (Rogers, 1983).	Cox et al. (2004), and Melamed et al. (1996)
Favorability toward information disclosure		The degree to which an individual favors information disclosure (Chaiken and Baldwin, 1981)	Chaiken and Baldwin (1981)
Benefits of information disclosure		Benefit belief × Value of outcome • Benefits belief: Perceived usefulness of disclosing personal information to obtain benefits information (Chaiken and Baldwin, 1981). • Value of outcome: Perceived value of rewards given in exchange of personal information (Chaiken and Baldwin, 1981).	Ajzen (1991)
Privacy concerns		General tendency to anxiety about the possible loss of privacy	Malhotra et al. (2004), Dinev and Hart (2006)

4.6 Analyses and Results

We approached 307 students for their voluntary participation; among them, 215 agreed to take part. Eight participants only partially completed the survey and were removed from our sample that had 208 participants, showing a 66% effective response rate. In Table 4.3, we report some descriptive statistics of our participants. As shown, approximately 66.0% of the participants were females, about 65% were younger than 25 years of age, 57% spent less than $100 a month for online purchases, and spent 4.3 hours on the Internet daily.

Table 4.3 Descriptive Statistics

Measure	Value	Number (%)
Gender	Male	102 (34.0%)
	Female	198 (66.0%)
Age	< 20	10 (3.4%)
	20-24	182 (61.5%)
	25-29	67 (22.6%)
	> 30	37 (12.5%)
Years in university	1-2 year	48 (16.1%)
	3-4 year	197 (66.1%)
	5-6 year	41 (13.8%)
	> 7 year	12 (4.0%)
Average amount spent for shopping online in the past three months	Less than $50	85 (28.3%)
	$51 ~ $ 100	86 (28.7%)
	$101 ~$150	39 (13.0%)
	$151~$200	26 (8.7%)
	$201~$300	26 (8.7%)
	> $ 300	38 (12.7%)
Time spent for the Internet		4.3 hours / a day

4.6.1 Measurements Assessments

We assessed our measurements in terms of construct reliability, and convergent and discriminant validity. To establish indicator reliability, we first removed items with a loading value equal to or lower than .6 (Götz et al., 2010). Then we examined construct reliability based on composite reliability and Rho A, using the common threshold of .7 (Bagozzi & Yi, 1988). As we summarize in Table 4.4, each construct showed a composite reliability greater than the threshold, thus suggesting appropriate construct reliability.

Table 4.4 Analysis of Construct Reliability

	Mean (Standard Deviation)	Cronbach alpha	Composite Reliability	AVE
Vulnerability	4.88 (1.41)	0.875	0.939	0.885
Severity	4.72 (1.54)	0.777	0.857	0.600
Benefits	22.62 (11.94)	0.746	0.847	0.651
Privacy concerns	4.05 (1.49)	0.789	0.862	0.610
Privacy self-efficacy	4.10 (1.40)	0.875	0.940	0.887

Note: AVE= Average Variance Extracted

We evaluated convergent validity by examining average variance extracted (AVE), using the common threshold of .5 (Götz et al., 2010). We assessed discriminant validity in terms of the square roots of AVEs and the pair-wise correlations between constructs (Fornell & Larcker, 1981). In general, we consider appropriate discriminant validity established when a construct's square root of AVE is significantly greater than the correlation between a pair of constructs. As we show in Tables 4.4 and 4.5, the AVE value of each construct exceeded .5 and was considerably greater than the correlations between any pair of constructs. In addition, we compared loading values of a construct with those of other constructs, and the results showed adequate discriminant validity. Together, our results indicated adequate convergent and discriminant validity of the measurements.

We assessed multicollinearity of measurement items by examining variance inflation factor (VIF), using the threshold of 3.3 (Cenfetelli & Bassellier, 2009) that is recommended in the context of variance-based structure equation model (Kock & Lynn, 2012). All inner and outer VIF values of the models were below the threshold, suggesting that multicollinearity is not a serious problem in our data.

Table 4.5 Square Roots of AVE and Correlations between Constructs

	BEN	PRC	SEL	SEV	VUL
BEN	**0.807**				
PRC	-0.125	**0.781**			
SEL	0.116	0.059	**0.942**		
SEV	-0.104	0.521	0.051	**0.775**	
VUL	-0.062	0.231	-0.164	0.433	**0.941**

Note: AFF=affect; BEN=privacy benefits; PRC=privacy concerns; SEL=privacy self-efficacy; SEV=severity; VUL=vulnerability.
* The square root of the AVE is shown on the diagonal.

4.6.2 Model Fit

We assessed the model fit, using the Chi-square/*df*, confirmatory fit index (CFI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR). Especially, SRMR may be more accurate because of their relative insensitivity to sample size and model complexity (Hu & Bentler, 1998). As we show in Table 4.6, although CFI values of indirect models are below the threshold (0.9), all other indices suggest that indirect models meet thresholds. Thus, our results showed that both models fit the data adequately.

Table 4.6 Overall Model Fit

Fit index	Recommended value	Direct ambivalence model	Indirect ambivalence model	Source
Chi-square/*df*	≤ 3.0	2.281	2.945	Chau and Hu (2001)
CFI	≥ 9.0	0.912	0.850	
RMSEA	≤ 0.08	0.066	0.080	Ulman (2006)
SRMR	≤ 0.08	0.056	0.057	Hu and Bentler (1998)

4.6.3 Hypothesis Test Results

At the path level, we estimated path coefficients, using partial least squares. As we show in Table 4.7 as well as Figures 4.3 and 4.4, privacy concerns showed a significant negative effect on attitude and information disclosure, in support of H1 and H4. While privacy risk was positively associated with privacy concerns, the effects of privacy self-efficacy were insignificant. Thus, our data supported H2(a) but didn't support H2(b). The effect of privacy concerns on information disclosure was significantly moderated by the ambivalence of privacy self-efficacy and privacy risk, in support of H3.

Perceived benefits and privacy risk were significantly associated with favorability of information disclosure. Thus, our data supported H5(a) and H5(b). Favorability toward information disclosure had significant positive effect on information disclosure, in support of H6. The ambivalence of privacy benefits and risk significantly moderated the relation between favorability and information disclosure, in support of H7.

4.6.4 Ex Post Analysis

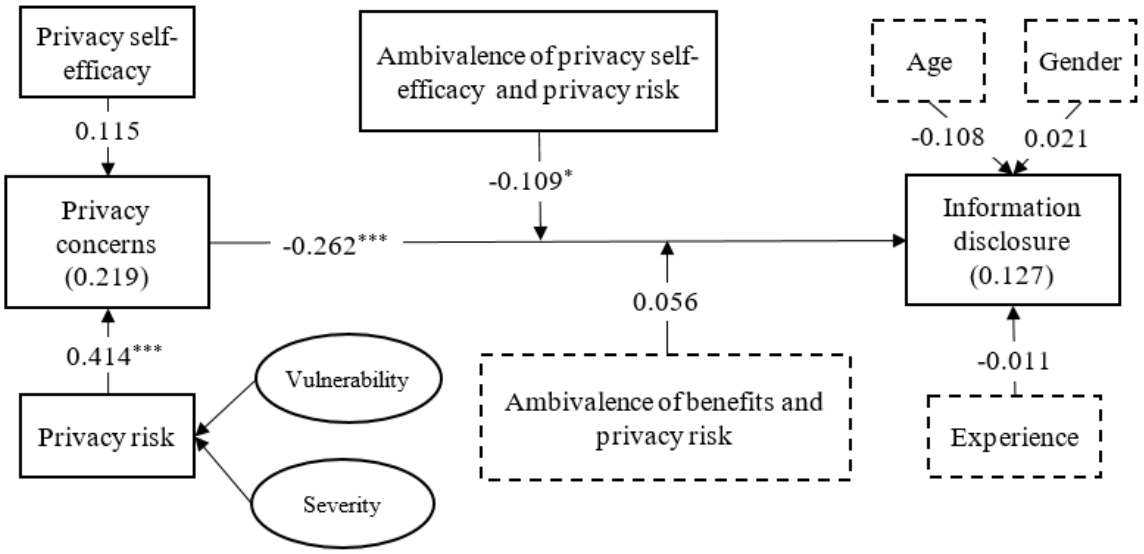
4.6.4.1 Alternative Indirect Ambivalence Model

To assure the internal validity of indirect ambivalence model, we examined an alternative model in which the effect of privacy concerns on favorability of information disclosure is moderated by the two different ambivalences: ambivalence of (a) privacy benefits and risk and (b) privacy self-efficacy and risk. As presented in Figure 4.5, the moderating effects of the ambivalences were insignificant. That is, the two ambivalences only affect the relation between favorability and information disclosure.

Table 4.7. Hypothesis Test Results

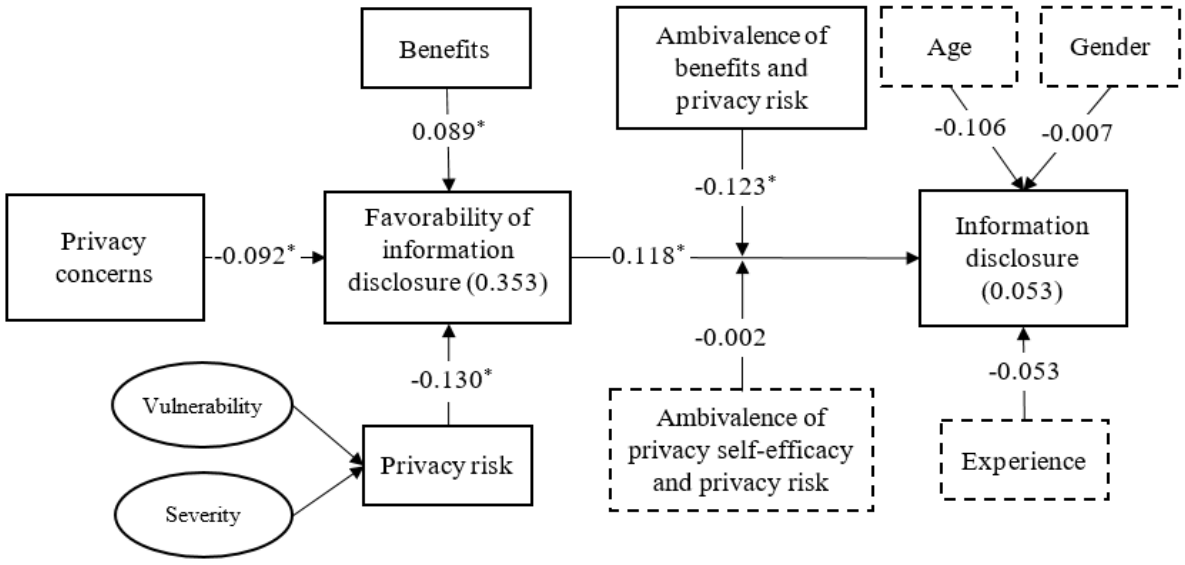
Exogenous	Endogenous	Direct Ambivalent Model	Indirect Ambivalence Model	Hypothesis	Result
FAV	IDB		0.118* (0.053)	H6	Supported
BEN	FAV		0.089* (0.040)	H4(a)	Supported
PRC	FAV		-0.092* (0.046)	H4	Supported
	IDB	-0.262*** (0.064)		H1	Supported
RISK	FAV		-0.130* (0.057)	H4(b)	Supported
	PRC	0.414*** (0.056)		H2(a)	Supported
SEL	PRC	0.115 (0.079)		H2(b)	Not supported
A_BEN_RIS	FAV→IDB		-0.123* (a) (0.055)	H7	Supported
A_SEL_RIS	PRC→IDB	-0.109* (a) (0.052)		H3	Supported
A_BEN_RIS	PRC→IDB	0.056 (0.061)		Control variable	
A_SEL_RIS	FAV→IDB		-0.002 (0.072)		
AGE	IDB	-0.108 (0.065)	-0.106 (0.061)		
GEN	IDB	0.021 (0.079)	-0.007 (0.055)		
EXP	IDB	-0.011 (0.058)	-0.053 (0.057)		
R^2	FAV		0.353		
	IDB	0.127	0.053		
	PRC	0.219			

Note: FAV=favorability toward information disclosure; BEN= privacy benefits; PRC=privacy concerns; RISK=privacy risk; SEL=privacy self-efficacy; A_BEN_RIS= ambivalence of privacy benefits and privacy risk; A_SEL_RIS= ambivalence of privacy self-efficacy and privacy risk; AGE=age; GEN=gender; EXP=experience of privacy invasion. The values in parenthesis denote standard error of path coefficients.
*p<0.05, **p<0.01, ***p<0.001



*p<0.05, **p<0.01, ***p<0.001

Figure 4.3 Analysis results of Direct Ambivalent Model



*p<0.05, **p<0.01, ***p<0.001

Figure 4.4 Analysis Results of Indirect Ambivalence Model

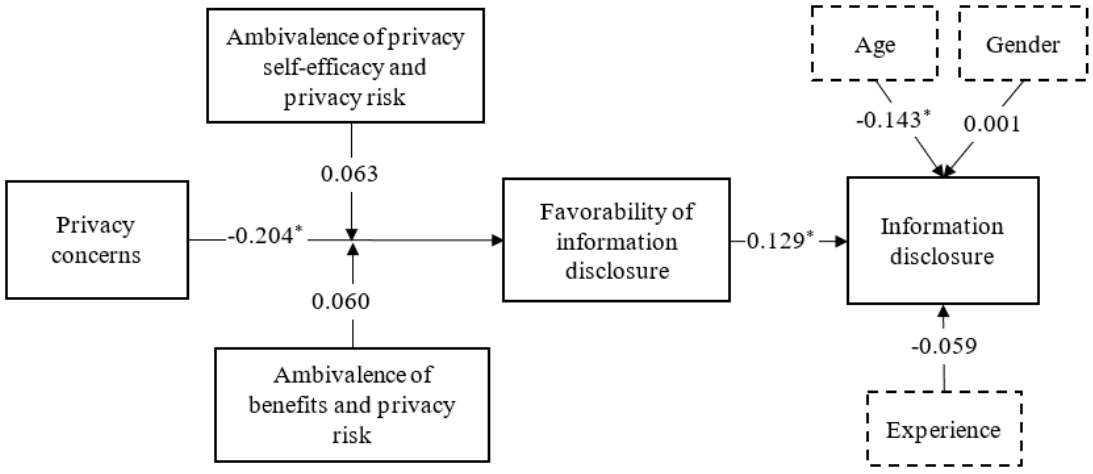


Figure 4.5 Alternative Indirect Ambivalence Model

4.6.4.2 The Comparative Effect of Affect

Heuristic-Systematic Model (HSM) (Chaiken et al., 1989) suggests that individuals try to minimize their cognitive effort in information processing (i.e., least effort principle) by relying on heuristic rules, given that these rules provide a certain level of confidence (Eagly & Chaiken, 1993). In this light, we expect that affect has greater effect in the presence of high attitudinal ambivalence, in which positive and negative cognitive are equivalently salient and more effort is required to process information. Thus, we separate data as high vs. low ambivalence group associated with privacy benefits and risk. Specifically, we calculated z-scores of attitudinal ambivalences and took about top and bottom 30% as high and low ambivalence group, respectively. Then we analyzed the effect of affect on favorability toward information disclosure and compared the path coefficients. Consistent with Steelman et al. (2014), our comparative results were obtained from a two-tailed *t*-test. As shown in Table 4.8, the result shows that affect has greater effect in the high ambivalence group.

Table 4.8. Comparisons of Affect's Effect

Construct	Path coefficient		t-value
	High ambivalence	Low ambivalence	
Affect → Favorability	0.480 (s=0.096, n=114)	0.450 (s=0.071, n=103)	2.594*

Note: s=standard error, n=sample size.
*p<0.05

4.7 Discussion

Our study contributes to extant literature by examining factors that moderate the relation between privacy concerns and information disclosure to online vendors through the lens of attitudinal ambivalence. Our results demonstrate that the ambivalence of the positive and negative cognitive beliefs moderate the effect of attitude (i.e., privacy concerns and favorability of information disclosure) on information disclosure behavior.

Our results offer several implications for research. First, our results highlight the importance of attitudinal ambivalence in explaining the strength of the relationship between attitude and behavior. Previous IS studies distinguish between positive and negative attitude and examine their respective effect on behavior. For example, Cenfetelli (2004) discriminates enabler of technology adoption from inhibitor and suggests that they are different in their sources and consequences. Dimoka (2010) examines the location, timing, and level of brain activity that underlies trust and distrust using fMRI and demonstrates that trust and distrust are different constructs. However, attitudinal ambivalence suggests the coexistance of positive and negative evaluations toward a focal object and highlights moderating effect of the ambivalence of the different evaluations on the relation between attitude and behavior. For example, according to attitudinal

ambivalence, when individuals appreciate an object such as an online website, they hold trust and distrust toward the website at the same time. As a result, the magnitude of the existing attitude toward the website is determined by the degree to which trust and distrust are equivalently strong. Therefore, our results may suggest that the examination of respective effect of positive or negative cognitive belief may offer limited explanation of the effect of attitude. Thus, it is essential to scrutinize attitudinal ambivalence for a better understanding of the relation between attitude and behavior. Further, the moderating effect of attitudinal ambivalence helps to figure out why previous studies observe mixed results of attitude's effect on behavior and reconcile the inconsistent effects of attitude or cognitive belief.

Second, our results reveal that different cognitive beliefs engage in attitudinal ambivalence, depending on whether attitude is positive or negative: while the ambivalence of privacy self-efficacy and risk affects the effect of negative attitude (i.e., privacy concerns), the ambivalence of privacy benefits and risk moderates the effect of positive attitude toward information disclosure (i.e., favorability). While previous studies commonly capture positive and negative evaluations of a focal attitude in examining the effect of attitudinal ambivalence (e.g., Armitage & Conner, 2000; Jonas et al., 1997; Thompson et al., 1995), our findings suggest the necessity of distinguishing positive and negative attitude and examining cognitive beliefs or evaluations relevant to attitude. In this light, a systematic identification of privacy concerns is essential for a better understanding of the roles of attitudinal ambivalence. Previous IS studies have identified a number of antecedents of privacy concerns such as experience, privacy awareness, demographic factors, or personality traits (Li, 2012; Smith et al., 2011). However, many previous studies

tend to rely on previous studies for choosing important antecedents to examine, such that the legitimacy and validity of chosen factors are not sufficiently assured. Legitimately identified antecedents of privacy concerns help to understand what antecedents of privacy concerns engage in attitudinal ambivalence.

Third, our results shed light on the condition in which direct and indirect effects of privacy concerns become negligible, and thus reconcile the mixed results of direct or indirect effect of privacy concerns. Privacy concerns have significant direct and indirect effect on information disclosure when both attitudinal ambivalences are low (i.e., partial mediation). When the ambivalence of privacy risk and privacy self-efficacy is only salient, privacy concerns indirectly affect information disclosure through favorability (i.e., full mediation). On the other hand, when the ambivalence of benefits and privacy risk is only salient, privacy concerns have significant effect on information disclosure. Our findings thus suggest the importance of examining moderating factors for a better understanding about the relation between privacy concerns and behavior. Previous studies seem to overlook the roles of moderating factors in examining the effect of privacy concerns. However, the mixed results of privacy concerns' direct or indirect effect call for more effort in examining the roles of factors moderating the effect of privacy concerns.

Last but not least, our findings seem to confirm *the least effort principle* in information processing. Individuals attempt to minimize their cognitive effort in information processing by relying on heuristic rules, given that these rules provide a certain level of confidence (Eagly & Chaiken, 1993). Our *ex post* analysis result shows that affect had greater effect in the presence of high attitudinal ambivalence, in which people hold equivalently strong cognitive beliefs of privacy benefits and risk associated with

information disclosure. That is, when the evaluations of privacy benefits and risk are equivalent, processing the information of benefits and risk requires more cognitive effort. Thus, people try to minimize the effort for information processing by relying on heuristic rules such as affect. This finding may offer an alternative explanation of why some previous studies observe ingenuine weak relationship between privacy concerns and information disclosure (e.g., Baek, 2014; Dienlin & Trepte, 2015). When the values and costs of information disclosure are similar, people need to process information more systematically, which requires more cognitive effort (Jonas et al., 1997). To minimize cognitive effort, people rely on heuristic rules for deciding information disclosure. As a result, the formed privacy concerns tend to be superficial and dubious, which can't resist changes (Baek, 2014).

CHAPTER 5

CONCLUSION

Our studies contribute to the literature by examining important but less explored issues associated with privacy concerns in e-commerce. In specific, our studies examine essential sources of privacy concerns and offer an alternative explanation of the discrepancy between privacy concerns and information disclosure in e-commerce.

We contribute to the literature by offering an alternative explanation of the inconsistent effect of privacy concerns, which is coined as the privacy paradox: psychological distance and attitudinal ambivalence. Our psychological distance approach provides an insight on the paradoxical phenomenon by examining how inconsistency of high- and low-level of construals of privacy concerns' determinants leads to privacy paradox. Especially our explanation sheds light on how general and situation specific factors jointly affect behavior, different from previous studies which take a static view and exclusively consider either general or situational factors. Further, while previous studies focus on factors that mitigate the effect of privacy concerns, they seem to pay little attention to examining the condition in which privacy concerns can't explain information disclosure in a reliable manner. In this light, our studies contribute to the body of knowledge by examining how change of construal level toward privacy concerns determinants due to the decreased psychological distance affects the relation between privacy concerns and

information in a specific situation. In specific, we analyzed the effect of psychological distance and construals through a longitudinal perspective, which enables a comparison of construals associated with privacy concerns' determinants between a general setting and a particular situation. Further, our study provides a fuller explanation of the inconsistent effect of privacy concerns by examining and comparing both generic factors and situation-specific factors. Finally, we contribute to privacy paradox research by specifying the condition in which privacy paradox occurs; the privacy paradox occurs when the high- and low-level construals of privacy concerns' determinants are inconsistent. However, there are several limitations. Different from our assumption, low-level construals of context-specific benefits and privacy risk could be connected to high-level construals of those factors in a general situation. Although we put a one-week interval between phases to mitigate the possible association, people could evaluate benefits and privacy risk in a particular situation, anchoring their abstract evaluations in a general situation. In this light, future studies are encouraged to examine the possible association between high- and low-level construals. Future research can also offer a better explanation of the privacy paradox by measuring actual behavior, instead of intention or willingness. Previous studies point out that intention may not correctly reflect actual information disclosure behavior (Smith et al., 2011). Further, future research can make a contribution by distinguishing a positive consistency condition from a negative consistency condition and examine the relation between general privacy concerns and information disclosure in a particular situation. A one-week interval between phases may not be sufficient to prevent carryover effect, which can construct a bridge between high- and low-level construals and lead to biased results. Self-selection bias is another weakness of our experimental design. Participants who felt

great interest about the topic were more likely to complete the experiments than otherwise. In this light, future research can attain the validity of results by preventing such biases.

We also seek to offer logical explanation of inconsistent effect of privacy concerns by examining the moderating effect of attitudinal ambivalence. While most previous studies focus on the inconsistency of direct effect of privacy concerns, little attention is paid to explaining why indirect effects of privacy concerns are inconsistent. Our study explains the inconsistencies by highlighting the moderating effects of attitudinal ambivalence. The analysis results highlight the necessity of examining the effect of the gap between a positive and a negative cognitive belief on the relation between IS related attitude and behavior. However, future study can extend the scope by considering other important cognitive beliefs that constitute privacy concerns or attitude of information disclosure and examining the effects of their ambivalence. Further, this study conceptualizes privacy concerns as attitude, which is an essential assumption in building research model. However, the conceptualization may not be justified. Last but not least, we collected data from university students, which restricts the generalizability of our findings.

We also contribute to privacy research by identifying essential antecedents of privacy concerns in e-commerce. Although previous studies suggest examining a number of antecedents of privacy concerns such as experience, privacy awareness, demographic factors, or personality traits, the presented antecedents seem less effective for explaining the formation of privacy concerns in e-commerce, largely due to lack of theoretical foundation and emphasis on either generic or context-specific factors only. The lack of theoretical foundation in choosing the key determinants of privacy concerns questions the legitimacy and validity of chosen factors. A proper theory renders legitimacy of the

antecedent choices by providing established premises for explaining why particular antecedents should be emphasized and how they may lead to the creation of online privacy concerns. Further, the less attention to indirect effects of plausible antecedents of privacy concerns may offer incomplete explanation of how privacy concerns are formed by the chosen factors. To close the gaps, we attempt to identify key determinants through a theoretical lens and provide more integrated perspective by incorporating different cognitive appraisals. Specifically, we select privacy risk, self-efficacy, response efficacy, notice, and consent as essential antecedents of privacy concerns, drawing on protection motivation theory and procedural fairness. While the former four antecedents are generic factors, the latter two factors are e-commerce specific. The consideration of both generic and context-specific factors may explain the determinants of privacy concerns in an effective manner. Further, we analyze direct and indirect effects of the factors, thereby helping to figure out the process of forming privacy concerns in a better way.

However, our study has several limitations that in turn point to further research directions. For example, we focus on individual cognitive appraisals and examine their effect on privacy concerns, but external factors such as industrial or government regulation also could influence privacy concerns. Thus, future research is encouraged to consider external factors and examine their effects and joint effects with cognitive appraisals as well. Further, while we only focus on rational, cognitive appraisals, we ignore the effects of non-cognitive factors such as affect or social influence. In this light, future research can provide better explanation by considering heuristic factors. Finally, although PMT helps to identify key cognitive appraisals that form anxiety or concerns, the theory is limited in explaining the process of how the cognitive appraisals shape concerns about privacy. Thus, future

research is required to have a better theoretical foundation for explaining the relationships between selected antecedents and privacy concerns. Finally, we indirectly examine the direct and moderating effects of culture by comparing two countries which hold quite different cultures. Future research can offer a better explanation of cultural roles in shaping privacy concerns by directly measuring individual cultural values and analyzing their effects.

APPENDIX A

ANALYSIS RESULTS (MTURK DATA)

A.1 Experiment Flow

We also collected data from MTurk workers. We first conducted a pilot study with MTurk workers. A total of 116 and 48 workers completed phase 1 and 2, respectively. We experienced significant casualty in phase 2. The pilot test results affirmed the overall feasibility of experimental design and clarity of the question items with some minor issues. After the pilot test, we hired 582 workers living in the U.S. in phase 1. Among them, we removed 42 data points due to their incorrect information about their MTurk ID. Since our experiment is longitudinal, MTurk ID is essential to track a specific worker across different phases for classification and assignment. To prevent further data loss due to the failure of manipulation check that we experienced with student data, we announced to MTurk workers that they would not get a bonus when they provided incorrect answers to manipulation check questions. We used 540 data points for analysis in phase 1. In phase 2, 352 MTurk workers participated in and completed the surveys, respectively. As we did with student data, MTurk workers were sorted by their z-scores of benefits and privacy risk. Then we classified the top and bottom 40% as high versus low group and removed the remaining middle 20% of MTurk workers for assuring our classification. The total number of workers used for data analysis in phases and descriptive statistics are presented in Tables A.1 and A.2.

Table A.1 The Number of Subjects Used for Data Analysis

	Consistency	Positive inconsistency	Negative inconsistency
Phase 1	540		
Phase 2	149	89	114

Table A.2 Descriptive Statistics

		Frequency / Average (Std.)	Percent
Gender	Female	205	0.380
	Male	335	0.620
Age		36.7 (10.2)	

A.2 Measurement Testing Results

We assessed construct reliability, and convergent and discriminant validity. We first removed items with a loading value lower than .6 to establish indicator reliability and then assessed construct reliability using Cronbach's alpha and composite reliability, using the common threshold of .7. As shown in Table A.3, each construct indicated appropriate construct reliability. The AVE value of each construct exceeded .5, which suggests adequate convergent validity of the constructs.

Table A.3 Analysis of Construct Reliability

Construct	Mean (Standard deviation)	Average Variance Extracted (AVE)	Composite Reliability	
			Composite Reliability	Cronbach's alpha
Privacy concerns	20.02 (4.85)	0.785	0.936	0.909
Benefits	18.35 (4.93)	0.867	0.963	0.949
Privacy risk	18.39 (4.94)	0.802	0.942	0.918
Privacy efficacy	18.86 (5.20)	0.746	0.921	0.926
Response efficacy	18.16 (4.69)	0.779	0.934	0.906

Discriminant validity was evaluated by examining whether a construct's square root of AVE is significantly greater than the correlation between a pair of constructs. As Table A.4 suggests, the AVE value of each construct was noticeably greater than the correlations between any pair of constructs.

A.3 Hypothesis Test Results

We present analysis results in Table A.5. The results supported all hypotheses except a negative inconsistency condition associated with privacy self-efficacy and response efficacy.

Table A.4 Square Roots of AVE and Correlations between Constructs

	Privacy concerns	Benefits	Privacy risk	Privacy self-efficacy	Response efficacy
Privacy concerns	**0.886**				
Benefits	-0.265	**0.931**			
Privacy risk	0.760	-0.358	**0.895**		
Privacy self-efficacy	-0.084	0.079	-0.111	**0.863**	
Response efficacy	-0.210	0.350	-0.244	0.492	**0.882**

Note: The square root value AVE of privacy risk and privacy concerns and their correlations with other constructs are not presented because they are conceptualized as second-order construct.

Table A.5 Summary of Analysis Results

Phase	Condition	Exogenous	Endogenous	Path coefficient	Hypothesis
Phase2	Consistency	GPC	GID	-0.577***	Supported
		GPC	PID	-0.487***	Supported
	Positive Inconsistency	GPC	GID	-0.459***	Supported
		GPC	PID	0.266 (n.s.)	Supported
	Negative Inconsistency	GPC	GID	-0.294***	Supported
		GPC	PID	-0.142 (n.s.)	Supported

Note: GPC=General Privacy Concerns; GID=Information Disclosure in a general situation; PID=Information disclosure in a particular situation; n.s.=not significant.

*p<0.05, **p<0.01, ***p<0.001

A.4 Ex Post Analyses

A4.1 High- and Low-level Construal

We examined the relationship between psychological distant and the level of construal by analyzing time for responding questions regarding privacy concerns' determinants. However, we removed a response of which response time for one question was over 4 minutes or lower than 5 seconds. The analysis result is presented in Table A.6.

A4.2 Test of Classification

To assure our group classification, we compared the responses of questions associated with privacy concerns' determinants between a general and a particular situation across different experimental conditions. The results are presented in Table A.7.

A4.3 Comparison of Information Disclosure

We compared information disclosure between a general and particular situation across different experimental conditions to see if information disclosure is more affected by situation-specific information. Table A.8 summarizes the analysis results.

Table A.6 Comparison of Response Time

Appraisal	Response time		F-statistic
	Phase 1	Phase2/3	
Threat[a)]	25.4	29.3	3.92*
Coping[b)]	27.01	37.0	38.14***

Note: Response time is the average time taken for responding a question

a) Threat appraisal consists of benefits and privacy risk.

b) Coping appraisal consists of self-efficacy and response efficacy.

*p<0.001, ***p<0.001

Table A.7 Comparison of Determinants of Privacy Concerns

Phase	Condition	Determinants	General	Particular	F-statistic	Classification
Phase 2	Consistency	Benefits	18.50	19.33	$0.81^{n.s.}$	Supported
		Privacy risk	17.68	18.45	$0.90^{n.s.}$	Supported
	Positive Inconsistency	Benefits	21.73	17.19	32.29^{***}	Supported
		Privacy risk	19.40	13.13	56.31^{***}	Supported
	Negative Inconsistency	Benefits	31.44	23.49	62.14^{***}	Supported
		Privacy risk	15.94	24.43	143.12^{***}	Supported

Note: n.s.=not significant,
$^{*}p<0.05$, $^{**}p<0.01$, $^{***}p<0.001$

Table A.8 Comparison Result of Information Disclosure

Condition	Average of GID	Average of PID	F-statistic
Consistency	3.122	2.960	$0.753^{(n.s.)}$
Positive Inconsistency	2.517	3.730	30.530^{***}
Negative Inconsistency	3.214	1.616	128.703^{***}

Note: GID=Information disclosure in a general situation; PID=Information disclosure in a particular situation
$^{+}p<0.1$, $^{*}p<0.05$, $^{**}p<0.01$, $^{***}p<0.001$

APPENDIX B

EXPERIMENTAL SCENARIOS

B.1 General Information

It is common practice that many online vendors recruit members to collect personal information for business purposes. The collected personal information allows vendors to provide products that fit to customers' needs/tastes and personalized services, which lead to increased sales and customer loyalty.

B.2 High Benefits and High Privacy Risk Group

An online research company, emarketbiz.com, is recruiting members on behalf of an online vendor, **Goodsales.com**, which is promoting a special event now. If you join the membership today, you can enjoy a variety of benefits given to members **ONLY**. **Goodsales.com offers greater benefits than most other online vendor do!**

- **15% extra discount** for first purchase
- **A $10 gift card**: $10 gift cards to 20% of the people who join membership today, via a lucky draw.
- **Personalized product recommendation**: You will get product recommendation that fits to your needs or taste every day. Don't waste time to search goods anymore!
- **Hot deal information**: You will be informed special deal for a variety of products which provides 30%~70% discount from original price in general!
- **E-coupons**: You can access e-coupons which are update every month (the coupons provide 0.5$ to 1.5$ discount to approximately 20~30 products).
- **Special promotion** for members, including buy one, get one free for specific products.
- **1% annual reward:** You will receive an annual 1% reward on qualified purchases (Reward is capped at, and will not exceed, $1,000 for any 12-month period).

Following the Privacy Act, we notify that this online vendor has violated Fair Information Practices Principles (FTPPs) of the U. S. Federal Trade Commission multiple times in the last 3 months by selling personal information to third parties without getting consent from information providers and allowing employees to freely access the collected personal information. In addition, **Goodsales**' information systems are unsecured and vulnerable for intrusion from outside.

B.3 High Benefits and Low Privacy Risk Group

An online research company, emarketbiz.com, is recruiting members on behalf of an online vendor, **Goodsales.com**, which is promoting a special event now. If you join the membership today, you can enjoy a variety of benefits given to members **ONLY**. **Goodsales.com offers greater benefits than most other online vendor do!**

- **15% extra discount** for first purchase
- **A $10 gift card**: $10 gift cards to 20% of the people who join membership today, via a lucky draw.
- **Personalized product recommendation**: You will get product recommendation that fits to your needs or taste every day. Don't waste time to search goods anymore!
- **Hot deal information**: You will be informed special deal for a variety of products, which provides 30%~70% discount from original price in general!
- **E-coupons**: You can access e-coupons which are update every month (the coupons provide 0.5$ to 1.5$ discount to approximately 20~30 products).
- **Special promotion** for members, including buy one, get one free for specific products.
- **1% annual reward:** You will receive an annual 1% reward on qualified purchases (Reward is capped at, and will not exceed, $1,000 for any 12-month period).

Following the Privacy Act, we notify that this online vendor has completely complied with Fair Information Practices Principles (FTPPs) of the U. S. Federal Trade Commission in collecting and using personal information. This vendor has never shared personal information without permission of information providers and security system of the vendor also ensures no unauthorized access to the collected personal information. This online vendor is very trustworthy and highly reputable.

B.4 Low Benefits and High Privacy Risk Group

An online research company, emarketbiz.com, is recruiting members on behalf of an online vendor, **Goodsales.com**, which is promoting a special event now. If you join the membership today, you can enjoy a variety of benefits given to members **ONLY**:

- **Personalized product recommendation**: You will get product recommendation that fits to your needs or taste every day. Don't waste time to search goods anymore!
- **Hot deal information**: You will be informed special deal for a variety of products which provides 30%~70% discount from original price in general!

Following the Privacy Act, we notify that this online vendor has violated Fair Information Practices Principles (FTPPs) of the U. S. Federal Trade Commission multiple times in the last 3 months by selling personal information to third parties without getting consent from information providers and allowing employees to freely access the collected personal information. In addition, **Goodsales**' information systems are insecured and vulnerable for intrusion from outside.

B5: Low Benefit and Low Risk Group

An online research company, emarketbiz.com, is recruiting members on behalf of an online vendor, **Goodsales.com**, which is promoting a special event now. If you join the membership today, you can enjoy a variety of benefits given to members **ONLY**:

- **Personalized product recommendation**: You will get product recommendation that fits to your needs or taste every day. Don't waste time to search goods anymore!
- **Hot deal information**: You will be informed special deal for a variety of products which provides 30%~70% discount from original price in general!

Following the Privacy Act, we notify that this online vendor has completely complied with Fair Information Practices Principles (FTPPs) of the U. S. Federal Trade Commission in collecting and using personal information. This vendor has never shared personal information without permission of information providers and security system of the vendor also ensures no unauthorized access to the collected personal information. This online vendor is very trustworthy and highly reputable.

APPENDIX C

MEASUREMENT ITEMS (CHAPTER 2)

Privacy concerns

1. All things considered, providing my personal information to online vendors would cause serious privacy problems.
2. I am concerned that the personal information I submit to online vendors could be misused.
3. I am concerned about threats to my personal privacy when I provide my personal information to online vendors.
4. I am concerned about disclosing personal information to online vendors, because it could be used in ways I did not foresee.

Benefits of information disclosure

1. Providing personal information is helpful for getting monetary benefits (e.g., coupon, discount) or personalized service (e.g., product recommendations, hot deal information) from online vendors.
2. Offering personal information is useful for receiving monetary benefits, personalized services, or beneficial information from online vendors.
3. Disclosing personal information works for getting monetary benefits, personalized services, or beneficial information given by online vendors.
4. Personal information disclosures enable me to receive monetary benefits, personalized services, or beneficial information from online vendors.

Privacy risk

1. In general, it would be risky to disclose my personal information to online vendors.
2. There would be high potential for privacy loss associated with providing my personal information to online vendors.
3. There would be too much uncertainty associated with my giving personal information to online vendors.
4. Providing a vendor with my personal information would create many unexpected problems.

Privacy self-efficacy

1. I can protect my online privacy even if there is no one around to help me do so.
2. In my mind, I have the knowledge and skills necessary for protecting my privacy online.
3. I think that it is not difficult finding effective ways to protect my own privacy in online settings.
4. I am confident that I am able to protect my privacy in online contexts.

Response-efficacy

1. I believe that there would be effective ways to reduce the risk of online privacy invasion (e.g., checking an online vendor's privacy policy), even if I reveal my personal information to online vendors.
2. In my belief, I could find effective means to protect my own privacy (e.g., checking third-part certification such as eTrust), even though I submit my personal information to online vendors.
3. I believe that actions (such as checking the list of companies violating fair information practice) work for protecting my own privacy, even though I reveal my personal information to online vendors.
4. By adopting effective means (such as checking privacy policy of online vendors), I can protect my own privacy.

Willingness to information disclosure

Are you willing to join membership by providing your personal information such as name, gender, email, and mailing address?

APPENDIX D

MEASUREMENT ITEMS (CHAPTER 3)

Vulnerability

1. In my estimation, my privacy is likely to be invaded in online settings.
2. Considering the different factors that could affect personal privacy online (e.g., how firms collect and analyze people's personal information), I think that the likelihood of invasion to my own privacy is high.
3. Even without taking any measure, the probability of having my privacy invaded online is slim.
4. In my estimation, the risk of invasion to my privacy online is higher than that of many other people.
5. I cannot see how my privacy can be invaded in online settings.

Severity

1. Privacy invasion is a more serious concern to me than any other online issues, such as dissemination of fake information, porn addiction, or trolling.
2. I believe that online privacy invasion is a serious problem as it poses a great threat to Internet users.
3. Concerns about online privacy invasion would significantly influence the way I use the Internet.
4. To me, privacy invasion remains as serious as it was ever before, despite the advances in online privacy protection.
5. Even if personal privacy could be invaded in an online setting, it would not be serious enough to affect my Internet usage behaviors.

Response efficacy

1. I believe that there are effective ways to reduce the risk of online privacy invasion.
2. In my opinion, privacy invasion is inevitable when people engage in online activities; that is, there is no way we can address this issue.
3. In my belief, there are effective actions that I can take to reduce the risk of online privacy invasion, such as providing incorrect information to online firms.

Self-efficacy

1. I can protect my own privacy online even if there is no one around to help me do so.
2. I have difficulties finding effective ways to protect my own privacy in online settings.
3. In my mind, I have the knowledge and skills necessary for protecting my privacy online.
4. I am confident that I am able to protect my own privacy in online settings.
5. I have full confidence of dealing with online firms' collecting and using my personal information; that is, I know how to protect my privacy.

Notice

1. I believe that an online firm always informs to me when it collects, processes, and uses my personal information for its business purposes.
2. Based on my understanding, all online firms state their online privacy policy in a clear and conspicuous manner so that I always know when they collect and use my personal information.
3. I think that online firms usually appreciate my awareness, through a notice, when they collect and use my personal information for various purposes.
4. I believe that online firms fully understand their invasion of my privacy by collecting, processing, and using my personal information without any notices.

Consent

1. I think that online firms collect, process, and use my personal information only after obtaining my consent.
2. In my opinion, online firms fully respect my rights to control, through an explicit consent, how my information can be collected, used, and shared.
3. I believe that an online firm clearly understands its invasion to my privacy when it collects, uses, and shares their personal information without my agreement.
4. I think that online firms usually understand the importance of my agreement to their collecting and using my privacy information.

Secondary use

1. When I provide my personal information to an online firm for a particular reason, I am always worried that the firm would use that information for other purposes.
2. I have great concerns that an online firm would sell my personal information (stored in its databases) to other firms.
3. I am afraid that an online firm would share with other firms my personal information it gathers online, without my authorization for doing so.
4. I am totally convinced that, without my authorization, online firms would not use my personal information for any secondary purposes.

Unauthorized access

1. I am suspicious that an online firm would devote the necessary resources and efforts to prevent unauthorized access to my personal information it collects.
2. I am not skeptical that an online firm would allocate the necessary resources to protect its databases that contain my personal information from unauthorized access, regardless of the cost.
3. I doubt that any online firms would take proper measures against unauthorized access to my personal information stored in their computers.
4. I am concerned about an online firm's mismanagement of my personal information by having the information accessible to unauthorized parties.

Collection

1. I have great concerns when an online firm asks me for personal information beyond what is normally required for transaction or service.
2. I feel nervous about providing my personal information to online firms.
3. I sense severe threats to my privacy when an online firm requests a lot of personal information from me.
4. Because of potential risks of self-disclosure, I usually think twice when an online firm asks for my personal information.

Error

1. I am not convinced that any online firm would take proper measures to ensure the accuracy of my personal information stored in their databases.
2. I am suspicious that online firms would implement the necessary procedures to detect and correct errors in my personal information they collect and store in computer-based systems.
3. I am apprehensive that all online firms would allocate the necessary time and efforts to verify the accuracy of my personal information stored in databases.
4. I doubt that any online firm would double check the accuracy of my personal information they collect online before saving it in databases, no matter how much this would cost.

APPENDIX E

MEASUREMENT ITEMS (CHAPTER 4)

Privacy concerns

1. All things considered, providing my personal information to online vendors would cause serious privacy problems.
2. I am concerned that the personal information I submit to online vendors could be misused.
3. I am concerned about threats to my personal privacy when I provide my personal information to online vendors.
4. I am concerned about disclosing personal information to online vendors, because it could be used in ways I did not foresee.

Vulnerability

1. In my estimation, my privacy is likely to be invaded in online settings.
2. Considering the different factors that could affect personal privacy online (e.g., how firms collect and analyze people's personal information), I think that the likelihood of invasion to my own privacy is high.
3. Even without taking any measure, the probability of having my privacy invaded online is slim.
4. In my estimation, the risk of invasion to my privacy online is higher than that of many other people.
5. I cannot see how my privacy can be invaded in online settings.

Severity

1. Privacy invasion is a more serious concern to me than any other online issues, such as dissemination of fake information, porn addiction, or trolling.
2. I believe that online privacy invasion is a serious problem as it poses a great threat to Internet users.
3. Concerns about online privacy invasion would significantly influence the way I use the Internet.
4. To me, privacy invasion remains as serious as it was ever before, despite the advances in online privacy protection.
5. Even if personal privacy could be invaded in an online setting, it would not be serious enough to affect my Internet usage behaviors.

Self-efficacy

1. I can protect my own privacy online even if there is no one around to help me do so.
2. I have difficulties finding effective ways to protect my own privacy in online settings.
3. In my mind, I have the knowledge and skills necessary for protecting my privacy online.
4. I am confident that I am able to protect my own privacy in online settings.
5. I have full confidence of dealing with online firms' collecting and using my personal information; that is, I know how to protect my privacy.

Perceived benefits

1. Providing personal information is helpful for getting monetary benefits (e.g., coupon, discount) or personalized service (e.g., product recommendations, hot deal information) from online vendors.
2. Offering personal information is useful for receiving monetary benefits, personalized services, or beneficial information from online vendors.
3. Disclosing personal information works for getting monetary benefits, personalized services, or beneficial information given by online vendors.
4. Personal information disclosures enable me to receive monetary benefits, personalized services, or beneficial information from online vendors.

Favorability

- Please indicate your favorability toward information disclosure.

REFERENCES

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21-29). ACM.

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, *7*(6), 82-85.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26–33.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*(2), 160-174.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Ajzen, I., & Fishbein, M. (2000). Attitudes and the attitude-behavior relation: Reasoned and automatic processes. *European Review of Social Psychology*, *11*(1), 1-33.

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, *86*(4), 797-804.

Alter, A. L., & Oppenheimer, D. M. (2008). Effects of fluency on psychological distance and mental construal (or why New York is a large city, but New York is a civilized jungle). *Psychological Science*, *19*(2), 161-167.

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

Armitage, C. J., & Conner, M. (2000). Attitudinal ambivalence: A test of three key hypotheses. *Personality and Social Psychology Bulletin*, *26*(11), 1421-1432.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*(2), 107–123.

Awad, N. F., & 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), 13–28.

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, *38*, 33-42.

Bagozzi, R. P. and Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191-215.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175-1184.

Bandura, A. (1997). *Self-efficacy: The Exercise of Control*, New York: Freeman & Company.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138-150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.

Bargh, J. A., Chaiken, S., Govender, R., & Pratto, F. (1992). The generality of the automatic attitude activation effect. *Journal of Personality and Social Psychology*, *62*(6), 893-912.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from http://firstmonday.org/ojs/index.php /fm/article/view/1394/1312

Barth, S., & de Jong, M. (2017). The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and Informatics* (forthcoming).

Beck, K. H. (1984). The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Social Behavior and Personality: An International Journal*, *12*(2), 121-125.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Benndorf, V., Kübler, D., & Normann, H. T. (2015). General privacy concerns, voluntary disclosure of information, and unraveling: An experiment. *European Economic Review*, *75*, 43-59.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*, *117*(1), 25-27.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, *30*(4), 805-825.

Bohner, G., Moskowitz, G. B., & Chaiken, S. (1995). The interplay of heuristic and systematic processing of social information. In W. Stroebe & M. Hewstone (Eds.), *European Review of Social Psychology* (Vol. 6, pp. 33–68). Chichester, UK: Wiley.

Bornemann, T., & Homburg, C. (2011). Psychological distance and the dual role of price. *Journal of Consumer Research*, *38*(3), 490-504.

Brislin, R.W., Lonner, W.J., & Thorndike, E.M. (1973). *Cross-cultural Research Methods*. New York: Wiley.

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research*, *5*(1), 62-70.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Interactive Marketing*, *11*(3), 44-57.

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013, May). Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 189-200). ACM.

Cenfetelli, R. T. (2004). Inhibitors and enablers as dual factor concepts in technology usage. *Journal of the Association for Information Systems*, *5*(11-12), 472-492.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly*, *33*(4), 689-707.

Chaiken, S., & Baldwin, M. W. (1981). Affective-cognitive consistency and the effect of salient behavioral information on the self-perception of attitudes. *Journal of Personality and Social Psychology*, *41*(1), 1–12.

Chaiken, S., Liberman, A., & Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. In J. S. Uleman & J. A. Bargh (Eds.), *Unintended Thought* (pp. 212–252). New York: Guilford.

Chaiken, S., Pomerantz, E. M., & Giner-Sorolla, R. (1995). Structural consistency and attitude strength. *Attitude Strength: Antecedents and Consequences*, 387-412.

Chau, P. Y., & Hu, P. J. H. (2001). Information technology acceptance by individual professionals: A model comparison approach. *Decision Sciences*, *32*(4), 699-719.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2-3), 181–202.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, *11*(3), 395-416.

Conner, M., Sparks, P., Povey, R., James, R., Shepherd, R., & Armitage, C. J. (2002). Moderator effects of attitudinal ambivalence on attitude–behaviour relationships. *European Journal of Social Psychology*, *32*(5), 705-718.

Cox, D. N., Koster, A., & Russell, C. G. (2004). Predicting intentions to consume functional foods and supplements to offset memory loss using an adaptation of protection motivation theory. *Appetite*, *43*(1), 55-64.

Culnan, M. (1993). How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*(3), 341–363.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342.

Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

DeMarree, K. G., Wheeler, S. C., Briñol, P., & Petty, R. E. (2014). Wanting other attitudes: Actual–desired attitude discrepancies predict feelings of ambivalence and ambivalence consequences. *Journal of Experimental Social Psychology*, *53*, 5-18.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, *34*(2), 373-396.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, *23*(2), 97-102.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behavior & Information Technology*, *23*(6), 413–422.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, *10*(2), 7-29.

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

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet general privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295-316.

Eagly, A. H., & Chaiken, S. (1993). *The Psychology of Attitudes*. Fort Worth, TX: Harcourt Brace Jovanovich.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of general privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57-74.

Eppright, D. R., Tanner Jr, J. F., & Hunt, J. B. (1994). Knowledge and the ordered protection motivation model: Tools for preventing AIDS. *Journal of Business Research*, *30*(1), 13-24.

Fazio, R. H., & Williams, C. J. (1986). Attitude accessibility as a moderator of the attitude–perception and attitude–behavior relations: An investigation of the 1984 presidential election. *Journal of Personality and Social Psychology*, *51*(3), 505-514.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Flender, C., & Müller, G. (2012, June). Type indeterminacy in privacy decisions: the privacy paradox revisited. In J.R. Busemeyer, F. Dubois, A. Lambert-Mogiliansky, & M. Melucci (Eds.), *Quantum Interaction* (pp. 148-159). Springer.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Forgas, J. P. (2011). Affective influences on self-disclosure: mood effects on the intimacy and reciprocity of disclosing personal information. *Journal of Personality and Social Psychology*, *100*(3), 449-461.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Fowler, F. J. *Survey Research Methods*, Thousand Oaks, CA: Sage, 1993.

Fukuyama, F. (1995). *Trust: The Social Virtues and The Creation of Prosperity*. New York: Free Press.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 91-109.

Glasman, L. R., & Albarracín, D. (2006). Forming attitudes that predict future behavior: A meta-analysis of the attitude-behavior relation. *Psychological Bulletin*, *132*(5), 778-822.

Götz, O., Liehr-Gobbers, K., and Krafft. M. (2010). Evaluation of structural equation models using the partial least squares (PLS) approach. In V. E. Vinzi, W. W. Chin, J. Henseler, & H. Wang (Ed.), *Handbook of Partial Least Squares* (pp. 691-711). Berlin: Springer Handbooks of Computational Statistics.

Griffith, D. A., Hu, M. Y., & Ryans, J. K. (2000). Process standardization across intra-and inter-cultural relationships. *Journal of International Business Studies*, *31*(2), 303-324.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19-28.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.

Hargittai, E. (2009). An update on survey measures of web-oriented digital literacy. *Social Science Computer Review*, *27*(1), 130-137.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hofstede, G. (1983). The cultural relativity of organizational practices and theories. *Journal of International Business Studies*, *14*(2), 75-89.

Hofstede, G. *Cultures and Organizations: Software of the Mind: Intercultural.* London: HarperCollins, 1994.

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

Hsu, C. W. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review*, *30*(5), 569-586.

Hu, L. T., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods*, *3*(4), 424-453.

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

IdentityForce (2017). 2017 Data breaches – The worst so far (https://www.identityforce.com/blog/2017-data-breaches accessed October 12, 2017).

Jensen, M., & Meckling, W. H. (1972). The theory of the firm: Managerial behavior, agency costs and ownership structure, *Journal of Financial Economics*, *3*(4), 305-360.

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Jonas, K., Diehl, M., & Brömer, P. (1997). Effects of attitudinal ambivalence on information processing and attitude-intention consistency. *Journal of Experimental Social Psychology*, *33*, 190-210.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387-402.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Kehr, F., Wentzel, D., & Kowatsch, T. (2014). Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure. In *Proceedings of International Conference on Information Systems*, Auckland, New Zealand

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163-1173.

Kettinger, W. J., & Lee, C. C. (2005). Zones of tolerance: Alternative scales for measuring information systems service quality. *MIS Quarterly*, *29*(4), 607-623.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, *24*(4), 13-45.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, *13*(7), 546-580.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Korzaan, M., & Boswell, K. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *The Journal of Computer Information Systems*, *48*(4), 15–24.

Krasnova, H., Veltri, N. F., & El Garah, W. (2014). Effectiveness of justice-based measures in managing trust and privacy concerns on social networking sites: An intercultural perspective. *CAIS*, *35*, 4.

Krosnick, J. A., Boninger, D. S., Chuang, Y. C., Berent, M. K., & Carnot, C. G. (1993). Attitude strength: One construct or many related constructs? *Journal of Personality and Social Psychology*, *65*(6), 1132–1151.

Latham, G. P., Winters, D. C., & Locke, E. A. (1994). Cognitive and motivational effects of participation: A mediator study. *Journal of Organizational Behavior*, *15*(1), 49-63.

Leung, K. (1987). Some determinants of reactions to procedural models for conflict resolution: A cross-national study. *Journal of Personality and Social Psychology*, *53*(5), 898-908.

Leung, K., & Tong, K. K. (2004). Justice across cultures: A three-stage model for intercultural negotiation. In M. Gelfand & J. M. Brett (Eds.), *Handbook of Negotiation and Culture* (pp. 313–333). Stanford, CA: Stanford University Press.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, Y. (2012). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 453-496.

Lian, J. W., & Lin, T. M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior*, *24*(1), 48-65.

Liberman N., Trope Y., & Stephan E. (2007). Psychological distance. In A.W. Kruglanski & E. T. Higgins (Eds.), *Social Psychology: Handbook of Basic Principles*. Vol. 2 (pp. 353–383). New York, NY: Guilford Press.

Liberman, N., & Förster, J. (2009). Distancing from experienced self: How global-versus-local perception affects estimation of psychological distance. *Journal of Personality and Social Psychology*, *97*(2), 203-216.

Liberman, N., Sagristano, M. D., & Trope, Y. (2002). The effect of temporal distance on level of mental construal. *Journal of Experimental Social Psychology*, *38*(6), 523-534.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163-200.

Luttrell, A., Petty, R. E., & Briñol, P. (2016). Ambivalence and certainty can interact to predict attitude stability over time. *Journal of Experimental Social Psychology*, *63*, 56-68.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572-585.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479.

Maio, G. R., Bell, D. W., & Esses, V. M. (1996). Ambivalence and persuasion: The processing of messages about immigrant groups. *Journal of Experimental Social Psychology*, *32*(6), 513-536.

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

Melamed, S., Rabinowitz, S., Feiner, M., Weisberg, E., & Ribak, J. (1996). Usefulness of the protection motivation theory in explaining hearing protection device use among male industrial workers. *Health Psychology*, 15(3), 209-215.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, *38*(12), 65-74.

Milliken, F. J. (1987). Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Academy of Management Review*, *12*(1), 133-143.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29.

Nam, C., Song, C., Lee, E., & Park, C. I. (2006). Consumers' privacy concerns and willingness to provide marketing-related personal information online. *Advances in Consumer Research*, *33*, 212-218.

Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection motivation and risk communication. *Risk Analysis*, *20*(5), 721-734.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, *38*(4), 63-77.

Palmer, C. G. (1996). Risk perception: An empirical study of the relationship between worldview and the risk construct. *Risk Analysis*, *16*(5), 717-723.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, 40(2), 215–236.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105–136.

Pedersen, D. M. (1987). Relationship of personality to privacy preferences. *Journal of Social Behavior & Personality*. *22*(2), 267-274.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123-205.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, *19*(2), 181-195.

Raden, D. (1985). Strength-related attitude dimensions. *Social Psychology Quarterly*, *48*, 312–330.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339-362.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*, 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology* (pp. 153–176). New York: Guilford.

Rosenberg, M. J. (1960). A structural theory of attitude dynamics. *The Public Opinion Quarterly*, *24*(2), 319–340.

Rust, R. T., & Huang, M. H. (2014). The service revolution and the transformation of marketing science. *Marketing Science*, *33*(2), 206-221.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, *32*(2), 344-354.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, *13*(4), 24-38.

Sheehan, K., & Hoy, M. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, *19*(1), 62–73.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review*, *17*(1), 9-38.

Smit, E. G., Van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15-22.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisiplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–197.

Smith, T. W., & MacKenzie, J. (2006). Personality and risk of physical illness. *Annual Review of Clinical Psychology*, *2*, 435-467.

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

Sparks, P., Conner, M., James, R., Shepherd, R., & Povey, R. (2001). Ambivalence about health-related behaviours: An exploration in the domain of food choice. *British Journal of Health Psychology*, *6*(1), 53-68.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in second generation e-commerce: Privacy preferences versus actual behavior. Pp. 38–47 in *Proceedings of the Third ACM Conference on Electronic Commerce*, edited by Michael P. Wellman and Yoav Shoham. New York: Association for Computing Machinery.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, *38*(2), 355-378.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36-49.

Sue-Chan, C., & Ong, M. (2002). Goal assignment and performance: Assessing the mediating roles of goal commitment and self-efficacy and the moderating role of power distance. *Organizational Behavior and Human Decision Processes*, *89*(2), 1140-1161.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. *Computers in Human Behavior*, *29*(3), 821-826.

Taddicken, M. (2014). The 'Privacy Paradox'in the social web: The impact of general privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248-273.

Tata, J. (2005). The influence of national culture on the perceived fairness of grading procedures: A comparison of the United States and China. *The Journal of Psychology*, *139*(5), 401-412.

Tedeschi, B. (2002). Everybody Talks about Online Privacy, but Few Do Anything about It. *New York Times*, June 3.

Terry, D. J. (1994). Determinants of coping: The role of stable and situational factors. *Journal of Personality and Social Psychology*, *66*(5), 895-910.

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

Thompson, M. M., Zanna, M. P., & Griffin, D. W. (1995). Let's not be indifferent about (attitudinal) ambivalence. In R. E. Petty & J. A. Krosnick (Eds.), *Attitude Strength: Antecedents and Consequences* (pp. 361-386). Mahwah, NJ: Lawrence Erlbaum

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review*, *117*(2), 440-463.

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology*, *17*(2), 83-95.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20-36.

Ullman, J. B. (2006). Structural equation modeling: Reviewing the basics and moving forward. *Journal of Personality Assessment*, *87*(1), 35-50.

Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2). Retrived from www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444.

Weber, E. U., & Hsee, C. (1998). Cross-cultural differences in risk perception, but cross-cultural similarities in attitudes towards perceived risk. *Management Science*, *44*(9), 1205-1217.

Williamson, O. E. (1988). The logic of economic organization. *Journal of Law, Economics, & Organization*, *4*(1), 65-93.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. Research-in-progress. *Thirty-third International Conference on Information Systems*, Orlando, FL.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, *19*(2-3), 137-149.

Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of 29th International Conference on Information Systems*, 14–17.

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

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

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710-722.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior*, *11*(6), 763-765.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy parad006Fx revisited. *Information, Communication & Society*, *16*(4), 479-500.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, *16*(4), 53-90.

Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. *Decision Support Systems*, *54*(2), 1085-1091.

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158-167.