THREE RESEARCH ESSAYS ON ONLINE USERS’ CONCERNS

AND WEB ASSURANCE MECHANISMS

Seyed Mohammadreza Mousavizadeh Kashipaz

Dissertation Prepared For the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

August 2016

APPROVED:

Dan J. Kim, Major Professor
Chang E. Koh, Committee Member
Audhesh Paswan, Committee Member
Robert Pavur, Committee Member and Ph.D.
Program Coordinator
Mary C. Jones, Chair of the Department of
Information Technology and
Decision Sciences
Marilyn Wiley, Dean of the College of
Business
Victor Prybutok, Vice Provost of the Toulouse
Graduate School

Mousavizadeh Kashipaz, Seyed Mohammadreza. *Three Research Essays on Online Users' Concerns and Web Assurance Mechanisms*. Doctor of Philosophy (Business Computer Information Systems), August 2016, 115 pp., 11 tables, 6 figures, references, 254 titles.

Online users struggle with different concerns whenever they use information systems. According to Miyazaki and Fernandez (2001), there are three important categories of concerns for online users: privacy concern, third party fraudulent behavior concern ("system security"), and online website fraudulent behavior concern ("security"). Kim, Sivasailam, and Rao (2004) proposed a similar categorization for web assurance dimensions. They argue that online websites are supposed to address users' privacy, security, and business integrity concerns to decrease user concerns. Although several researchers tried to answer how different factors affect these concerns and how these concerns affect users' behavior, there are so many ambiguities and contradictions in this area. This Essay I in this work develops a comprehensive map of the role of online privacy concern to identify related factors and categorize them through an in-depth literature review and conducting meta-analysis on online privacy concern. Although users have concerns about their privacy and security, there is still growth in the number of internet users and electronic commerce market share. One possible reason is that websites are applying assurance mechanisms to ensure the privacy of their users. Therefore, it could be an interesting research topic to investigate how privacy assurance mechanisms affect users concern and, consequently, their behavior in different concerns such as e-commerce and social networking sites. Different types of web assurance mechanisms are used by websites. The most prevalent among these assurance mechanisms include web assurance seals and assurance statements and privacy customization features. Essay II and III aims to address how these mechanisms influence

e-commerce and social networking sites users’ behavior. Essay II applies the procedural fairness theory by Lind and Tyler (1988) to explain how and why the web assurance mechanisms affect consumers’ perceived risks. Essay III addresses the issue of self-disclosure on social networking sites. Applying protection motivation theory, this study aims to evaluate the effect of web assurance mechanisms on online privacy concern and self-disclosure behavior on the social networking sites.

ACKNOWLEDGEMENTS

First, I would like to acknowledge the guidance and knowledge of my dissertation chair, Dr. Dan Kim. It has been a great pleasure working with him on this dissertation and learning from him along the entire Ph.D. program. Next, I would like to thank my dissertation committee members, Dr. Chang Koh, Dr. Audhesh Paswan, and Dr. Robert Pavur, for their very helpful feedbacks and support. Finally, I would like to thank my wife, family and friends, from near or far, for their love and unconditional support. I could never complete this milestone without having you and your thoughts.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

PROLOGUE

Online users struggle with different concerns whenever they use information systems. According to Miyazaki and Fernandez (2001), there are three important categories of concerns for online users: privacy concern, third party fraudulent behavior concern ("system security"), and online website fraudulent behavior concern ("security"). D. J. Kim, N. Sivasailam, and H. R. Rao (2004) proposed a similar categorization for web assurance dimensions. They argue that online websites are supposed to address users' privacy, security, and business integrity concerns to decrease user concerns. Although several researchers tried to answer how different factors affect these concerns and how these concerns affect users' behavior, there are so many ambiguities and contradictions in this area.

As one of the most important concerns for online users, online privacy concern (OPC) has been studied by several researchers in the literature. Information privacy has been recognized as an important issue in management, and its significance will continue to escalate as the value of information continues to grow (Mason, 1986). According to Rainie, Kiesler, Kang, and Madden (2013), more than 50% of Internet users express that they are concerned with their information privacy; 66% of them posit that current law does not protect them against privacy threats. OPC continues to drive customers away from online businesses (Kukar-Kinney & Close, 2010) and become an important issue for social networking sites (SNS) to acquire more users.

Previous studies revealed that a variety of factors affect OPC in different contexts. Some of these factors include individual characteristics (Junglas, Johnson, & Spitzmüller, 2008; Morton, 2013), web assurance mechanisms (Milne & Culnan, 2004; Wu, Huang, Yen, & Popova, 2012), website reputation and familiarity (Li, 2014a), trust (Taylor, Davis, & Jillapalli, 2009), and more.

Moreover, prior studies found that many different variables are affected by OPC. Some of these variables include behavioral intention (Van Slyke, Shim, Johnson, & Jiang, 2006; Wu et al., 2012), attitude toward a behavior (Arpaci, Kilicer, & Bardakci, 2015), trust (Castañeda & Montoro, 2007; Yang & Miao, 2008), and more. Although these studies were aimed at enhancing our knowledge about the role of privacy concern on the internet, our understanding still remains fragmented for several reasons. First, there are some contradictions in the findings of previous studies. For example, some studies suggest that trust negatively affects privacy concern (Taylor et al., 2009), whereas others find that trust is negatively affected by OPC (Castañeda & Montoro, 2007). Second, findings of previous studies suggest diverse antecedents for OPC. Thus, there is no consistent view of the Information assurance process specifically for OPC in the literature. Therefore, one of the important questions in the literature that should be addressed by researchers is what the antecedents and consequences of OPC are.

Although users have concerns about their privacy and security, there is still growth in the number of internet users and electronic commerce market share. One possible reason is that websites are applying assurance mechanisms to ensure the privacy of their users. Therefore, it could be an interesting research topic to investigate how privacy assurance mechanisms affect users concern and, consequently, their behavior. Different types of web assurance mechanisms are used by websites. The most prevalent among these assurance mechanisms include web assurance seals and assurance statements. According to Kim, Steinfield, and Lai (2008) web assurance seals are signs that are provided by a third party to assure users about website security, privacy, and the business integrity of that website. Assurance statement refers to “mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website" (Bansal, Zahedi, & Gefen, 2015a). Assurance mechanisms have been studied in e-commerce context with different research constructs (Bansal et al., 2015a): most studies explore the effect of privacy assurance statement as a primary privacy assurance mechanism on trust in e-commerce websites (Liu, Marchewka, & Ku, 2004; McKnight, Choudhury, & Kacmar, 2002; McKnight, Kacmar, & Choudhury, 2004; Wu et al., 2012); some others investigate its effect on intention to disclose information (Meinert, Peterson, Criswell, & Crossland, 2006; Peterson, Meinert, Criswell, & Crossland, 2007; Wang, Beatty, & Foxx, 2004). Despite these ongoing studies, there is a lack of theory oriented studies that addressed the role of web assurance mechanisms in e-commerce and SNS contexts. Thus, this study aims to conduct theory oriented research to address two questions: (1) how web assurance mechanisms affect online consumers' concerns and consequently the users' behavioral intention to shop online, (2) How web assurance mechanisms influence SNS users' privacy concerns and sharing behavior.

This dissertation contains three essays.

Essay I aims to develop a comprehensive map of the role of OPC to identify related factors and categorize them through an in-depth literature review and conducting meta-analysis on OPC. More specifically, this study aims to address the following research questions: (1) which of the antecedents of OPC are stronger based on previous research findings, and (2) What is the actual role of variables such as trust and risk that have contradictory role in the assurance literature.

Essay II is motivated by the lack of integrated view on how web assurance mechanisms influence consumers' perceived concerns regarding online shopping. This study applies the procedural fairness theory by Lind and Tyler (1988) to explain how and why the web assurance mechanisms affect consumers’ perceived risks. In addition, this study suggested three categories of risks that online consumers perceive in online shopping based upon the findings of Miyazaki and Fernandez (2001). This essay provides a holistic view on how web assurance mechanisms affect purchase intention by consumers’ perceived concerns. Synthesizing prior studies, it focuses on three focal consumers concerns to (1) theorize their potential associations to consumers’ purchase intention and (2) explore the website features (i.e., third-party assurance seals and website assurance statements) that contribute to the mitigation of these concerns.

Essay III addresses the issue of self-disclosure on SNS. Applying protection motivation theory (PMT), this study aims to evaluate the effect of web assurance mechanisms on OPC and self-disclosure behavior on the SNS. This study explains this effect by suggesting a risk calculus process and argues that SNS users’ level of OPC is the result of evaluating threats of self-disclosure and users’ perceived coping ability against these threats. Essay III has two main objectives. First, to study how privacy assurance mechanisms affect SNS users’ protection motivation by applying protection motivation theory as the theoretical lens. Second, to investigate the influence of privacy concern as part of the PMT on SNS users’ protection motivation and self-disclosure.

ESSAY I: A LITERATURE REVIEW ON ONLINE PRIVACY CONCERNS: A META-ANALYSIS APPROACH

Introduction

The information assurance literature suggests privacy, security, and business integrity as the three important dimensions of Information assurance (D. J. Kim et al., 2004). Whenever users interact with a website they have different levels of concerns about their privacy, security, and business integrity of the website owners. However, there is no assurance requirements mandated by law in the online arena for users' concern. Thus, online customers have a serious concern about the privacy of their information whenever they do a transaction on the internet (Carlos Roca, José García, & José de la Vega, 2009). Recent reports revealed that consumers' online privacy concerns (OPC) are increasing (Pingitore, Meyers, Clancy, & Cavallaro, 2013). Furthermore, privacy and security concerns are not limited to online transactions. Previous studies reported these concerns as important concerns of users on social networking websites (SNS) as well (e.g., Jiang, Heng, & Choi, 2013; Lankton & Tripp, 2013; Tsoi & Chen, 2011). A recent study shows that more than 50% of internet users are concerned about their privacy. Among these users, 66% believe that the current law is not able to protect them against privacy threats (Rainie et al., 2013). Another study reports that about 70% of internet users are concerned about disclosure of their information without their permission. Moreover, about 50% of these users reported that they are concerned about their online activity data being used to deny employment or loan applications (Rainie & Anderson, 2014). Online websites need to know users concerns about their privacy and create some mechanisms to eliminate, or at least minimize, these concerns.

OPC has been investigated in diverse disciplines such as Information Systems (Hui, Teo, & Lee, 2007; Kim, Steinfield, et al., 2008), Marketing (Luo, 2002; Sheehan & Hoy, 2000), Accounting (Duh, Sunder, & Jamal, 2002; Kauffman, Lee, Prosch, & Steinbart, 2011), and many others. In addition, the concept of OPC has been discussed across many contexts such as electronic commerce (Liu, Marchewka, Lu, & Yu, 2005; Van Slyke et al., 2006), mobile commerce (Okazaki, Li, & Hirose, 2009; Tao, 2008), SNS (Jiang et al., 2013; Lankton & Tripp, 2013; Tsoi & Chen, 2011), organizations (Shawn F, Ryan T, & Ronald E, 2010; Smith, Milberg, & Burke, 1996), and healthcare (Bansal & Davenport, 2010). Previous studies revealed that a variety of factors affect OPC in different contexts. Some of these factors include individual characteristics (Junglas et al., 2008; Morton, 2013), web assurance mechanisms (Milne & Culnan, 2004; Wu et al., 2012), website reputation and familiarity (Li, 2014a), and trust (Taylor et al., 2009). Moreover, prior studies found that many different variables are affected by OPC. Some of these variables include behavioral intention (Van Slyke et al., 2006; Wu et al., 2012), attitude toward a behavior (Arpaci et al., 2015), and trust (Castañeda & Montoro, 2007; Yang & Miao, 2008).

Although these studies were aimed at and, to some extent, able to enhance our knowledge about the role of privacy concerns on the internet, our understanding still remains fragmented. This is due to several factors. First, there are some contradictions in the findings of previous studies. For example, some studies suggest that trust negatively affects privacy concern (Taylor et al., 2009), whereas others find that trust is negatively affected by OPC (Castañeda & Montoro, 2007). The actual role of risk in this context is still ambiguous. Although, several studies in the literature suggested risk as a consequence of OPC, some researchers argue that users' privacy concern is an outcome of their perceived risk. Second, the role of OPC is not the same in different contexts. For instance, some researchers argue that OPC has a moderating role (Bansal et al., 2015a). Other researchers suggest that OPC directly affects individuals' behavioral intention (Lin & Liu, 2012; Yang & Wang, 2009). In addition, several studies show that OPC has an indirect effect on behavioral intention (Castañeda & Montoro, 2007; Liu et al., 2005). Finally, findings of previous studies suggest diverse antecedents for OPC. Thus, there is no consistent view of the Information assurance process specifically for OPC in the literature.

To explore these research gaps, this study develops a comprehensive map of the role of OPC that aims to identify related factors and categorize them through an in-depth literature review. More specifically this study addresses the following research questions:

- Which of the antecedents and consequences of OPC are more important and how much is the relationship strength of each?
- What is the actual role of variables such as trust and risk that have contradictory role in the assurance literature?

Although, meta-analysis as a knowledge accumulation technique has become a popular research approach in IS research, this approach is still underutilized compared with other disciplines such as psychology (Hwang & Schmidt, 2011). Diversities and contradictions in the previous research findings urge this study to adapt a meta-analysis approach to address the contradictory findings.

Literature Review

Online privacy concern has been studied in several contexts such as e-commerce, SNS, healthcare, finance, and online communications. For example, in the e-commerce context, the majority of studies focused how online consumers' concerns about privacy are influenced by different factors and how OPC affects online intention or behavior regarding the e-commerce website or the product and services that the website sells (e.g., Eastlick, Lotz, & Warrington, 2006; Li, 2014a). Those studies that concentrate on OPC in the SNSs context mostly investigate how different factors influence SNS users perceived OPC and how this perception influences their intention or behavior regarding using these websites or disclosing information in them (Jiang et al., 2013; Tan, Qin, Kim, & Hsu, 2012).

Different studies defined privacy frequently based on the context and maturity of the research about privacy. According to Smith, Dinev, and Xu (2011), privacy is a multidimensional and dynamic concept which overlaps with some other related concepts such as confidentiality, anonymity, secrecy, and security. Therefore, defining privacy is complicated and difficult. Although, the definition of privacy is very complicated, different researchers tried to explain the concept of privacy as precisely as they could. Culnan and Bies (2003, p. 326) developed one of the most frequently used definitions of privacy. They defined privacy as “the ability of individuals to control the terms under which their personal information is acquired and used” (p. 326).

Since it is almost impossible to measure privacy itself, almost all empirical studies utilized online privacy concern as a proxy of privacy (Smith et al., 2011). Smith et al. (1996), defined online privacy concern with four dimensions: collection, errors, secondary use, and unauthorized access to information. OPC as a dimensional concept has been investigated by several studies in different contexts (e.g., Okazaki et al., 2009; Osatuyi, 2015; Shawn F et al., 2010). According to the Smith et al. (2011) APCO macro model, the OPC literature focused on Antecedents and consequences for OPC in different contexts. Thus, in this section we focused on how literature investigates these two broad categories of factors.

Antecedents of Online Privacy Concern

Several studies investigated antecedents of online privacy concern in different contexts and different points of view. According to Smith et al. (2011), there are five important categories of antecedents for OPC: privacy experiences, privacy awareness, personality differences, demographic differences, and culture and climate. A large number of studies found users' personality characteristics as important antecedents of online privacy concern. According to Junglas et al. (2008) personality traits such as agreeableness, consciousness, emotional stability, extraversion, and openness are important indicators of OPC for SNS users. Computer anxiety and tech-savvy are other characteristics of users that influence their concern about privacy (Li, 2014b; Osatuyi, 2015; Spake, Zachary Finney, & Joseph, 2011). Risk propensity defined as whether a person is risk-seeker, risk-neutral, or risk-averse (Yao-Hua Tan, 2000), was suggested as another personality characteristic that affect OPC (Xu, Teo, & Tan, 2005).

Users' perceptions about different components of an online environment were suggested as antecedents for OPC. Users' perception about the website itself could be an indicator for their level of OPC. For instance, perceived playfulness of a website influences user's privacy concern (Jung, McKnight, Jung, & Lankton, 2011). Based upon privacy calculus framework, perceived benefits and risks of users from using online environment affect their OPC (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Additionally, previous research showed that users with higher level of self-efficacy have lower level of OPC (Yao, Rice, & Wallis, 2007; Youn, 2009). Demographics were also studied by several researchers as important antecedents of OPC. According to Youn (2009), Mohamed and Ahmad (2012), and Fogel and Nehmad (2009) women have more concern about their privacy when they need to disclose their personal information compared to men.

Previous studies revealed that users' privacy awareness influences their privacy concern (Brecht, Fabian, Kunz, & Mueller, 2011; Zlatolas, Welzer, Heričko, & Hölbl, 2015). Malhotra, Kim, and Agarwal (2004) and Phelps, Nowak, and Ferrell (2000) defined privacy awareness as the extent to which online users are aware of privacy practices. Furthermore the previous negative experiences of internet users regarding their privacy affect the OPC. Users who have history of any type of privacy issue perceive more concern about their information privacy (Bansal, 2008; Okazaki et al., 2009).

Third parties' activities were investigated as important factors that influence users' OPC. For example, Wirtz, Lwin, and Williams (2007) suggests that users who perceive that there is sufficient legal regulation in place to protect their privacy have less concern about their privacy. In addition, previous research suggests that the third party assurance seals on the websites negatively affects their privacy concern since users perceive that a third party controls all the privacy related activities that the website performs (Xu et al., 2005). Government as another third party in the online environment may perform some activities that affect online users' privacy concern. According to Wirtz et al. (2007) business policies and government regulations affect users' OPC.

Consequences of Online Privacy Concern

OPC may ultimately affect different aspects of online users, websites, or even third parties' behavior but the existing research found diverse paths to this ultimate behavior. According to Smith et al. (2011), OPC influences regulations, behavioral reactions, trust, and perceived risks. Although the consequences of OPC have been studied by so many researchers, there is so much diversity among the findings in the literature. This diversity is not only limited to the consequences of OPC but also exists about how OPC affects the outcomes.

Several researches suggest that OPC influences users' behavior or intention to perform a behavior directly or indirectly (e.g., Li, 2014a; Tan et al., 2012; Yang, 2012). According to Lankton and Tripp (2013) users who perceive high levels of OPC have less intention to continue to use an online website. Furthermore, some other studies suggest that OPC affect users' intention to disclose their information on the website instead of using the website (Osatuyi, 2015; Sun, Wang, Shen, & Zhang, 2015). Although, these studies argue that OPC affect intention, some other researchers believe that OPC can directly influence users' behavior. For example, Zhou and Li (2014) suggests that online consumers' OPC negatively affects their e-commerce website use continuance. Another consequence for OPC is information disclosure behavior on a website (Becker & Pousttchi, 2012; Zhao, 2012).

Some researchers believe that OPC affects users' behavior in three different ways: fabricate, protect, and withholding. Fabricate refers to users' effort to provide wrong information about their identity to prevent sharing their identity with unauthorized people. Protect behavior refers to using technology to prevent potential privacy issues. Finally, withholding refers to users' refusal to provide information to the websites (Keith, Thompson, Hale, Lowry, & Greer, 2013). Therefore users minimize their cost by applying any of these strategies whenever they have certain levels of OPC (Lwin, Wirtz, & Williams, 2007).

Perceived risks of using websites has been suggested by so many researchers as an important outcome for OPC. Applying the privacy calculus framework, these studies argue that OPC affect users perceived risk and then users decide to perform a behavior based on the calculus between this risk component and the benefit they perceive (Keith et al., 2013; Smith et al., 2011). Finally, one of the most frequent consequences of OPC among the existing studies is trust (e.g., Bansal & Gefen, 2010; Eastlick et al., 2006; Wu et al., 2012). Trust in an online environment refers to “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (Mayer, Davis, & Schoorman, 1995, p. 712). In fact, most of the researchers who studied the effect of OPC on trust argue that OPC can affect users’ behavioral reaction by influencing their perceived trust.

Antecedence/Consequences of Online Privacy Concern

Current research found some contradictory results about the antecedents and consequences of OPC. Although the majority of the researchers suggests that trust is an outcome of users’ OPC, findings of several studies suggest that trust can be an antecedents for the OPC (Miltgen & Smith, 2015; Xu et al., 2005). Procedural justice, defined as “degree to which an Internet user perceives that online companies give him or her procedures for control of information privacy and make him or her aware of the procedures” (Son & Kim, 2008, p. 511), is another factor that has an unclear role in the existing literature. According to Krasnova and Veltri (2010) and Wirtz et al. (2007), perceived procedural justice in an online environment influences users’ privacy concern. Interestingly, Park (2009) argues that OPC negatively influence users’ perception about the procedural justice of a website.

Integrated Framework of Online Privacy Concern Conceptual Model

To develop an integrated model to study OPC, this study first focuses on the existing processes in online interactions between users and websites. Previous researches on OPC suggested website, user, and third parties (e.g., government) as three important entities in the study of OPC (Junglas et al., 2008; Lankton & Tripp, 2013; Morton, 2013). Going deeper in OPC literature, users process different pieces of information to end up with a specific level of privacy concern with a website. As shown in Figure 1, Third parties such as government and web assurance providers provide sources of information for users that affect their perceptions of privacy (Hoffman, Novak, & Peralta, 1999; Kim, Steinfield, et al., 2008). Furthermore, websites provide several cues for the users that affect their perception. For example a website's reputation is a cue for users that affects their perceived privacy concern (Eastlick et al., 2006). Another input for the process is the users' characteristics, beliefs, and experiences. Each online user has some specific characteristics that affect his/her online privacy concern (Junglas et al., 2008). The process of these different pieces of information and cues leads to several consequences such as self-disclosure and purchase intention.

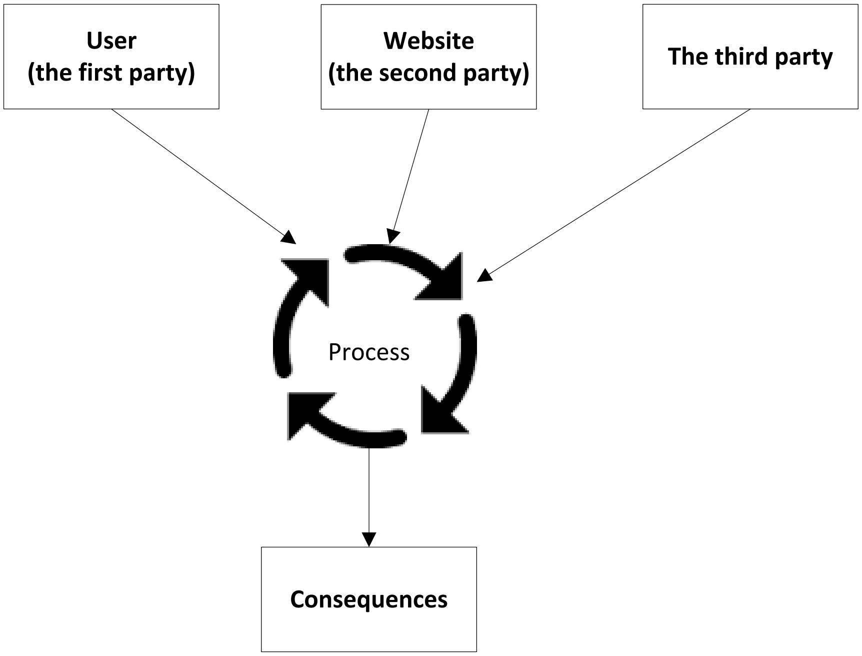


Figure 1. Conceptual model of OPC

Based on the in-depth literature review to identify and categorize major OPC related factors. This study specifies and categorizes the variables that exists in each category in the conceptual model.

Antecedents

Website

OPC literature investigates the effect of website's characteristics in this domain. According to Eastlick et al. (2006), websites' reputation affects online consumers privacy concern and trust. Presence of a privacy policy is a factor that affects users' OPC and trust in websites (Bansal et al., 2015a). Moreover, enjoyment is another factor that was suggested as another characteristic of the website that affects OPC (Lankton & Tripp, 2013). Finally, some studies indicated that social structure of a website may influence OPC. For instance, Moscardelli and

Divine (2007) suggestes that online users reporte lower levels of concern when they find informative peers on the website.

User

Online users have several personal characteristics and previous experiences that play an important role in the OPC context. According to Junglas et al. (2008), personality traits such as agreeableness, consciousness, emotional stability, extraversion, and openness are important indicators of OPC for SNS users. Moreover, some other studies suggested that users' demographics, such as gender and age, affect their level of privacy concern (e.g., Chen, Zhang, & Lee, 2013; Moscardelli & Divine, 2007; Zhang, Chen, & Lee, 2013). Additionally, research shows that users with a higher level of self-efficacy have a lower level of OPC (Yao et al., 2007; Youn, 2009).

Third Party

There are several types of third party assurance seals used by websites to ensure their users regarding the effectiveness of these websites' privacy related activities. According to Lala, Arnold, Sutton, and Guan (2002), web assurance seals are mechanisms that websites use to decrease users' OPC. Two aspects of seals have been emphasized by previous research. (1) presence of the seal affect OPC (D. J. Kim et al., 2004) and (2) information quality of the seal (Lala et al., 2002). Government is another party that was investigated in the area of OPC. According to Wirtz et al. (2007), business policies and government regulations affect users' privacy concerns. In addition, culture affects users' privacy concerns. Different cultures may have different concerns regarding their information privacy. For example, a study by Hsu (2006) found that political systems and cultural background affect online users OPC by studying OPC in China, The Netherlands, Taiwan, and the USA.

Consequences

Behavioral Intention

An in-depth review of the literature specified that there are three broad categories of consequences. Although intention was suggested frequently as an outcome, the type of behavior corresponding to the intention is very diverse. In the e-commerce studies OPC has been reported by several researches as a factor that affect online consumers' purchase intention (e.g., Stewart & Segars, 2002; Taylor et al., 2009; Yang & Miao, 2008). According to the SNS literature, users' privacy concern negatively affects their intention to disclose their personal information (Lo, 2010). The level of privacy concern in online users also affects their intention to use an information system (e.g., Jung, Lankton, McKnight, & Jung, 2012; Xu & Teo, 2004).

Behavior

Online users perform different types of protective responses based on their OPC. According to Wirtz et al. (2007), online users respond in three different ways based upon their privacy concern: fabricate, protect, withholding. In addition, continuing to use (Zhou & Li, 2014), online spending (Akhter, 2012), self-disclosure (Jiang et al., 2013), and information disclosure (Yang, 2012) were suggested as other behavioral consequences of OPC in previous research.

Methodology

Data Collection

This study followed the procedures suggested by Hedges and Olkin (1985) and Hunter and Schmidt (2004) to conduct the meta- analysis. Different strategies were applied to identify and acquire a complete and relevant collection of published and unpublished studies. An initial search was conducted in Google Scholar by using all the related keywords to the OPC such as online privacy, website, and privacy concern. Next, a similar search was performed in various online databases that contained studies in the areas of communication, information systems, marketing, and decision sciences. These databases include JSTOR, ScienceDirect, Elsevier, Emerald, IEEE Xplore, EBSCO, and ACM. Articles were found from a variety of journals such as *Computers in Human Behavior, Information and Management, Decision Support Systems, MIS Quarterly, Information Systems Research, Electronic Commerce Research and Applications, Journal of Information Privacy and Security, Journal of Advertising, Tourism Management, Information Technology and Management, Electron Commerce Research, Journal of Business Research, Journal of the Academy of Marketing Science*. The next step was to scan the conference proceedings and dissertations related to OCR. This study searched International Conference of Information Systems, Americas Conference on Information Systems, Pacific Asia Conference on Information Systems, European Conference on Information Systems, and Hawaii International Conference on Systems Sciences Dissertations were searched in ProQuest Dissertations.

The search for the relevant studies resulted in 176 empirical articles. In the next step, studies that measured online privacy concern and correlated it with at least one variable in the context of e-commerce and social media were included in the meta-analysis sample. The next step was to remove all those studies that met one of the following criteria: (1) those studies that used the same data with at least another study, and (2) those studies that did not report the necessary statistics for meta-analysis that will be explained in the next section of this study. The final sample includes 78 studies, with 50 journal articles, 23 conference proceedings, and 5 dissertations. The meta-analysis was conducted on the relationship between OPC and any variable that correlated with OPC. There was 105 different variables in the sample that correlated with OPC. Among these variables, 57 were antecedents and 50 were consequences of OPC. The sample size of the studies ranged from 44 to 2642 (*M* = 433.94, *SD* = 390.64) and these studies were published in 2002 and later.

Data Analysis and Results

We followed the procedure suggested by Hedges and Olkin (1985) to combine estimated effect sizes of the relationships between OPC and other variables. The effect size that was used for the meta-analysis was the zero-order correlation r. For those studies that have not reported the correlation value, the Student's t and F ratios with one degree of freedom in the numerator were converted to correlation applying the formula outlined by Hunter and Schmidt (2004). In those cases that none of these statistic were reported, standardized beta coefficients were converted to *r* by using the procedure suggested by Peterson and Brown (2005).

Although Hedges and Olkin (1985) suggested that correlations overestimate the effect sizes and Fisher z transformed rs can minimize this overestimation, recent studies such as Hunter and Schmidt (2004) note that Fisher z-transformation may cause serious inaccurate results in meta-analysis because this transformation produces an estimate of the mean correlation that is more biased and less accurate than the mean correlation that is produced by untransformed correlations. Therefore, for the purpose of this study we did not used the z-transformated correlations. This study corrected the measurement errors by using the reliability estimates reported by each study (Hunter & Schmidt, 2004). The reason was that the reliability estimates are not the same across all the studies. Cronbach's alpha was used as the estimate for the reliability. In those cases that Cronbach's alphas was not reported the composite reliability estimates of the variables was used.

The corrected weighted mean correlations and their 95 percent confidence intervals were computed by applying the procedure outlined by Hedges and Olkin (1985). The weighted estimates reflect the strength of the relationship between the variable and the meta-analysis variable and the confidence interval explains the interval for the corrected weighted mean correlations. We also computed the 90 percent credible interval to explain distribution of the corrected weighted mean correlations (Whitener, 1990). Confidence interval can be used to examine the significance of the relationship between the two variables in the meta-analysis. Intervals that do not include zero indicate a significant relationship. Credible intervals that are large enough or do not include zero indicate possible moderators (Whitener, 1990).

As another measure of the significance of the variance among correlations, the Q statistic as a homogeneity test was computed. We applied the procedure suggested by Hedges and Olkin (1985) to compute the Q statistic (Formula 2). Q is approximately distributed as a chi-square statistic in which the degrees of freedom equals k (number of studies) minus one. The significance of the Q statistic supports the existence of the moderators. The reason is that Q statistic explains heterogeneity in the residual variances of the correlations.

$$Q = \sum_{i=1}^{k} (n_i - 3)(r_{ci} - r_{c+})$$

$$r_{c+} = w_1 r_{c1} + \cdots + w_k r_{ck}$$

Note. r_c: Corrected correlation, r_{c+}: Weighted average of corrected correlations.

Formula 2. Q-statistics formula

Finally, to examine the robustness of the findings of the meta-analysis the fail-safe N statistic was computed for each of the relationships as suggested by Lipsey and Wilson (2001). This test determines how many studies with zero pairwise correlations are needed to reduce the mean effect size to a specified or criterion level.

Antecedents of Online Privacy Concern

Table 1 summarizes the meta-analysis results for all the antecedents of OPC that existed in at least two studies in our sample to create a general picture of the antecedents of OPC. In order to compare the strength of the relationships the weighted mean correlations should be compared. According to Cohen (1988) Pearson product moment correlations less than .10 are considered as trivial effect sizes, those between .10 and .30 are considered as small effect sizes, those between .30 and .50 are considered medium effect sizes, and those greater than .5 are considered large effect sizes.

The strongest antecedent of OPC with large effect size is computer anxiety (r_c = .66, N = 715). The effect sizes for interaction justice (r_c = -.45, N = 1,214), disposition to privacy (r_c = .44, N = 220), privacy policy (r_c = -.42, N = 2,457), perceived vulnerability (r_c = .40, N = 1,154), perceived anonymity of self (r_c = -.38, N = 316), privacy control (r_c = -.38, N = 1,484), perceived risks (r_c = .38, N = 660), reputation (r_c = -.36, N = 587), regulations (r_c = -.36, N = 1,605), familiarity (r_c = -.34, N = 254), perceived anonymity of others (r_c = .33, N = 316), and negative experience (r_c = .31, N = 1,790) are moderate. Finally, distributive justice (r_c = -.29, N = 977), trust (r_c = -.25, N = 2,598), procedural justice (r_c = -.24, N = 977), agreeableness (r_c = -.24, N = 598), privacy awareness (r_c = .23, N = 1,772), self-efficacy (r_c = -.23, N = 1,297), frequency of use (r_c = -.23, N = 946), and perceived benefits of disclosure (r_c = -.20, N = 330) have small effects on OPC.

The 90% credible intervals were wide, suggesting the presence of moderating effect. Furthermore, Majority of the Q statistics are significant indicating that the distribution of the r_c for corresponding pairwise relationship is heterogeneous and some characteristics other than measurement errors contribute to the overall variance (Lipsey & Wilson, 2001). The fail-safe N values indicate that the weighted mean corrected correlations significantly differ from zero. 5 to 246 studies with an effect size of zero are needed to reduce the mean to a trivial effect size. Therefore, the weighted mean corrected correlations computed are reliable.

Consequences of Online Privacy Concern

As shown in Table 2, users' OPC has a large effect on withholding (r_c = .89, N = 710), deflective behavior (r_c = .84, N = 710), protect (r_c = .67, N = 710), purchase intention (r_c = -.58, N = 728), fabricate (r_c = .56, N = 854), risk (r_c = .53, N = 5,301), and trust (r_c = -.51, N = 7,725). In addition, disruptive behavior (r_c = .42, N = 740), defensive behavior (r_c = .40, N = 740), intention to use (r_c = -.32, N = 5,283), and self-disclosure (r_c = -.32, N = 1,230) are moderately related to OPC. Finally, the analysis results revealed that the effect sizes for the effect of OPC on information disclosure behavior (r_c = -.28, N = 4,823), continue to use (r_c = -.26, N = 721), intention to disclose information (r_c = -.20, N = 2,911), privacy setting use (r_c = .16, N = 1,827), and online spending (r_c = .10, N = 1,858) are small. Similar to the antecedents of OPC, the 90% credible intervals were wide and the majority of the Q statistics were significant suggesting the presence of moderators.

Table 1

Meta-analysis of the antecedents of OPC

Variables	K^a	N^b	r	r_c^d	Std. Deviation	95 % Confidence Interval		90 % Credible Interval		Q statistic	Fail-safe N
						Lower	Upper	Lower	Upper		
User											
Agreeableness	2	598	-0.22	-0.24	0.11	-0.34	-0.13	-0.33	-0.15	3.49	61
Extroversion	2	598	-0.04	-0.04	0.00	-0.18	0.09	-0.14	0.05	0.00	13
Computer anxiety	3	715	0.53	0.66	0.27	0.56	0.77	0.26	1.07	43.31**	246
Disposition to privacy	2	220	0.34	0.44	0.20	0.25	0.64	0.25	0.63	4.13*	109
Internet Experience	4	2,114	0.02	0.02	0.09	-0.05	0.09	-0.12	0.15	18.08**	5
Familiarity	2	254	-0.28	-0.34	0.10	-0.53	-0.15	-0.39	-0.29	1.31	87
Negative experience	4	1,790	0.27	0.31	0.07	0.20	0.40	0.24	0.36	5.83	147
Perceived anonymity of others	2	316	0.29	0.33	0.16	0.20	0.45	0.24	0.41	2.40	79
Perceived anonymity of self	2	316	-0.35	-0.38	0.35	-0.51	-0.26	-0.69	-0.08	11.88**	96
Perceived benefits of disclosure	2	330	-0.15	-0.20	0.077	-0.37	-0.04	-0.29	-0.12	0.94	53
Perceived risks	4	660	0.33	0.38	0.22	0.25	0.51	0.10	0.67	21.57**	141
Perceived vulnerability	3	1,154	0.34	0.40	0.15	0.23	0.57	0.21	0.59	17.79**	147
Privacy awareness	2	1,772	0.20	0.23	0.06	0.16	0.31	0.19	0.28	3.17	57
Privacy control	2	1,484	-0.32	-0.38	0.07	-0.46	-0.30	-0.44	-0.32	3.18	97
Self-efficacy	4	1,297	-0.19	-0.23	0.22	-0.40	-0.06	-0.52	0.06	43.97**	118
Trust	5	2,598	-0.21	-0.25	0.09	-0.43	-0.06	-0.34	-0.16	12.46*	160
Frequency of use	2	946	-0.16	-0.23	0.06	-0.40	-0.06	-0.28	-0.18	0.77	60
Website											
Privacy policy	3	2,457	-0.38	-0.42	0.11	-0.50	-0.34	-0.54	-0.30	15.47**	161

Variables	K[a]	N[b]	r	r_c[d]	Std. Deviation	95 % Confidence Interval		90 % Credible Interval		Q statistic	Fail-safe N
						Lower	Upper	Lower	Upper		
Distributive justice	3	977	-0.25	-0.29	0.08	-0.41	-0.17	-0.34	-0.24	3.51	112
Interaction justice	4	1,214	-0.40	-0.45	0.26	-0.57	-0.33	-0.83	-0.08	65.23**	230
Procedural justice	3	977	-0.21	-0.24	0.11	-0.36	-0.12	-0.37	-0.12	8.10*	94
Reputation	2	587	-0.31	-0.36	0.14	-0.55	-0.17	-0.46	-0.26	3.63	91
Third party											
Regulations	2	1,605	-0.33	-0.36	0.14	-0.44	-0.29	-0.52	-0.21	15.75**	93

Note. *p < .05; ** p < .01

[a] The number of studies. [b] The total sample size. [c] The weighted mean correlation. [d] The weighted mean corrected correlation.

Table 2

Meta-analysis of the consequences of OPC

Variables	K^a	N^b	r	r_c^d	Std. Deviation	95 % Confidence Interval		90 % Credible Interval		Q statistic	Fail-safe N
						Lower	Upper	Lower	Upper		
Intention to use	13	5,283	-0.28	-0.32	0.30	-0.37	-0.27	-0.73	0.09	333.16**	534
Intention to continue to use	3	975	-0.07	-0.08	0.10	-0.19	0.04	-0.16	0.01	5.43	31
Intention to disclose information	9	2,911	-0.17	-0.20	0.16	-0.42	0.01	-0.47	0.06	85.32**	239
Information disclosure behavior	8	4,823	-0.22	-0.28	0.18	-0.37	-0.18	-0.61	0.06	205.84**	284
Purchase intention	2	728	-0.52	-0.58	0.01	-0.67	-0.49	-0.64	-0.53	0.01	148
Self-disclosure	4	1,230	-0.28	-0.32	0.17	-0.45	-0.19	-0.44	-0.20	9.38*	164
Continue to use	2	721	-0.19	-0.26	0.31	-0.37	-0.15	-0.61	0.08	33.09**	67
Defensive behavior	2	740	0.34	0.40	0.02	0.28	0.52	0.33	0.47	0.13	99
Deflective behavior	2	740	0.73	0.84	0.33	0.72	0.96	0.46	1.21	38.17**	208
Disruptive behavior	2	740	0.37	0.42	0.22	0.30	0.54	0.19	0.66	16.45**	104
Fabricate	3	854	0.46	0.56	0.46	0.39	0.73	0.28	0.85	25.50**	208
Protect	2	710	0.56	0.67	0.41	0.59	0.74	0.48	0.85	8.65**	164
Withhold	2	710	0.73	0.89	0.14	0.82	0.97	0.83	0.96	1.06	221
Online spending	2	1,858	-0.09	-0.09	0.07	-0.16	-0.04	-0.16	-0.05	4.27*	28
Privacy setting use	2	1,827	0.11	0.16	0.20	0.09	0.23	-0.07	0.38	35.78**	37
Risk	15	5,301	0.45	0.53	0.20	0.44	0.634	0.18	0.89	258.25**	987
Trust	21	7,725	-0.43	-0.51	0.30	-0.61	-0.42	-0.98	-0.05	540.80**	1365

Note. *$p < .05$; ** $p < .01$

[a] The number of studies. [b] The total sample size. [c] The weighted mean correlation. [d] The weighted mean corrected correlation.

Discussion

Findings

This study reviewed a large sample of the studies relevant to information assurance in the context of e-commerce and social media for the meta-analysis. Among all the 85 studies which were included in the meta-analysis, there were 50 journal articles, 23 conference proceedings, and 5 dissertations. The results of the analysis showed significant heterogeneity among majority of the variables suggesting the presence of the moderation effect. This study also categorized the variables in the meta-analysis based on the integrated framework suggested at in previous sections.

Antecedents/Consequences

As we discussed earlier, there are some contradictory results in the information assurance literature about the antecedents and consequences of OPC. This contradiction arises when some researchers suggest a factor as an antecedent of OPC while the others studied that variable as the consequence of OPC. Findings about the relationship between trust and online privacy concern is not consistent. Whereas many studies suggest trust as a consequence of OPC (e.g., Yang, 2012), we found a few researchers who argue that trust affects user's privacy concern (e.g., Taylor et al., 2009). This study addressed this inconsistency in the literature. The results of this study revealed that 21 studies found that users' privacy concerns affect their trust while only 5 researchers suggest trust as an antecedent for privacy concern. Thus, the current literature findings suggest that trust is affected by online privacy concerns.

The other important contradictory finding in the current research is about the relationship between risk and OPC. While several studies suggest that users' online privacy concerns affect their perception of risk from the online environment (e.g., Odeyinde, 2013; Plummer, Hiltz, & Plotnick, 2011), some researchers argue that this relationship is directionally vice versa OPC (e.g., Kehr et al., 2015). This study's findings showed that risk is more likely to be a consequence of OPC. The reason is that the number of studies that proposed perceived risk as a consequence for OPC (N = 15) are more than those that posited perceived risk as an antecedents of OPC (N = 4).

Antecedents

Results of this study show that there is too much diversity among the antecedents of OPC in the current research. The number of studies that include any of the antecedents of OPC ranged from 1 to 5 indicating that there is not an agreement about the antecedents of the online privacy in the research. The majority of antecedents in the literature were user's characteristics. Among these user characteristics a few of them were repeated in more than two studies and, among those, only computer anxiety is a strong antecedent for the OPC. Among the rest of the user characteristics disposition to privacy, familiarity, negative experience, perceived anonymity of others, perceived anonymity of self, perceived risks, perceived vulnerability, and privacy control had moderate effects on users' OPC.

Furthermore, among the website characteristics and features, only privacy policy, interaction justice, reputation had moderate effect on users' OPC. The rest of the antecedents related to website had very small effect sizes. This finding shows that these three antecedents of OPC may be more useful to assure users about the privacy of their information. Finally, the only antecedent of OPC which was studied more than one time in the literature and had a small effect size was regulations.

Consequences

Our findings indicate that users' privacy concerns are highly related to fabricate, protect, and withholding that are the three responses to the OPC suggested by previous research. Furthermore, online privacy is highly associated with purchase intention compared with purchase behavior (online spending). Thus, consumers' privacy concern affect their intention to purchase directly. The results also revealed that behavioral intentions have stronger effect sizes than the behaviors suggesting that OPC affect intention to perform behavior directly. Finally, as we discussed earlier, this study found that OPC has a very strong influence on users' perception about trust and risk.

Implications

This study has implications for academia and practice. From the point of view of academia, this study provides a big picture of the most significant factors in the information assurance literature. There is ambiguity and diversity about the antecedents and consequences of online privacy concern in the literature and this study addresses this ambiguity and diversity by categorizing all these factors and identifying the strongest relationships by conducting the meta-analysis. There are three important categories of factors that influence online users concern for privacy: user, website, and third-party related factors. We found that factors related to the third-party have not been studied enough and there is too much diversity about them. One reason for that is that collecting data about the third-parties' activities is not convenient for researchers. Therefore, future research may focus on this area more than before.

Explaining how information privacy concern, online trust, and perceived risk affect each other based on an in-depth review of the current information assurance literature, this study resolves the ambiguity regarding the role of these factors among different studies. Although, some studies suggest users' online trust and perceived risk as antecedents of OPC, this study supports that online trust and perceived risks are consequences of OPC. Future research may apply this finding by focusing on these two variables in this role more than before. Another implication of our finding for academia is to explain how OPC affect users' behavior through affecting their intention. Our findings show that there is a strong relationship between users' online privacy concern and their intention to perform behavior while the weighted mean effect sizes associated between OPC and behaviors are very small. This finding supports previous studies suggested that stimuli affects users' intention and users' intention affects their behavior (Smith et al., 2011). Whereas Smith et al. (2011) claim that most of the current research measured intention instead of behavior, our finding shows that even those studies that measured behavior of users found small effect sizes.

Our findings have several implications for practitioners. First, online websites may apply findings of this study to influence users' privacy concern and assure them about their privacy. Thus, the important question that the future research and website managers should address is how they can affect the most significant antecedents by applying the mechanisms which are available. Second, our findings show that users' privacy concern is an influential element in the assurance process that can affect users' trust and risk perception. Thus, website managers may focus on diminishing these concerns more than before to affect users' trust and risk perceptions.

Limitations and Future Research

Like any other studies, this study has limitations. First, the inclusion of studies with significant finding rather than null finding is a possible bias of this study. The fail-safe N statistics indicated that there should be a large number of unpublished or unincluded studies in our meta-analysis to change our finding. In addition to minimize this bias in our sample, this study includes several conference proceedings and dissertations in the sample size. If this bias exists in our sample, then our findings indicate an overestimated relationship between OPC and its antecedents and consequences.

The second limitation of this study is the inclusion of the pairwise relationships for those antecedents and consequences that have not been studied enough in previous research (i.e., k<5). Because of the diversity among the antecedents and consequences of OPC in assurance literature, there were so many antecedents and consequences that have not been studied enough. Because of this limitation, the results of meta-analysis for those variables with small ks (k<= 3) can be a threat of the validity of the findings (Hunter & Schmidt, 2004). Although there are limitations about the sample size, there is no assumption that is not likely to hold with small sample sizes in the analysis of this study (Rosenthal, 1984, p. 118).

Third, the current research has not investigated some antecedents and consequences of OPC enough. For example, there was too much diversity among the studies that investigated the influence of third party related factors on OPC. Thus, future research may focus on more emphasis on studying unstudied factors in information assurance. Finally, the Q-tests results revealed high heterogeneity for some antecedents and consequences in this study suggesting the presence of moderators in this study. Thus, future research may also identify and examine the moderator effect of possible moderators such as sample size, context of study, gender, and more.

Conclusion

Decreasing the online user’s level of concern is one of the most important objectives of websites because, the higher the level of concern, the more reluctant consumers are to interact with that websites in different ways. The present meta-analysis provides new information on the relationships involving online privacy concern and its’ related antecedents and consequences in the information assurance literature. The information is particularly important for clarifying the conceptual ambiguities surrounding the effect of privacy concern. Overall, this meta-analysis can be of value because it can be used as a stepping stone for future studies on information assurance. Moreover, these insights provide website managers with opportunities to improve the returns information assurance on their investments.

ESSAY II: A CONCERN-BASED CONSUMER DECISION MAKING MODEL IN ELECTRONIC COMMERCE: THE ROLE OF WEB ASSURANCE MECHANISMS AND PERCEIVED CONCERNS

Introduction

In recent years, online shopping has become more popular than ever before. The latest analysis of the U.S. Census of Bureau reported the retail e-commerce sales for the second quarter of 2015 was $83.9 billion – an increase of 4.2 percent from the previous quarter (DeNale, Liu, & Weidenhamer, 2015). Worldwide, the total retail e-commerce sale is projected to rise to $2.489 trillion in 2018 (Bhaiya, 2015). As an important online business model, Business-to-Consumer (B2C) electronic commerce represents a major online transaction platform which appeals both buyers and sellers (Chen, Hsu, & Lin, 2010). For sellers, the efficient use of time combined with the technological improvements drive them to develop digital storefronts for the provision of goods and services. For buyers, online shopping provides convenience, time and money savings, and hedonic values which promote consumers towards online purchases (Eroglu, Machleit, & Davis, 2001). In fact, there is no constraint of time and space in B2C retailing that would convince both buyers and sellers choosing this channel (Kalakota & Whinston, 1997).

While online shopping introduces a myriad of benefits, consumers may develop concerns and worries with regard to their online purchases. Prior studies have reported that online consumer's concerns play important roles in their purchasing decisions (Miyazaki & Fernandez, 2001). Miyazaki and Fernandez (2001) identify three focal online concerns that hinder online consumers in their purchase decisions: product and service concerns, security concern, and privacy concern. Product and service concern refers to the fraudulent behavior of the online retailers in association with product and service. Examples are such as delivery of defective product and unsatisfactory service after sales. Transaction security concern is about potentially malicious activities related to online transactions such as unauthorized transactions and altering and breaching transaction information (Miyazaki & Fernandez, 2001, p. 34). Privacy concern refers to consumers' risk perception of the likelihood that a retailer or other unauthorized entities inappropriately use their confidential information without their permission (Kim, Ferrin, & Rao, 2008).

To mitigate these concerns, online vendors have developed several assurance mechanisms including assurance statements and third-party assurance seals. Designated to e-vendors by third-party industry authorities, assurance seals are indications of seal-bearing vendors' compliance with a high standard of technical and/or business practices. In contrast, assurance statements are vendor-initiated second-party efforts that convey business policies and procedures to warrant a safe shopping environment. Both third-party assurance seals and second-party vendors' assurance statements are important assurance mechanisms of e-commerce transactions for first-party online buyers to convince their purchasing decisions in e-commerce.

Although most previous studies have discussed the broad values of assurance mechanisms in increasing consumers trust (McKnight et al., 2004; Han Zhang, 2005), it has been much silent on the joint effects of the two assurance mechanisms on online consumers' concerns, which are often simultaneously adopted by e-commerce vendors to alleviate concerns. Specifically, we contend that assurance mechanisms affect purchase intention through alleviating consumer concerns. This contrasts to prior studies which have implied an indirect effect, through trusting beliefs or risk perception, of web assurance features on consumer behaviors (K. Kimery

& M. McCord, 2002) but have not confirmed if such an effect is actually mediated by other constructs.

Motivated by the understudied area above, this study attempts to fill the gap by examining how these two assurance mechanisms affects consumers' concerns and their subsequent purchase intention. Specifically, we analyze the relationships among the pertinent factors to contend that the two assurance mechanisms positively affect consumers' purchase intention by alleviating the three focal online consumers' concerns– a mediation effect. In this study, we explicitly answer following two research questions: (1) "how do consumers' three focal online concerns (i.e., privacy concern, product and service, and transaction security concern) affect their purchase intention?" and (2) "how do third-party assurance seals and second-party security assurance statements influence online consumers' concerns and subsequently their purchase intention?"

This study makes several contributions. First, the results show that assurance statements outperform assurance seals in alleviating consumer concerns: (a) assurance statements reduce all three consumer concerns whereas assurance seals reduce transaction security concerns only; and (b) the effect of assurance statements on transaction security concern is greater than that of assurance seals. Second, we find that the effect of assurance statements and assurance seals on purchase intention is mediated by online consumers' concerns. As a consequence, the study sheds new insights on the effects of assurance mechanisms on the domain of information security and assurance. Finally, we report that assurance seals supplement the effects of assurance statements on privacy concern and product and service concern and that consumers' purchase decisions are affected by both information concern and privacy concern but not product/service concern which is a non-information security concern.

In the next section, we review literature on information security and assurance mechanisms and major inhibitors of online consumers' purchase decisions. Then we propose a research model and hypotheses. We present research methodology to validate the proposed research model. After presenting the data analysis and results, we discuss the findings of the study along with the theoretical contributions and practical implications.

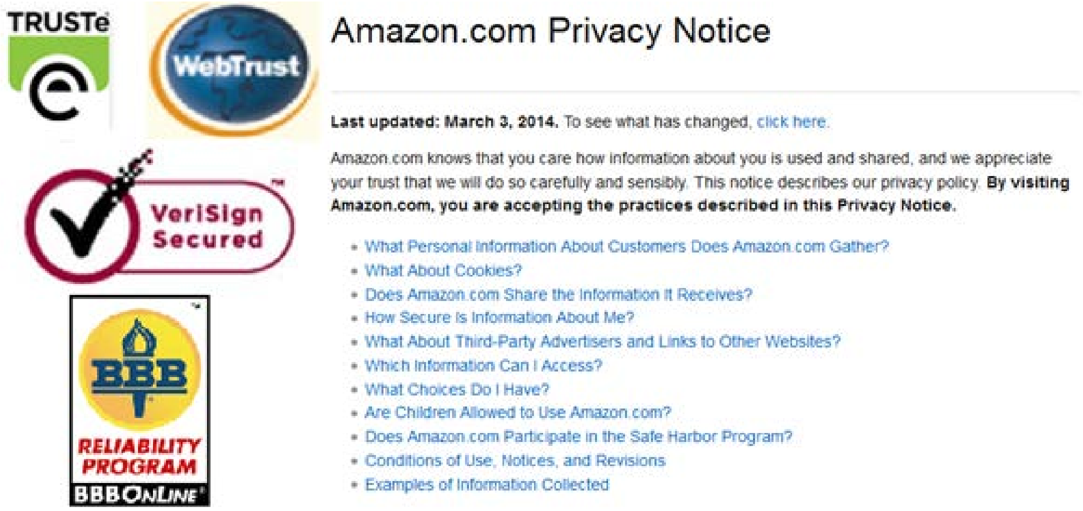
Literature Review

Information Security and Assurance Mechanisms

To manage today's overwhelming issues of the interlocking fields of cyber security, information privacy, network security, and socio-technical aspects of security, information assurance mechanisms on security are needed. Information assurance contains all the elements of information security (i.e., confidentiality, integrity, and availability) and provides a view of information protection that includes assurance mechanisms in different levels of controls (e.g., technology, operations, and security education & training awareness programs). According to Maconachy, Schou, Ragsdale, and Welch (2001, p. 306) INFOSEC is define as "protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats". The Information Systems Security Committee (NSTISSC) argues that infoirmation assurance incorporates protection, detection and reaction capabilities to protect and defend information and information systems (Maconachy et al., 2001). Thus, information assurance is not only a measure for protecting information and information systems (the goal of information security) but also a control that helps users and IT professionals to detect and react against possible threats.

To respond to consumers' concerns about security and privacy in e-commerce, online vendors opt for information assurance mechanisms that help remedy concerns and negative feelings of their buyers. Two most popular assurance mechanisms recognized by the prior studies are third-party assurance seals and self-exposure assurance statements. Third-party assurances seals refer to "an assurance of an Internet vendor provided by a third-party certifying body such as a bank, accountant, consumer union, or computer company" (Kim, Ferrin, et al., 2008, p. 550). The web seals are created in order to decrease online consumers' concerns of online transactions (Han Zhang, 2005). The effect of seals on consumer purchasing behavior has been studied by a number of researchers. For example, McKnight et al. suggest assurance seals as important signaling tools for online shopping websites to increase their consumers' trust (McKnight et al., 2004). Yet their empirical results show that assurance seals do not impact on trust in the web business. Likewise, Kim, Ferrin, et al. (2008) studied the effect of the assurance seals on consumers' perceived trust and risks regarding online shopping website. Their results show that assurance seals do not have any effect on consumers' trust while they have a significant effect on their perceived risk.

In addition to posting assurance seals, e-commerce websites publish their own assurance statements as a part of business privacy notice, security policy, or customer satisfaction guarantee (see Figure 2 for examples). Assurance statements assure and appease consumers that help will be provided and consumer concerns, issues, and problems will be resolved. Arcand et al. argue that assurance statements are another important mechanism to support online consumers (Arcand, Nantel, Arles-Dufour, & Vincent, 2007). Similarly, Bansal, Zahedi, and Gefen (2008) propose a set of assurance statements as an effective facilitator on consumers’ provision of personal information during online transactions. These statements generally increase the consumers’ perceived control of the website through their information.



Amazon.com Privacy Notice

Last updated: March 3, 2014. To see what has changed, click here.

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

- What Personal Information About Customers Does Amazon.com Gather?
- What About Cookies?
- Does Amazon.com Share the Information It Receives?
- How Secure Is Information About Me?
- What About Third-Party Advertisers and Links to Other Websites?
- Which Information Can I Access?
- What Choices Do I Have?
- Are Children Allowed to Use Amazon.com?
- Does Amazon.com Participate in the Safe Harbor Program?
- Conditions of Use, Notices, and Revisions
- Examples of Information Collected

Figure 2. Examples of assurance mechanisms

The findings from the existing literature are summarized in Table 3. While prior studies have shed insights on web assurance, they are limited in a number of ways which warrant new research. First, a vast majority of the existing research has focused on either self-initiated assurance statements (Arcand et al., 2007; Gauzente, 2004; D. Kim, N. Sivasailam, & H. R. Rao, 2004; Nemati & Dyke, 2009) or third-party assurance seals (Hu, Wu, Wu, & Zhang, 2010; Kim, 2008; Kim, Ferrin, et al., 2008; K. Kimery & M. McCord, 2002; McKnight et al., 2004; Park, Bhatnagar, & Rao, 2010; H. Zhang, 2005) with few exceptions (Bansal, Zahedi, & Gefen, 2015b; F Belanger, J.S Hiller, & W.J Smith, 2002; Kim, Steinfield, et al., 2008). As a result, these studies miss the opportunities to compare the effects of both assurance features. Between the two features, one may play a dominant role or even displace the other when it comes to affecting online consumers. Second, findings on the effects of web assurance features are mixed to date. While some studies find constructive effects (Arcand et al., 2007; Bansal et al., 2015b; Hu, Wu, Wu, & Zhang, 2005; Hu et al., 2010; Kim, 2008; Kim, Ferrin, et al., 2008; Nemati & Dyke, 2009; H. Zhang, 2005), others report either a lack of consturctive effects (Arcand et al., 2007; Bansal et al., 2015b; Kim, Ferrin, et al., 2008; K. Kimery & M. McCord, 2002; McKnight et al., 2004) or even destructive effects (Arcand et al., 2007; Nemati & Dyke, 2009). Although the mixed findings may be attributed to the choice of assurance constructs used and the research designs employed, they clearly suggest that more research needs to be conducted in order to gain an improved understanding of how web assurance features affect individual users. Third, in the study of web assurance, existing literature has predominately borrowed the theoretical lens of trust (Bansal et al., 2015b; Hu et al., 2005, 2010; Kim, 2008; Kim, Ferrin, et al., 2008; K. Kimery & M. McCord, 2002; McKnight et al., 2004; Nemati & Dyke, 2009). Findings on whether web assurance affects consumer trust does not explain if these features successfully alleviate consumer concerns over uncertainties in online purchase. Put differently, prior studies haven't tested if constructs such as trusting beliefs relay (i.e., mediate) the effect of web assurance mechanisms on user behavior. Finally, many studies examine web assurance features through their presence (yes/no) (Arcand et al., 2007; Hu et al., 2005, 2010; D. Kim et al., 2004; Kim, Ferrin, et al., 2008; McKnight et al., 2004; Park et al., 2010; H. Zhang, 2005), users' reading/notice of assurance features (yes/no) (K. Kimery & M. McCord, 2002; Nemati & Dyke, 2009), and users' awareness/attention to assurance features (high/low) (Kim, Steinfield, et al., 2008; K. Kimery & M. McCord, 2002). As a consequence, they have failed to capture online consumers' subjective evaluation of these mechanisms, which is important for understanding how consumers interpret and evaluate these safeguards.

Considering these existing gaps, in this study, we develop a conceptual model to theorize the values, as perceived by online consumers, of the two web assurance features in addressing consumer concerns, which may in turn promote consumer purchase intention. As discussed before, little is known if any one of the two web assurance features proves to be more effective in reducing the key concerns held by online consumers. Nor does the literature suggest if the positive effect of one assurance feature will be displaced by the other feature. As most e-commerce websites utilize both assurance features, our model helps develop a holistic view on how co-existence of the two features jointly affects average users. When they are co-present, their relative effects in promoting purchase intention may be contingent upon how individual consumers value internal assurance versus external assurance. We further project that the effects of both web assurance mechanisms on user purchase intention may be mediated by the key concerns, a mediating effect that has not been explored in the past.

Table 3

Summary of key findings from literature on assurance mechanisms

Studies	**Constructs related to Assurance Mechanism**	**Key Findings**
Arcand et al. (2007)	Presence of privacy statement (yes/no), reading privacy statement (yes/no)	First, the mere presence of privacy statement has a positive impact on perceived control over privacy. Second, the mere presence of privacy statement has no effect on perceived trust. Third, reading the privacy statement reduces perceived control and perceived trust in study 1 while it casts no effect in study 2.
F Belanger et al. (2002)	User ranking of the importance of assurance statements and seals	First, customers rank privacy statements and seals (security and privacy) as less important than security features. Second, customers rank privacy statements, security seals and privacy seals of equal importance.
Bansal et al. (2015b)	Privacy policy adequacy, perceived	First, third party assurance seals have no effect on trust in website. Second, privacy policy adequacy has no effect on trust in health website for customers with high privacy

	presence of third party assurance	concern. Third, the effect of privacy policy adequacy on trust in website is positively moderated by privacy concern in e-commerce websites and is negatively moderated privacy concern in financial and health websites.
Gauzente (2004)	User ratings of perceived “reassuringness” of assurance statements	First, highly concerned consumers will demand more regarding privacy and security statement, as suggested by correlation analysis. Second, consumers rank security and control as the most component of privacy and security statement.
Hu et al. (2010)	Presence of assurance seals (yes/no)	First, there exists an attenuating interaction effects rather than synergistic effects between privacy and the security functions and the transaction-integrity functions of assurance seals and between the privacy. Second, the effects of security or transaction-integrity assurance function on consumers' initial trust are moderated by the privacy assurance function.
Hu et al. (2005)	Presence of assurance seal (yes/no)	First, a seal that promotes privacy, security, or transaction-integrity increases consumers’ trust toward an online store that displays the seal. Second, a seal that promotes two or more assurance doesn’t increase consumers’ trust than a seal that promotes only one assurance.
Kim (2008)	Perceived importance of third-party seals	Perceived importance of third-party seals is positively related to consumer trust in e-vendors in a Type II (i.e., collectivist–strong uncertainty avoidance–high long-term orientation–high context) culture but not in a Type I (i.e., individualistic–weak uncertainty avoidance–low long-term orientation–low context) culture.
Kim, Ferrin, et al. (2008)	Presence of third-party seals (yes/no)	First, the presence of third-party seal reduces perceived overall risk. Second, presence of third-party seals doesn’t reduce perceived trust.
D. Kim et al. (2004)	Presence of assurance statements (yes/no)	First, companies that deal with monetary transactions describe business integrity in their assurance statements more than other companies. Second, more reputable companies describe more in their assurance statements than less reputable companies.
Kim, Steinfield, et al. (2008)	Awareness of web assurance features, perceived importance of web assurance features	First, consumers’ awareness of web assurance mechanisms positively affects their perceived importance of web assurance mechanisms. Second, consumers’ awareness of web assurance mechanisms is affected by their security concern. Second, consumers’ awareness of web assurance mechanisms is not affected by their privacy concern.

K. Kimery and M. McCord (2002)	Assurance seal notice, and attention to seal	First, consumers' seeing an assurance seal has not effect on their trust in an e-retailer. Second, increased attention to an assurance seal has no effect on consumer trust.
McKnight et al. (2004)	Presence of assurance seals (yes/no)	First, privacy seals do not affect trust in web services. Second, industry seals does not affect trust in web services.
Nemati and Dyke (2009)	Presence of privacy statements (yes/no)	First, the presence of privacy statement increases consumer trust. Second, the presence of statement increases perceived risks as well. The authors attribute this negative effect to the increased awareness of potential threats that such statements bring to customers. Finally, changes in privacy statement contents don't affect perceived trust and risk.
Park et al. (2010)	Presence of assurance seals (yes/no)	First, the presence or absence of third-party assurance seals moderates the effect of service performance on customer satisfaction. Second, the presence or absence of third-party assurance seals moderates the effect of service performance on repeat purchase intention. Third, customer satisfaction for vendors with seals has less diminishing sensitivity than for vendors without seals.
H. Zhang (2005)	Displaying assurance seals (yes/no)	First, displaying information and reliability assurance seals increases consumers' willingness to buy (WTB). Second, displaying reliability assurance seals increases WTB than information assurance seals. Third, information assurance seals increase WTB for online commodity products whereas reliability assurance seals increase WTB for both online commodity and look-and-feel products. Fourth, trust promoting seals affect WTB of inexperienced online shoppers more than they affect experienced shoppers.

Major Inhibitors of Online Consumers' Purchase Decisions

While product purchase decisions in the offline context are mainly affected by the price and quality of product (Chang & Wildt, 1994), online purchase decisions are possibly affected by other additional factors. To date, several studies have explored the main drivers of online purchase decisions. Brown et al. suggest that product type, prior purchasing experience from the website, and gender may effect online consumers' purchase decisions (Brown, Pope, & Voges, 2003). In addition, Bai, Law, and Wen (2008) and Qureshi et al. (2009) note that website quality affect consumers’ purchase intention through its effect on consumer satisfaction. Likewise, Poddar, Donthu, and Wei (2009) argue that consumer personality as well as website quality are pertinent to consumers’ online purchase intention. Park, Lennon, and Stoel (2005) further point out that the visual presentation of goods in websites may relate to consumers’ purchase intentions. Still, Chen et al. (2010) show that a number of attributes such as usability, delivery, and convenience are associate with purchase intention. Otim and Grover (2006) address that pre-purchase, post-purchase, and transaction related services along with product satisfaction and pricing strategy affect online consumers’ purchase decisions.

The existing literature has explored the potential inhibitors of consumers’ online purchase decisions. Due to the information asymmetry, consumers make decisions with limited information (Kim, Ferrin, et al., 2008) while vendors may behave opportunistically to exploit consumers’ trust (Al Kailani & Kumar, 2011). Therefore, consumers’ purchase decisions are inherent to uncertainties (Bhatnagar, Misra, & Rao, 2000; Forsythe & Shi, 2003). Through an extensive review of prevailing literature on online shopping adoption, Chang, Cheung, and Lai (2005) highlight several factors that affect online consumers’ purchase decisions. These factors address information privacy, transaction security, and vendor fraudulent behavior such as product scams and credit card faults. By surveying online consumers, Miyazaki and Fernandez (2001) classify online shopping concerns into four categories: privacy, system security, security, and inconvenience. In their research, privacy concern is associated with the infringement by retailers to disclose consumers’ information to others; system security refers to unauthorized third-party access to consumers’ information; security describes potential non-delivery of ordered goods; inconvenience addresses several issues related to online shopping such as the inability for one to touch or feel the actual goods. Synthesizing prior studies, this study mainly focuses on three focal consumers concerns (i.e., privacy, security, and product & service concerns) to theorize their potential associations to consumers' purchase intention.

Among the concerns that matter to online consumers in their decision making, security and privacy stand out as two fundamental issues (France Belanger, Janine S Hiller, & Wanda J Smith, 2002). Online sellers collect different types of consumer information such as name, address, phone number, email address, etc. Once captured, consumer information could be transferred to third-parties, reused without consent, or exploited for secondary use (Lowry, Cao, & Everard, 2011). Therefore, for online consumers, privacy is an important concern (Kim, Ferrin, et al., 2008). Privacy concern is on the rise in the recent years as a result of the use of pervasive technologies (Flavián & Guinalíu, 2006). It has been investigated in an extensive body of the literature as an important factor that affects individuals' decision making (Dinev, Xu, Smith, & Hart, 2013). Smith et al. (2011) report privacy experience, privacy awareness, personality awareness, demographic differences, and culture as important antecedents of privacy concern.

In parallel, Furnell and Karweni (1999) and Salisbury, Pearson, Pearson, and Miller (2001) stress that security concern is one of the most enduring theme of e-commerce. This view is also held by Ranganathan and Ganapathy who recognize security as the single most important predictor of online purchase intention (Ranganathan & Ganapathy, 2002). As a *Wild West*, the Internet serves as an open platform that is accessed by cyber criminals on a 24-7 basis. The lack of effective regulation, the lack of security awareness, and the under-preparedness of online vendors all render e-commerce activities susceptible to attacks. A wide array of cyber-attacks such as hacking, social engineering, and dissemination of malwares pose a constant threat to vendors and the consumer data that they retain (Lazzarotti, 2014). Casaló, Flavián, and Guinalíu (2007) suggest that it is important to study both concerns yet the prevailing literature has primarily on one over the other. Recent studies sometimes doubt the significance of these concerns on consumers' decision making. Van Slyke et al., for example, find that privacy does not have a direct negative effect on online transaction (Van Slyke et al., 2006).

Research Model and Hypotheses

A number of studies in the literature discuss the relationship between risk and purchase intention in online shopping (e.g., Chang et al., 2005; Kim, Ferrin, et al., 2008; Van der Heijden, Verhagen, & Creemers, 2003). The valance framework by Peter and Tarpey Sr (1975) addresses that consumers evaluate products based on desirable and undesirable features. They argue that in the risk-benefit typology there are three strategies that consumers can decide to purchase a product: (1) minimizing perceived risk, (2) maximizing perceived return or benefit, and (3) maximizing net benefit, which is defined as the difference between perceived benefit and risk. Based on the valance framework, consumers' concerns are important factors that affect consumers' purchase decision when buying a product from a specific vendor. Consumer concerns may be cultivated by a broad range of factors with examples such as consumers' perceived risks.

In online transactions, consumers must surrender their private information in return of goods or services. Accordingly, information security and privacy issues render chief issues that concern online buyers. Procedural fairness theory argue that individuals are willing to disclose their information if they perceive that their information is used fairly and if they consider that they will not suffer negative consequences (Milne & Gordon, 1993; Stone & Stone, 1990). Procedural fairness refers to "the perception by the individual that a particular activity in which they are a participant is conducted fairly” (Culnan & Armstrong, 1999, p. 107). Fair information practice is based on two concepts: (1) people have the right to know why their information is collected and (2) people should have the right to control the way their information is used (Culnan & Armstrong, 1999). Procedural fairness theory suggests that transparency of vendor’s actions is an important mechanism to mitigate consumers’ concerns regarding their information (Li, 2012; Stone & Stone, 1990). To this end, e-commerce vendors often employ two important assurance mechanisms as suggested by the web assurance literature (Hui et al., 2007): (1) third-party assurance seals (Lala et al., 2002) and (2) assurance statements (Milne & Culnan, 2002, 2004). Assurance statements describe e-vendors’ rules regarding issues such as consumers’ information collection and usage (Hui et al., 2007). Meanwhile, assurance seals increase consumers’ perceive control over the vendors’ processes. Assurance granting bodies control and certify all the processes that the e-vendors adopts in managing the information security and privacy (Kim, Ferrin, et al., 2008). According to the two concepts of the fair information practice in procedural fairness theory mentioned before, assurance statements increase the transparency of the security and privacy features used by the vendors and assurance seals ensure consumers about the control over the vendors’ actions. Therefore, we suggest that assurance statements and assurance seals influence consumer concerns negatively. In addition, the uncertainties with vendor opportunism render a valid concern when a consumer worries about the potential of mis-presentation of product information, non-delivery, or failure to honor after-sale warranty. That is, a consumer may become worry about the potential of presentation of incorrect product information, non-delivery, or failure to honor after-sale warranty – which is termed as product and service concerns in this research. The three individual concerns resemble the major categories of online consumers' concerns as proposed by Miyazaki and Fernandez (2001). In line with the findings of Miyazaki and Fernandez (Miyazaki & Fernandez, 2001) as well as e-commerce related risk-return typology, we propose a research model (Figure 3).

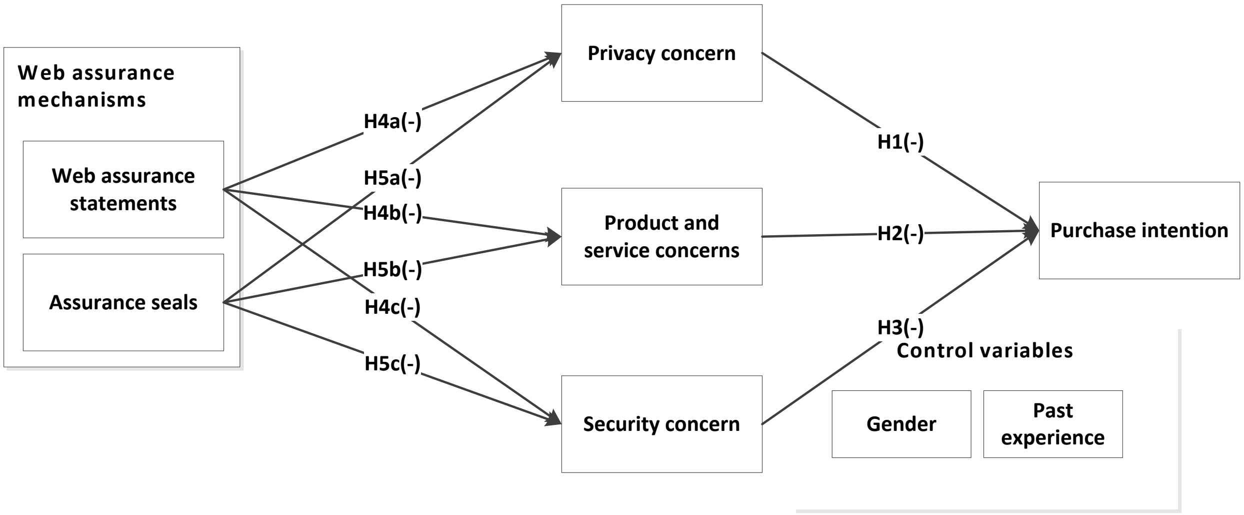


Figure 3. Research model

The research model addresses three different concerns of online consumers and suggests their effects on consumers' purchase intention; two assurance mechanisms (i.e., assurance statements and assurance seals) lessen the effects of three different concerns. Further, we propose the effects of assurance mechanisms indirectly influence on purchase through three different concerns as mediators in the model. The mediating effects of three different concerns for each assurance mechanism are hypothesized separately as H6a and H6b in the hypothesis development section later.

Westin (1967, p. 7) defines information privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". France Belanger et al. (2002) argue that privacy concern as one key factor influences online consumers' purchase intention. Privacy concern refers to consumers' worry about the likelihood that a retailer tries to use their confidential information without their permission (Kim, Ferrin, et al., 2008). Illegal use of consumers' personal information has harmful consequences, such as identity theft (Ratnasingham, 1998); therefore, privacy concerns is one of major worries of online consumers (e.g., Ackerman, Cranor, & Reagle, 1999; Miyazaki & Fernandez, 2001). Privacy concern may cause online consumers to expect negative outcomes from online shopping. In fact, online retailers acquire a great deal of information from consumers compared to other types of commerce, which can increase consumer concern and negatively affect their purchase intention. Thus, if online consumers perceive that online retailers inappropriately manage their personal information, they may not trust the online retailers, in turn, forming a hindrance, which will decrease their willingness to make further business relationships with the online retailers. Therefore, we hypothesize that:

H1: Online consumers' privacy concern negatively affects their purchase intention.

Product and service concern refers to uncertainty about fraudulent behavior of an online retailer in association with products and services. Consumers' concern about a product or service could be related to different aspects of the services. Examples are such as on time delivery or flexible return policies of a product. E-commerce literature underscored product and service concern as one of the important issues for online consumers (Miyazaki & Fernandez, 2001). Online consumers who have more concerns about possible issues with the product or service that they plan to procure from an online may feel more uncertainties with regard to buying a product or service. Therefore, they may have less intention to shop online. In fact, many prefer to shop from other channels such as offline shopping in order to avoid such risks. So we hypothesize that:

H2: Online consumers' product and service concern negatively affects their purchase intention.

Transaction security concern refers to "concerns about potentially malicious individuals who breach technological data protection devices to acquire consumers' personal, financial, or transaction- oriented information" (Miyazaki & Fernandez, 2001, p. 34). Also termed as "system security", transaction security concern indicates the importance of online consumers' worries about their transactional information. One of the distinguished features of e-commerce is making a transaction online, which provides convenience and flexibility of shopping. If online consumers have concerns about their online transaction information that they share with the online retailer or they believe that online retailer cannot safeguard secure transactions from unauthorized access such as hacking, they may avoid purchasing from the Internet. Based on the above arguments, we hypothesize that:

H3: Online consumers' transaction security concern negatively affects their purchase intention.

Assurance statements refer to vendors' words or pledges described in their websites to ensure their consumers about appropriate controls over the sensitive transaction information of their customers (Singer, Hippler, & Schwarz, 1992). These assurance statements explain the purpose and intended use of consumer information and convey their privacy handling policy to their consumers. It, therefore, helps increase consumers' perceived control over their information which has been shared with these websites (Arcand et al., 2007). By increasing the perceived control over personal information, consumers develop less uncertainties about the information that their share with the e-commerce website. Xu et al. (2005), for example, suggest that privacy assurance statement is an effective mechanism that reduces users' perceived privacy risk in the context of location-based services. Likewise, Belanger et al. comment that the presence of strong assurance statements is the first step to insure consumers that their personal information are inaccessible by unauthorized parties (France Belanger et al., 2002). In addition, the presence of assurance statements is indicative of vendors' benevolence in sustaining consumers' welfare – protection of private information. It, therefore, fosters consumers' trusting belief in online stores. Following the *trust transfer* mechanism (Delgado-Márquez, Hurtado-Torres, & Aragón-Correa, 2013; Lu, Yang, Chaung, & Cao, 2011; Stewart, 2003), consumers tend to develop a high level of trusting belief towards an online store with respect to other qualities such as product and services. As consumers make an inference about vendors' care of their privacy, they subsequently expect that the online store will behave in a similar manner in addressing other important matters. For example, such a trustful website would be likely to commit to its claims about the product and service provided so the consumer may have less concern. Finally, we contend that assurance statements may alleviate consumer's concern on transaction security. Transaction security relates to unauthorized access to consumer information, which is often addressed in assurance statements which prevent all types of data misuse including unauthorized access. As a result, the use of assurance statements by an online store provides a partial remedy to threats on transaction security. Accordingly, consumers may become less concerned regarding the disclosure of their transaction data such as their credit card information, etc. We hypothesize that:

H4a: Assurance statements diminish online consumers' privacy concern.

H4b: Assurance statements diminish online consumers' product and service concern.

H4c: Assurance statements diminish online consumers' transaction security concern.

In contrast to assurance statements which are developed by individual e-commerce vendors as the second-party of e-commerce transactions, assurance seals are created by third-party professional assurance services. Market leading assurance seals are such as Web Assured, BBB Online, WebTrust, and TRUSTe. These seals are developed following a common framework (e.g., a set of core principles and criteria) to address common issues in business management and technology usage. Assurance seals are provided by a third party to insure consumers that proper measures and practices have been adopted by the vendors, with important tasks such as the provision of goods and services, safeguarding credit card transactions, and management of consumer data (WebTrust, 2015). E-commerce websites use third-party assurance seals to ensure their consumers that their business and website meet the industry standards and guarantee the required standard quality of their services at least. Assurance seals are obtained when an online business develops adequate policies and procedures that achieve the objectives of core principles established by the seal-granting authorities. The key principles often concern a wide range of imperative issues such as information confidentiality, service availability, processing integrity, protection against unauthorized access (both physical and logical), and privacy (WebTrust, 2015). The achievement of assurance seal certification serves the proof that an e-commerce transaction is attuned to the potential risks and are equipped with controls that address those risks. In addition, e-commerce firms are monitored by the seal-granting authorities to ensure continuous compliance. Mechanisms that a website applied to increase the control of data transmission to or from that website negatively affect consumers concerns about their privacy (TRUSTe, 2015). The existence of the assurance seals also indicates that the website contains security features to conform to the industry standards (Chellappa & Pavlou, 2002). As assurance seals signifies trust, consumers expect assurance seals certified websites to display integrity (Miyazaki & Krishnamurthy, 2002). Subsequently, consumers develop the beliefs that vendors will keep their promises in other practices such as the provision of quality product and services. Therefore, we posit that:

H5a: Assurance seals diminish online consumers' privacy concern.

H5b: Assurance seals diminish online consumers' product and service concern.

H5c: Assurance seals diminish online consumers' transaction security concern.

Presence of assurance statements on an online shopping website affects consumers' trust in the vendor as well as consumers' perceived control (Arcand et al., 2007). This is because assurance statements signify vendors' respect of consumer privacy and indicates vendors' intention to properly manage consumers' information. Therefore, assurance statements help mitigate uncertainties that are associated with the future use of consumer information and subsequently they ease consumer fear. Bansal et al. (2008) suggest that assurance statements promote users to interact with an organization by supplying personal information to facilitate transactions. Because assurance statements affect consumer's purchase intention by alleviating their concerns about the uncertainties, we expect the effect of assurance statements on purchase intention is mediated by consumer concerns. The assurance seals have similar role as assurance statements. K. M. Kimery and M. McCord (2002) argued that e-commerce websites, which have specific assurance seals, agreed to apply the third party's standards and use specific technology. The assurance seal is a mechanism which is used by e-commerce websites to increase perceive control in the consumers (Arcand et al., 2007). It is applied by online shopping websites to reduce consumers' perceived concerns of online transactions (Han Zhang, 2005). Assurance seals convince buyers that a website has been controlled and monitored by the third party and that it has met the acceptable level of service. Given that third-party assurance seals affect consumer's purchase intention through reducing their concerns about the risks exists in online shopping, we expect its effect on purchase intention is mediated by the key concerns. Thus, we hypothesize that:

H6a: Online consumers' concerns mediates the effect of assurance statements on purchase intention.

H6b: Online consumers' concerns mediates the effect of assurance seals on purchase intention.

We also include gender and past experience with the e-commerce website as control variables, because online consumers may have different perceptions on assurance mechanisms and different level of concerns in terms of gender and e-commerce experience (e.g., Chen & Sharma, 2015; Wakefield, 2013)

Methodology

Instrument Development and Data Collection

To measure all research constructs, measurement items from previously validated were identified and adjusted. All measurement items are listed in Appendix A. A set of survey data was collected from students in a large public university in the southwest United States. Survey responses were only from students who had an ongoing shopping experience. We asked them about their ongoing attempts to buy a product online and to answer the questions on the survey based on their shopping experience. The original sample consists of 335 responses. After removing incomplete and invalid responses, we ended up with 321 usable responses. Table 4 summarizes the demographics of the participants in the study.

Table 4
Demographics

Demographic	**Distribution**		
Gender	215 Male (67%)	106 Female (33%)	
Age	135, 18-21 years (42%)	96, 22-25 years (33%)	90, 26 years or older (25%)
Academic status	293 undergraduate students (91%)	28 graduate students (9%)	

Measurement and Structural Model

We used Partial Least Square (PLS) with Smart PLS as our statistical analysis tool to test the proposed hypotheses. PLS uses metric properties of the scales in order to measure variables, as well as the strength and direction of relationships among these variables (Barclay, Higgins, & Thompson, 1995). PLS offers a wide range of benefits which are valued in this research: (1) suitability to exploratory research where relationships have not been previously tested, (2) tolerance of possible violations of multivariate normality and use of non-interval scaled data, (3) avoidance of parameters estimation biases, and (4) independence of parameter estimation from sample size (Henseler, Ringle, & Sinkovics, 2009). Our study explores the joint effects of two popular e-commerce design features – assurance statements and third-party assurance seals – on consumers' purchase intention, which has received little attention in the existing literature. PLS is therefore appropriate. We conducted a three step analysis procedure: (1) analyzing the measurement model in order to assess item reliability and validity, (2) checking the common method bias, and (3) analyzing structural model assessment to assess the model's predictive power.

The adequacy of the measurement model is an important concern which is assessed by analyzing reliability, internal consistency, and discriminant validity (Hulland, 1999). Internal consistency of each construct is assessed by analyzing Cronbach's alpha, composite reliability, and Average Variance Extracted (AVE) (Hair Jr, Anderson, Tatham, & William C, 1995). Cronbach's alpha and composite reliability are supposed to be at least 0.50 (Nunnally & Bernstein, 1978) while AVE is more than 0.50 (Fornell & Larcker, 1981). In Table 5, the diagonal values represent the square root of AVE which is measured for variance shared between a construct and its indicators, or convergent validity. According to Table 5, Cronbach's alpha, composite reliability, and AVE values prove the internal consistency of constructs based on the above constraints.

Table 5
Reliability and validity

Constructs	AVE[a]	CR[b]	CA[c]	1.	2.	3.	4.	5.	6.
1. Assurance Statements	0.84	0.94	0.9	**0.92**					
2. Assurance Seals	0.82	0.93	0.89	0.51	**0.91**				
3. Privacy Concerns	0.68	0.91	0.88	-0.45	-0.25	**0.82**			
4. Product & Service Concern	0.72	0.89	0.83	-0.26	-0.12	0.34	**0.85**		
5. Transaction Security Concern	0.78	0.95	0.93	-0.65	-0.52	0.30	0.31	**0.88**	
6. Purchase Intention	0.85	0.95	0.91	0.46	0.37	-0.31	-0.21	-0.57	**0.92**

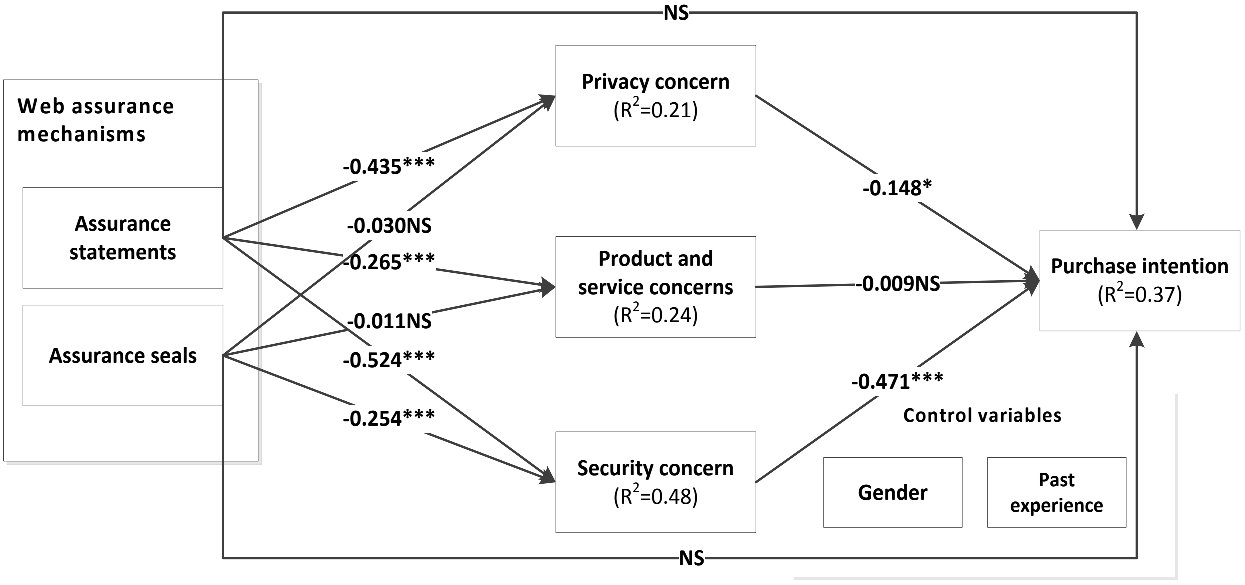
Note. The diagonal elements (in bold) represent the square roots of AVE.
[a] Average variance extracted. [b] Composite reliability. [c] Cronbach's alpha.

There are two constraints for examination of discriminant validity. First, AVE values are supposed to be greater than off-diagonal correlations. Second, each construct related item must load highly on the construct it is measuring and cross-loadings are supposed to be lower than the within-construct item loadings (Ko, Kirsch, & King, 2005). Appendix B reflects the loading values of all the items used in the measurement instrument. The two criteria for examination of discriminant validity are acceptable.

Common method bias could be important source of measurement errors (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). According to Campbell and Fiske (1959) presence of common method bias in measurement causes erroneous conclusions. We apply two different methods to evaluate check the presence of common method bias. We use Harman’s single factor test as the first method. According to Podsakoff et al. (2003), there are two conditions for the presence of common method bias: (1) presence of a single factor in the factor analysis, (2) presence of a single factor which accounts for the majority of the covariance among the variables. We conduct unrotated factor analysis for all 22 items and the results indicate 6 factors account for 79 percent of the variance in the data while the first factor accounts for less than 50% of the total variance. Therefore, using Harman’s single factor test we conclude that common method bias is unlikely to be present in our measurement model.

As the second method to test presence of the common method bias we used the approach suggested by Podsakoff et al. (2003) following the procedure of Liang, Saraf, Hu, and Xue (2007). The results of the test (See Appendix C) indicate that the theoretical constructs are loaded highly significant compared to common method bias construct. In fact, in almost all cases the items are loaded in significantly on common method bias construct. Thus we conclude that the common method bias does not seem to be serious issue in our measurement model.

In order to assess the structural model, we need to examine path coefficients and R-square values. The path coefficients show the strengths of the relationships between independent and dependent variables in the model and R-square values indicate the predictive power of the model for dependent variables. To test the statistical significance of path coefficients, a bootstrapping technique was used. The overall results of the analysis are shown in Figure 4.



Note. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (Two-tailed significance); NS: Not significant

Figure 4. Results of PLS analysis

Both privacy concern and security concern have a negative and significant effect on purchase intention with β = -.145 and β = -.473, respectively, supporting H1 and H3. Unlike our expectation, product and service concern does not have significant influence on purchase intention, not supporting H2. Regarding the effects of two assurance mechanisms, assurance statements significantly reduce privacy concern (β = -.436), product and service concern (β = -.265) and security concern (β = -.254); Assurance seals only significantly influences security concerns (β = -.254). Thus, H4a, H4b, H4c, and H5c are supported while H5a and H5b are not. Approximately 33% of variance in purchase intention is explained by the three focal concerns; About 21%, 24% and 48% of privacy concern, product and service concern, and security concern are explained by both assurance mechanism, respectively. Regarding control variables, the results show that gender and past experience with the e-commerce website are not significant as control variable in this study.

Considering recent critiques of the traditional mediation tests (Zhao, Lynch, & Chen, 2010) introduced by Baron and Kenny (1986), this study applied the recent view on mediation analysis proposed by Preacher and Hayes (2004)[1]. Our theoretical model corresponds to a multi-mediator model (Hayes, 2013) in which the effect of independent variables (i.e., assurance seals and assurance statements) on the dependent variable (i.e., purchase intention) is mediated by online consumer concerns (H6a and H6b). We used the Preacher and Hayes (2004) applying Preacher and Hayes (2008) to test H6a and H6b. Table 6 summarizes the results of the mediation effect tests. According to Zhao et al. (2010), if the bootstrap confidence intervals for the estimates of the indirect effects does not include zero and the indirect effect of independent variable on the dependent variable is significant then there is a mediation effect. Based on the results of the mediation tests, we can conclude that consumers' concerns mediate the effects of both assurance statements and assurance seals, supporting H6a and H6b.

To make sure that our research design and analysis had enough power to find the significant relationships for all the dependent variables in this study, we applied the power analysis method for multiple regression suggested by Cohen (1988) and Cohen, Cohen, West, and Aiken (2013). The results of the power analysis show that the calculated powers of all the

[1] This method overcomes some issues identified of traditional methods by focusing on ordinary least squares (OLS) regressions supplemented by analyses based on bootstrapping for assessment of indirect effects. According to MacKinnon, Lockwood, and Williams (2004)this method has been shown to constitute a more valid and powerful method for assessing indirect effects.

dependent variables is more than .95. Therefore, statistical power of our analysis is not an issue in this study.

Table 6

Preacher-Hayes mediation effect test results

Hypothesis	**Relationship**	**95% Confidence Interval**		**Indirect Total Effect (t-value)**	***p*-value[a]**	**Supported**
		Lower	**Upper**			
H6a	Assurance Statements→Purchase Intention-Mediated by Consumers Concerns	0.276	0.485	0.485 (9.46)	< 0.001	Yes
H6b	Assurance Seals→Purchase Intention-Mediated by Consumers Concerns	0.208	0.362	0.355 (7.18)	< 0.001	Yes

Note. [a] $p < 0.05$ is significant

Post-hoc Analysis

To examine whether the two assurance mechanisms complement or substitute each other, this study examines the interaction effects of assurance seals and assurance statements on the three consumer concerns. We applied the method suggested by Chin, Marcolin, and Newsted (2003) to examine the interaction effects using Smart PLS. The analysis results (See Table 7) reveal that the interaction effect of assurance seals and assurance statements on privacy concerns and product and service concerns are significant ($p < 0.001$). In contrast, the interaction effect of the two assurance mechanisms on transaction security concerns is not significant ($p > 0.05$). This finding suggests that the two mechanisms studied in this work complement each other in such a way that when one mechanism is available the effect of the other one on consumer concerns will increase.

Discussion

The results show that privacy concern and security concern are important to online consumers as they relate to consumers' purchase intention; assurance seals and assurance statements are important remedies for these two concerns. Unlike our expectation, the effect of product and service concern on purchase intention is not significant. This finding contradicts previous studies (e.g., Miyazaki & Fernandez, 2001; Spreng, Harrell, & Mackoy, 1995) that have posited a significant negative effect of online consumers' concern on their purchase decision. One possible explanation for this contradiction is that most of our respondents chose popular online shopping websites such as Amazon and eBay and, therefore, did not have much concern with product and service risks. The great wealth of consumer data in these major websites is likely to attract cyber criminals around the globe and, hence, subject the sites to more transaction security issues. Meanwhile, the large accumulation of consumer data on these sites may also entice vendors to monetarize consumer privacy for profits. Therefore, privacy concern and transaction security concern still represent valid concerns for consumers who visit these shopping websites.

Table 7

Test results for interaction effect of assurance mechanisms on consumer concerns

Relationship	Coefficient
Assurance Statements × Assurance Seals → Privacy Concerns	-0.246***
Assurance Statements × Assurance Seals → Product & Service Concerns	-0.207***
Assurance Statements × Assurance Seals → Transaction Security Concerns	-0.108^{NS}

Note. *** $p < 0.001$, ^{NS} Non-significant

In addition, we test the mediating role of consumer concerns using Preacher-Hayes mediation test method and the results confirmed the mediating effect of consumers' concerns. Another interesting finding is that third-party assurance seals negatively relate to one's transaction security concerns whereas assurance statements negatively relate to all three concerns. Compared with third-party assurance seals which cast a total effect of 0.12 (-0.254*-0.473), assurance statements have a greater total effect of 0.31 (-0.436 × -0.145 + -0.524 × -0.473) on consumers' purchase intention. This suggests that online vendors may opt for more selfreliance (i.e., own assurance statements) than seeking external assistance (i.e., third-party assurance seals) in mitigating consumer concerns.

In summary, online consumer purchase intention is affected by consumer's concerns regarding privacy and transaction security in e-commerce websites. Online shopping websites could increase consumers' purchase intentions by decreasing these concerns through the use of assurance mechanisms in their websites. The interaction effect of assurance statements and seals on privacy concerns and product and service concerns are significant; this result suggests that the two mechanisms studied in this work can be complement of each other in such a way that when one mechanism is available the effect of the other one on consumer concerns will increase.

Implications

The study contributes to literature in several ways. Firstly, our study categorizes online consumers' concerns and empirically tests the relationship between these concerns and consumers' purchase intention. In line with procedural fairness theory, our research model underscores the value of web assurance mechanisms in mitigating consumers' concerns. Previous researches in this context suggested that popular assurance mechanisms affect consumers' purchase intention by influencing consumers' trust (e.g., K. M. Kimery & M. McCord, 2002; McKnight, Choudhury, & Kacmar, 2000). In this paper, we posit consumers' concerns instead of trust as mediators for the effect of web assurance mechanisms. We suggest that web assurance mechanisms on the website negatively affect concerns that consumers have in their online shopping experience so that purchasing decisions can be made easier. That is why we believe that consumer concerns play more important role in this situation. Post hoc analysis further shows the two assurance mechanisms complement each other in affecting consumer concerns.

Second, we empirically confirm that online consumers' concerns mediate the effect of assurance statements and assurance seals on purchase intention. These findings contribute to the existing literature by supporting that consumers' concerns should be considered as an important mediation for purchase intention, which has been omitted as consideration in previous studies. Future researchers could apply our research model to different contexts such as mobile commerce in order to further examine the importance of consumers concerns.

Third, we find product and service concern as an insignificant predictor for consumers' purchase intention. This is an interesting finding because it is not consistent with the result of other studies (e.g., Miyazaki & Fernandez, 2001; Spreng et al., 1995). This contradictory finding may show that online consumers are not much concerned about the products and services that provided by the online vendors; they are more concerned about fraudulent behaviors of the online vendors including misuse of their personal information and transaction related information (Olivero & Lunt, 2004). Interestingly, this finding suggests the differentiating importance of the three concerns. That is, consumer concerns on security and privacy are deemed more important than concern on product and services (a non-information security related concern), when the three are jointly considered by online consumers. Findings as such as new to the literature on consumer concerns as they underscore security and privacy as pronounced threats to online users.

From practical perspective, this study has a number of implications. First, our study's results show that an assurance seal does not have any effect on a consumers' perceived privacy and product and service concerns. One possible explanation is that the online shopping websites have not communicated the assurance seals' values to the consumers appropriately. Because of a lack of communication consumers are not able to understand the value of the assurance seal. In response to this finding, vendors of online stores may provide educational materials that help consumers uncover the true meanings of assurance seals. Doing such may help leverage more benefits of assurance seals as one effective assurance mechanism.

Second, the study stresses the effect of privacy and transaction security concerns on consumers' purchase intention and explains this effect by using assurance mechanisms, online vendors could decrease these concerns and increase their sale and profitability. Therefore, this could be an important implication for practitioners to decrease their consumers concerns. For the least, vendors may prioritize their resources on these two assurance mechanisms. Finally, although assurance seals negatively affect consumers' privacy concerns, assurance statements affect all the three categories of concerns discussed in this study. Thus e-commerce websites may benefit from this finding by improving the assurance statements that they use on their website to decrease their consumers' concerns more than before.

Limitations and Future Research

Like any other studies, this study has a number of limitations. The first limitation of our study is that we used university students as our sample frame. Some researchers argue that a student sample lacks external validity (Gordon, Slade, & Schmitt, 1986), though there are a number of studies in the context of e-commerce that used students as their sample frame (e.g., France Belanger et al., 2002; Pavlou, 2003; Yenisey, Ozok, & Salvendy, 2005). Another limitation of our study is that our research model only focused on the effect of consumers concerns on purchase intention. The reason for this is because the primary focus of our research was in finding the effect of assurance mechanisms on purchase intention. According to the Valance framework by Peter and Tarpey Sr (1975), consumers used three factors to product purchase decisions: (1) minimizing perceived risk, (2) maximizing perceived return or benefit, and (3) maximizing net benefit which is defined as the difference between perceived benefit and risk. Thus, lack of consideration of benefit in our research model could be one limitation for our research that could be addressed by future studies. The third limitation of our research is that we did not consider personal factors such as risk aversion discussed by Donthu and Garcia (1999) in our model. For the sake of parsimony, we focus on consumers' concerns in our research while avoiding the involvement of other factors discussed by previous researchers (e.g., Chang et al., 2005).

Conclusion

Although, there has been a rapid growth in the e-commerce growth in the recent years, online consumers still have different concerns whenever they interact with these websites. Web assurance mechanism are one of the information assurance measures that e-commerce websites use to affect these concerns. Applying procedural fairness theory, this study examines how web assurance mechanisms influence consumers' purchase intention by affecting their privacy, transaction security, and product and services concerns. Whereas assurance seals only affect consumers' transaction security concerns, web assurance statements affect all the three concerns of consumers in the research model. This finding reveals that online consumers' web assurance statements are a more effective mechanism than assurance seals in the e-commerce context. Moreover, we find the two assurance mechanisms complement each other in mitigating consumer concerns. In addition, this work's findings show that consumers' purchase intention is only affected by privacy and security concerns, but not non-information security concerns such as the product/service concern. Finally, we find that online consumers' concerns mediate the effect of the two assurance mechanism on consumers purchase intention.

ESSAY III: A STUDY OF THE EFFECT OF PRIVACY ASSURANCE MECHANISMS ON SELF-DISCLOSURE IN SOCIAL NETWORKING SITES FROM THE VIEW OF PROTECTION MOTIVATION THEORY

Introduction

Along with recent advancement of web technologies, social networking sites (SNSs) affect people's life styles by enabling them to perform so many different activities which were not easy to do before. Ofcom technology tracker reports that over 50% of the internet users stated that using SNSs is one of the major reasons of using the Internet (Ofcom, 2014). SNS users are able to quickly access and easily share personal information and opinions such as pictures of friends and family, and political views (Jiang et al., 2013). Because of such predominant and rampant of SNSs, users' information privacy issues become important challenge not only for SNS users but also for the SNS service providers and governing organizations (Boyd & Ellison, 2010).

Rainie et al. (2013) report that more than 50% of the Internet users express that they are concerned with their information privacy; 66% of them posit that current law does not protect them against privacy threats. Moreover, results of a survey, conducted in the United States, reveal that among the SNS users who are concerned with information privacy, majority of them still disclose their personal information on SNSs (Madden, Fox, Smith, & Vitak, 2007). It seems that many SNS users tend to disclose their personal information in SNSs while they are still concerned with the privacy of their information. Thus, it is interesting to investigate why SNS users are still interested in sharing their information on SNSs while they are concerned with their privacy. We guess several reasons for this contradictory sharing behavior of SNS users. One possible reason is that SNSs are applying several privacy assurance mechanisms to ensure their users concerns with their privacy (Squicciarini, Paci, & Sundareswaran, 2010). Therefore, it is an interesting and timely issue to empirically test the effect of privacy assurance mechanisms on SNS users' privacy concern and behavioral intentions such as protection motivation and information disclose behavior.

Drawing upon the literature review on online privacy concern, we identify that while the information system research has made some progresses on understanding antecedents of SNS users' privacy concern, still there are some gaps that should be addressed. First, although practitioners applied different mechanisms to address privacy concern, there are some gaps in the literature regarding theory-oriented investigation of how these mechanisms affect online privacy concern (Bansal et al., 2008; Kim, Steinfield, et al., 2008; Squicciarini et al., 2010). Second, privacy assurance mechanisms are mostly investigated in the e-commerce context. Thus, there is a gap in the literature on how privacy assurance mechanisms affect SNS users' privacy concern and disclosure behavior. Third, protection motivation theory (PMT) has been applied in IS literature to study protection attitudes and behavior (e.g., Bulgurcu, Cavusoglu, & Benbasat, 2010; Crossler, Long, Loraas, & Trinkle, 2014; Herath & Rao, 2009; Johnston & Warkentin, 2010) without considering fear or risk as part of PMT (Floyd, Prentice-Dunn, & Rogers, 2000; Tanner Jr, Hunt, & Eppright, 1991). Hence, there is an opportunity to apply PMT in the SNS context to investigate online privacy concern and self-disclosure by applying the concept of fear from PMT. Finally, although PMT suggests that fear appeal process leads to change in attitude and behavior regarding a threat, most of previous studies only investigated fear appeal effect on protection related behaviors. Prior studies mostly investigated the effect of protection motivation on behavioral intention to uses protection mechanism. Our study may be able to investigate whether fear appeal process suggested by PMT can affect SNS users to not to disclose their information or just motivate them to protect their information by applying different types of protection mechanisms other than those they currently use.

To address the existing gaps, we focus on a set of privacy assurance mechanisms used on most SNSs and propose a risk calculus process in which these mechanisms affect SNS users' privacy concern and self-disclosure behavior. Therefore, the objectives of this research are:

- To study how privacy assurance mechanisms affect SNS users' protection motivation by applying PMT as the theoretical lens.
- To investigate the influence of privacy concern as part of the PMT on SNS users' protection motivation and self-disclosure.

This study formulates a conceptual research model by applying PMT as the overarching theory. PMT postulates that individuals' protection motivation is formed by a cognitive process. In this cognitive process individuals evaluate the effectiveness of the in hand coping mechanisms and the existing threat. The output of this cognitive process which is named fear appeal is the level of protection motivation in an individual (Maddux & Rogers, 1983; Rogers, 1975). More specifically, PMT posits that an individual's protection motivation is the result of their fear of a threat and this fear is the consequence of the threat significance and coping power that an individual perceives.

In addressing our research objectives, we argue that the existing privacy assurance mechanisms on a SNS influence Users' appraisal of threat severity and vulnerability, and coping mechanisms. This appraisal process forms a level of privacy concern of users. Finally, their level of privacy concern affects their motivation to protect their information and disclose themselves on a SNS.

This study makes a number of contributions. (1) This work extends the information assurance literature by applying PMT to theoretically explain the risk calculus process in which users' privacy concern is formed. (2) This paper also introduces protection motivation as a mediator of the effect of privacy concern on self-disclosure which was overlooked by prior studies. (3) We also introduce privacy customization features exist on the SNS as another type of privacy assurance mechanism which have not been studied by previous research. (4) Although previous research has investigated privacy assurance mechanisms in e-commerce context, this study is one of the first studies that investigates privacy assurance mechanisms on SNSs. (5) SNSs may apply the findings of this study to decrease users' privacy concern and motivate them to share more personal information about themselves. To this end, they can provide more in-depth privacy assurance statements and design more customizable privacy related features to influence the risk calculus process that affects users' privacy concern.

Literature Review

Assurance Mechanisms, Privacy Concern, and Online Self-Disclosure

Online privacy assurance refers to "mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website" (Bansal et al., 2015a, p. 2). SNS users can be considered as customers in this definition. Privacy assurance mechanisms have been studied in e-commerce context with different research constructs (Bansal et al., 2015a): most studies explore the effect of privacy assurance statement as a primary privacy assurance mechanism on trust in e-commerce websites (Liu et al., 2004; McKnight et al., 2002; Wu et al., 2012); some others investigate its effect on intention to disclose information (Meinert et al., 2006; Peterson et al., 2007; Wang et al., 2004).

Self-disclosure refers to “what individuals voluntarily and intentionally reveal about themselves to others – including thoughts, feelings and experiences” (Posey, Lowry, Roberts, & Ellis, 2010, p. 183). Self-disclosure is an activity that has several benefits and risks for the person who performs this activity (Xu, Teo, Tan, & Agarwal, 2009). Self-disclosure has been investigated in many contexts. A group of studies elaborated the factors that affect customers to disclose their information on e-commerce websites (e.g., Culnan & Armstrong, 1999; Dinev & Hart, 2004; Laufer & Wolfe, 1977). Some other studies investigated the antecedents of information disclosure on SNSs (Chen, 2013; Chen & Sharma, 2015; Jiang et al., 2013; Posey et al., 2010).

Prior research posited different factors that affect online self-disclosure. Posey et al. (2010) suggested that social benefits and costs together with social norms and perceived collectivism influence online community users to disclose their personal information. Extroversion and internet risk are other factors that were suggested by previous studies as antecedents of self-disclosure (Chen, 2013; Chen & Sharma, 2015). Koohikamali, Gerhart, and Mousavizadeh (2015) also argued that incentives may affect SNS users to disclose their location (as a type of personal information).

Different theories has been applied by previous studies to investigate self-disclosure behavior on online communities (Li, 2012). Risks and benefits trade-off perspective was applied by several researchers to explain the antecedents of self-disclosure. Jiang et al. (2013) suggested that privacy concerns and social rewards are important antecedents of self-disclosure behavior on SNSs. The trade-off between disclosure-privacy benefits and risks was suggested as an important factor that affects self-disclosure on online communities (Xu et al., 2009). Prior researches posit several benefits of self-disclosure such as formation of intimacy with others (Altman & Taylor, 1973), social acceptance or opinion leadership (Chen, 2013), reduction in stress by emotional experiences (Greenberg & Stone, 1992). Some other studies suggest privacy concern as the main risk for individuals when they share their personal information on online communities (Dwyer, Hiltz, & Passerini, 2007; Ioinson & Paine, 2007). Theory of reasoned action by Fishbein and Ajzen (1975) is another theoretical lens that was used by several studies to investigate the antecedents of self-disclosure behavior (Chen & Sharma, 2015; Koohikamali et al., 2015).

Information privacy refers to "an individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization" (Buchanan, Paine, Joinson, & Reips, 2007, p. 158). Many studies used different theoretical perspectives to study antecedents of privacy concern in online environment (Li, 2012). Privacy calculus theory is one of the theories used by several studies to frame the antecedents of online privacy concern (Culnan & Armstrong, 1999; Dinev & Hart, 2004, 2006; Hann, Hui, Lee, & Png, 2007). This theory suggests that individuals intend to disclose information based on a calculus of positive and negative outcomes of disclosure behavior (Li, 2012). Another theoretical lenses that has been used to study online privacy concern are personality theories (e.g., Bansal & Gefen, 2010; Junglas et al., 2008; Korzaan & Boswell, 2008). Studies that applied these theories aimed to investigate the personality related factors that affect individuals' online privacy concern.

Background Theory

PMT, developed by Rogers (1975), explains and predicts protection attitudes and behaviors of an individual who is exposed to a threat (Maddux & Rogers, 1983; Rogers, 1975; Weinstein, 1993). This theory is one of those theories that has been used by researchers to investigate the privacy in different contexts (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009; Dinev & Hart, 2004; Junglas et al., 2008; Youn, 2009). PMT suggests that there are three important component in fear appeal: (1) the severity of the threat' negative outcomes; (2) The probability that the threat occurs; and (3) the efficacy of protective responses (Rogers, 1975). Maddux and Rogers (1983) revise the original version of PMT by adding self-efficacy as the forth component that affects protection motivation behavior. PMT suggests two cognitive processes that an individual carry out to cope with a threat: threat appraisal and coping appraisal. As the output of this process a level of fear from the threat is formed in an individual (Floyd et al., 2000; Maddux & Rogers, 1983).

Generally, threat is defined as "something that is a source of danger that can bring harm (physical or mental) to an individual" (Junglas et al., 2008, p. 390). According to PMT, threat appraisal is a process of estimating the severity and susceptibility of a threat while coping appraisal refers to the process of evaluating the efficacy of protection responses and the perceived self-efficacy of the individual who is exposed to the threat (Junglas et al., 2008). While the original and the revised versions of the PMT suggest that the threat and coping appraisal are parallel processes that happen concurrently (Maddux & Rogers, 1983; Rogers, 1975), a number of studies argue that these two processes are sequential (Scherer, 1988; Tanner Jr et al., 1991). Tanner Jr et al. (1991) argue that threat appraisal must occur prior to other evaluations such as coping appraisal. PMT also addresses that there are two sources of information that influence the threat and coping appraisal: environmental and inter-personal sources of information. Environmental sources of information are verbal persuasion and observation and inter-personal sources consist of personality variables and prior experiences (Floyd et al., 2000).

Research Model and Hypotheses

In this study we applied PMT as the background theory to investigate self-disclosure behavior of SNS users. PMT was applied in several previous researches to study online privacy concern in different contexts (e.g., Mohamed & Ahmad, 2012; Youn, 2009). For example, Youn (2009) applied PMT to study privacy concern and factors influence website users to provide personal information to the websites. Thus, this study created the research model based upon PMT. Applying PMT, privacy assurance statement and privacy customization features on the SNS are considered as environmental sources of information that influence users' threat and coping appraisal. SNS users process these sources of information to evaluate vulnerability of and severity from the threat. They also evaluate the effectiveness of privacy assurance mechanisms and their self-efficacy based on these sources of information. Prior research named this evaluation process as risk calculus (Li, 2012) in which users evaluate the threat significance and coping strength of themselves. The output of the risk calculus process is their perceived fear of or concern with sharing personal information on SNS. According to PMT, users' fear from threat (privacy concern) influence their protection motivation and protection-related behavior (Maddux & Rogers, 1983; Rogers, 1975; Weinstein, 1993).

Considering PMT as our theoretical lens in the context of SNSs, we propose our research model (see Figure 5). This research model proposes that privacy assurance mechanisms affect SNS users' privacy concern via the cognitive process of risk calculus; SNS users' privacy concern affects their protection motivation (As the output of PMT) and the self-disclosure behavior; and protection motivation mediates privacy concerns on self-disclose behavior.

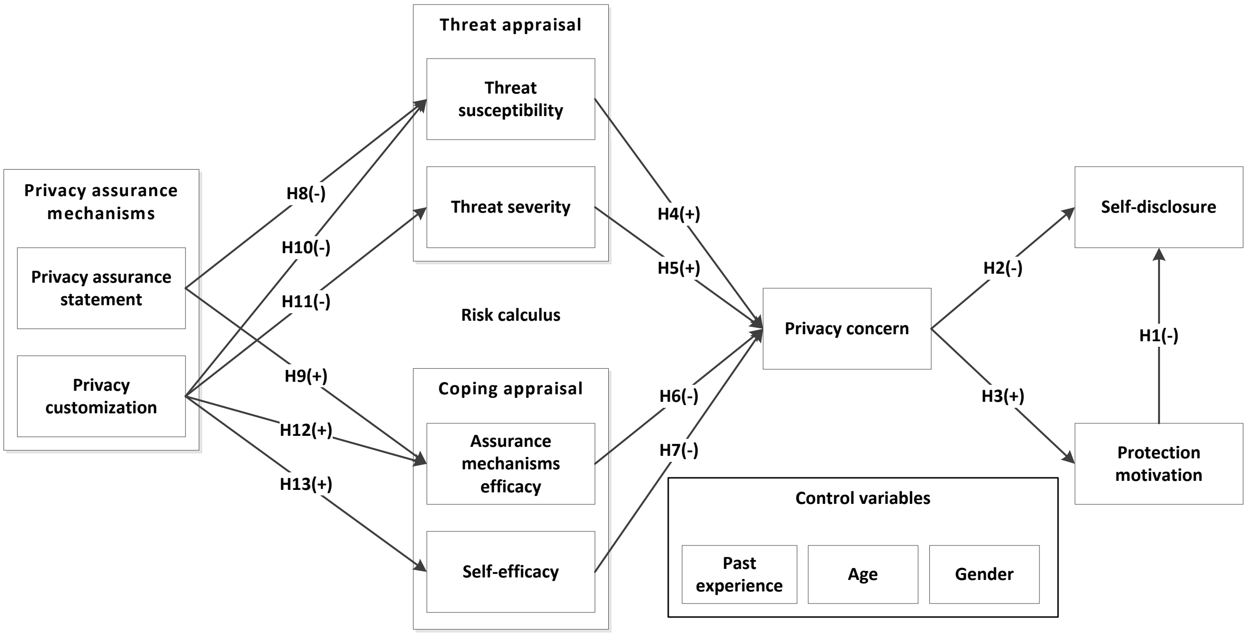


Figure 5. Research model

PMT suggests that protection motivation refers to individual's intention to perform protection behavior (Boer & Seydel, 1996; Norman, Boer, & Seydel, 2005). Theory of reasoned action argues that Behavioral intention regarding a behavior affects an individual to perform that behavior (Fishbein & Ajzen, 1975). Therefore, when SNS users are more motivated to protect their information, they perform protective behaviors. According to Wurtele and Maddux (1987) individuals who are more motivated to perform protective behavior, employ "pre-caution strategy". In this strategy they act cautiously to be safe from the threat. Raman and Pashupati (2004) argue that individuals employ two different strategies to protect their privacy in the internet: approach, and avoidance. Approach strategy results in seeking for a solution and avoidance strategy lead users to refuse using internet. When SNS users want to protect their privacy on the SNS, it is more likely for them to employ avoidance strategy since they already evaluated the coping mechanisms and based on their evaluation they are motivated to protect their privacy. In other words, some SNS users are intent on protecting their information based on their appraisal of threats and coping mechanisms in that situation. These users know that there is only one solution for them to protect their information since they are already applying the existing assurance mechanisms. This solution is to not to disclose their personal information. Other SNS users who are not intent on protecting their information based on their appraisal of the SNS will not be that cautious regarding sharing their information. Hence, they are more likely to share their personal information on the SNS. So we hypothesized that:

H1. The amount of protection motivation SNS users feel negatively affects their self-disclosure behavior.

Dwyer et al. (2007) suggest that SNS users who are more concerned with their privacy, share their information less frequently on SNS compare to those who have not such concern. Privacy concern is suggested as an important impediment for internet users whenever they want to share their information on the internet (Youn, 2009). Online privacy concern is defined as "individuals' concern about the threat to their information privacy when submitting their personal information on the Internet" (Bansal et al., 2015a, p. 3). According to this definition, when SNS users perceive that the SNS cannot protect their information against a threat, they perceive more privacy concern. A possible reaction to this concern is to decide to not to share their personal information. Indeed, SNSs are supposed to provide protection over SNS users' information to address their privacy concerns otherwise users will not share their information on

SNS (Chen, 2013; Westin, 1967). This protection is a claim made by SNS and SNS is supposed to act based on that. This leads to the following hypothesis:

H2. SNS users' privacy concern negatively affects their self-disclosure behavior.

According to PMT, people assess their coping strength and their vulnerability when they make decision to share information. This assessment results in a certain level of fear from Threat. PMT argues that the more individuals fear from a threat the more they will be motivated to perform a protection behavior (Boer & Seydel, 1996; Floyd et al., 2000; Norman et al., 2005). Privacy concern in online communications refers to fear of being monitored, losing anonymity, identity theft, and so forth (Brown & Muchira, 2004; Lee, 2000; Milne & Culnan, 2004; Miyazaki & Fernandez, 2000, 2001; Youn, 2009). Hence, SNS users who are more concerned with their privacy on a SNS, feel more fear from sharing information on SNS. Users' privacy concern (fear of threat) affects users' behavioral intention to disclose their information (Bansal et al., 2015a; Pavlou, 2003). To response to this concern those who have higher level of concern, are more intent to protect their information on that SNS. Thus, we suggest that:

H3. SNS users' privacy concern positively affects their motivation to protect their information.

Threat appraisal process refers to the assessment of possible threats which exist in the relationship between SNS user and the SNS as a potential sources of harm or lose (Solomon, Mikulincer, & Benbenishty, 1989). Threat appraisal is a cognitive process in which an individual assess the risks of performing a specific behavior. The result of this assessment is a certain level of risk or fear perceived by that individual (Folkman, 1984). In the context of SNS, users assess the risks of sharing information in a similar way. SNS users evaluate severity of the potential negative outcomes of sharing personal information and their vulnerability to these potential outcomes. This assessment form the level of fear from sharing personal information on SNS. This fear of losing privacy named online privacy concern in online communications (Brown & Muchira, 2004; Lee, 2000; Milne & Culnan, 2004; Youn, 2009).

According to PMT literature, threat appraisal is the result of an assessment of threat severity and susceptibility (Rogers, Cacioppo, & Petty, 1983). Threat severity refers to the extent to which the SNS users are vulnerable to losing their privacy while the threat susceptibility refers to the probability of occurrence of a privacy threat (Johnston & Warkentin, 2010). When SNS users believe that the privacy threat is more probable to happen, they feel more fear from sharing their information. In fact, they perceive that they are more likely to be subjected to negative consequences of sharing information. Similarly, the severity of the potential negative consequences of sharing on SNS intensify SNS users' fear of losing privacy. As a result, we suggest the following hypotheses:

H4. SNS users' perceived threat susceptibility positively affects their privacy concern.

H5. SNS users' perceived threat severity positively affects their privacy concern.

Coping appraisal process refers to someone's assessment of his/her ability to cope with a threat (Rogers et al., 1983). According to PMT individuals' perception of their ability to avert with the threat affect their perception about the effectiveness of the coping responses (Rogers, 1975; Rogers et al., 1983). Therefore, they may perceive less fear of the threat when they believe that they are armed with effective coping mechanisms. Individuals' perception of having control over a specific situation is the result of their assessment of their coping ability in that situation. This perceived control affects individuals' perceived fear in that situation (Dinev & Hart, 2004;

Folkman, 1984). In the SNS context, privacy refers to someone's right to disclose his/her information (Westin, 1967). Individuals' control over their information is a condition of that right. SNS users' perception of coping ability against threat of losing information enhances their perceived control over the threat. Finally, SNS users, who have more control over their information, perceive less concern with their privacy.

PMT suggests that coping appraisal is broken to two separate processes: (1) to assess the effectiveness of the coping mechanisms that someone can use against a threat (response efficacy), and (2) to evaluate one's ability to apply coping mechanisms against a threat (self-efficacy) (Maddux & Rogers, 1983; Rogers et al., 1983). When SNS users feel that privacy assurance mechanisms are more effective, they perceive more control over their information. According to Bowman and Stern (1995), individuals' perceived control over a threat comes from their perception of the effectiveness of coping mechanisms. Additionally, self-efficacy is another important factor that affects someone's ability to protect his/her information by using coping mechanisms. Individuals' perception of their ability to use assurance mechanisms which are available on the SNS, affects their perceive control. Thus, they believe that they are able to control the threat whenever they are in a risky situation. These SNS users perceive less concern with sharing their information on the SNS. Therefore, we hypothesize:

H6. SNS users' perceived effectiveness of assurance mechanisms negatively affects their privacy concern.

H7. SNS users' self-efficacy negatively affects their privacy concern.

Privacy assurance mechanisms are considered as coping mechanisms to SNS users that enable them to protect themselves against threats of information disclosure (Bansal et al., 2015a). Privacy assurance statement refers to one of the main messages and arguments that websites communicate with their users to ensure the adequacy of their protection measures against users' privacy threats (Bansal et al., 2015a). In fact, in the context of this study privacy assurance statement refers the extent to which privacy assurance statement communicates SNS service providers' efforts and commitments toward preventing threats against users' privacy. According to Rogers and Thistlethwaite (1970), individuals who are exposed to threats seek to find assurance against those threats. Thus, SNS users seek to find information about how the SNS protect them against privacy threats. The more protection that SNS users perceive from the statement the less they perceive the privacy threat to be susceptible. The reason is that the privacy statement reflects how and for what purposes customer's information will be used. therefore, privacy assurance statement affects users to have better assessment of the risks of information disclosure behavior (Bansal et al., 2008). It means that the presence of privacy assurance statement helps them to better evaluate the susceptibility of privacy threats since they are more informed about SNS's privacy policy. In fact, the privacy statement assures SNS users that their information will be safe on the SNS and it will be used for the purposes that do not have any negative consequences for them. Consequently, we posit that:

H8. Privacy assurance statement negatively affects SNS users' perceived threat susceptibility.

Assurance mechanisms efficacy refers to effectiveness of the assurance mechanisms which are available on the SNS (Witte, 1992) such as privacy assurance mechanisms or privacy customization features. Privacy assurance statement on a SNS affects its users' evaluation of the coping mechanisms on the SNS. Presence of privacy assurance statement on a SNS reflects that the SNS aims to protect its users' personal information (Stutzman, Capra, & Thompson, 2011) and for this purpose that SNS develops several predefined processes. The main goal of Privacy assurance statement is to improve the awareness of SNS users regarding the SNS activities to protect users' privacy. Therefore, users understanding about this statement affects their perceive effectiveness of the SNS's assurance mechanisms. Thus, we suggest that:

H9. Privacy assurance statement positively affects SNS users' perceived effectiveness of privacy assurance mechanisms.

Privacy customization in this study refers to users' efforts to use technological features, available on the SNS, to protect their information privacy by controlling the flow of their information in SNS (Xu, Teo, Tan, & Agarwal, 2012). Those users' who set their privacy preferences are less likely to have any privacy issues compare to those who do not. Individuals employ "pre-caution" strategy in order to protect themselves from threat (Maddux & Rogers, 1983). Similarly SNS users limit the access of other users to their personal information to decrease the probability of the occurrence of privacy threat. Therefore, SNSs which enable users to customize their privacy preferences decrease their users' perceived threat susceptibility. Additionally, this cautious behavior of SNS users affect their perceived vulnerability to privacy threats. The reason is that the cautious users protect their information to be accessible by those trustable users. Thus, they will not lose their privacy as much as those who do not customize their privacy preferences. Consequently, we hypothesize that:

H10. Privacy customization features which are available on SNSs negatively affect SNS users' perceived threat susceptibility.

H11. Use of privacy customization features which are available on SNSs negatively affects SNS users' perceived threat severity.

When SNS users are able to change their privacy preferences on SNS (ability to specify who can see your posts, photos, and etc.), they perceive more control over the information they disclose on the SNS (Stutzman et al., 2011). Perceived control affects SNS users' perception regarding the effectiveness of the assurance mechanisms (Arcand et al., 2007). The privacy customization features on the SNS help users to cope with the risk of unauthorized access to their information. Therefore, these features affect their assessment of the coping mechanisms on the SNS. SNS users who are able to customize their privacy preferences are more likely to share their information. The reason is that they perceive that the SNS privacy customization feature is effective and is able to protect their privacy. If they did not have such perception they would not share their information on SNS. Additionally, SNS users' perceived control over their information affects their self-efficacy. They perceive that they are able to protect their information by using these features (Stutzman et al., 2011). In fact, these features influence users' perception of their ability to control others' access to their information. Users' perceived control influences their assessment of the coping mechanisms. As a result, we hypothesized that:

H12. Use of privacy customization features which are available on SNSs positively affects SNS users' perceived effectiveness of privacy assurance mechanisms.

H13. Use of privacy customization features which are available on SNSs positively affects SNS users' self-efficacy.

In addition, this study includes several control variables such as age, gender, and past experience in the research mode because prior studies has reported the potential impacts of age, gender, and past experience on the self-disclosure (Chen & Sharma, 2015; Wakefield, 2013).

Methodology

Instrument Development and Data Collection

Most of the items in our measurement model were adopted from prior studies. We defined some new items to measure a number of new constructs we proposed in this study (See Appendix D). The reason was that we did not find appropriate items in previous literature for those constructs. Moreover, we measured all items by using 7-points Likert scale.

The data was collected from undergraduate students of a large university in southwest United States. Students were voluntarily participated in online surveys with course credits. 256 students participated in our survey. Other than currently active users of SNSs, there were no other filtering criteria in this study. After removing incomplete and invalid responses, we ended up with a sample of 241 respondents indicating a usable sample size rate of 94.1%. Table 8 shows a summary of demographic information of the respondents. As shown in the table, ages is heavily weighted toward 18-25 years old (80.1%). Undergraduate students are mostly young and educated and this age group fits within the largest group of SNS users (Lenhart, Purcell, Smith, & Zickuhr, 2010).

Table 8
Demographics

Demographic	**Distribution**	
Gender	120 Male (49.8%)	121 Female (50.2%)
Age	193 respondents are within age group 18-25 years (80.1%)	
Dispensable Income per year	175 respondents have less than $15000 dispensable income (72.6%)	

Measurement and Structural Model

To test our research model we applied structural equation modeling by using Smart PLS 2.0. Partial Least Square (PLS) measures the direction of relationships and those strengths by using metric properties of the measurement scale (Barclay et al., 1995). This study applied three steps of analysis: (1) An assessment of measurement model by evaluating item reliability and validity, (2) a check for the presence of common method bias, and (3) a structural model assessment to evaluate the model's predictive power.

To check the adequacy of the measurement model, this study examined items reliability and validity (Hulland, 1999). The reliability of each construct is assessed by analyzing the Cronbach's alpha, and composite reliability. Values above 0.7 typically indicate acceptable reliability of the measurement model (Nunnally & Bernstein, 1978; Nunnally, Bernstein, & Berge, 1967). Average Variance Extracted (AVE) is also used to test for the convergent validity. AVE values above the benchmark of 0.70 are generally deemed as adequate and show that the latent variable explains more than half of the variation in the indicators (Fornell & Larcker, 1981). The diagonal values on Table 9 represent the square root of AVE. These are measures for the variance shared between a construct and its indicators and explain the convergent validity of the measurement model. The values of Cronbach's alpha, composite reliability, and AVE, demonstrate the internal consistency and convergent validity of the measurement model.

To test for the discriminant validity of the measurement model, this study applied two methods. First, AVE values are supposed to be greater than the off-diagonal correlations which is true in our case (see Table 9). Second, the related items of each construct are supposed to load highly on the factor the construct measures and cross-loadings are supposed to be lower than the within construct loadings (See Appendix E) (Ko et al., 2005).

Table 9
Reliability and validity

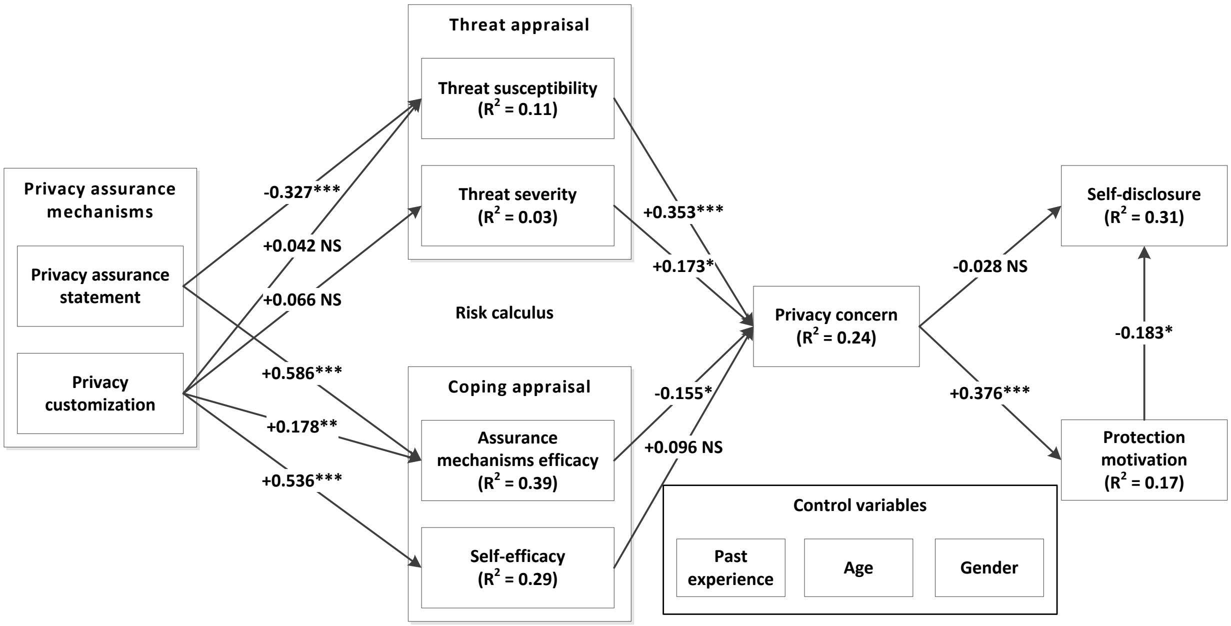
Construct	AVE[a]	CR[b]	CA[c]	1	2	3	4	5	6	7	8	9
1. Self-disclosure	0.71	0.91	0.89	**0.84**								
2. Protection motivation	0.73	0.93	0.91	-0.20	**0.85**							
3. Privacy concern	0.85	0.96	0.94	-0.07	0.38	**0.92**						
4. Threat susceptibility	0.81	0.95	0.94	-0.09	0.11	0.43	**0.90**					
5. Threat severity	0.85	0.96	0.94	-0.11	0.23	0.27	0.26	**0.92**				
6. Assurance mechanisms efficacy	0.86	0.95	0.92	0.15	0.08	-0.23	-0.31	-0.04	**0.93**			
7. Self-efficacy	0.88	0.96	0.93	0.23	0.15	-0.02	-0.14	0.01	0.43	**0.94**		
8. Privacy assurance statement	0.86	0.95	0.92	0.19	-0.12	-0.22	-0.33	-0.06	0.60	0.29	**0.93**	
9. Privacy customization	0.72	0.93	0.90	0.03	0.34	0.12	-0.06	0.07	0.21	0.54	0.06	**0.85**

Note. The diagonal elements (in bold) represent the square roots of AVE.
[a] Average variance extracted [b] Composite reliability. [c] Cronbach's alpha.

Common Method Bias (CMB) could be an important source of measurement error (Podsakoff et al., 2003). Presence of CMB may result in erroneous conclusions (Campbell & Fiske, 1959). To evaluate the presence of the CMB in our measurement model we applied two different methods. First we applied Harman's single factor test suggested by Podsakoff et al. (2003). They suggest that CMB exists in the measurement model in two conditions: (1) a single factor in the factor analysis, and (2) a single factor in factor analysis which accounts for majority of the covariance among the variables. The results of unrotated factor analysis for all 35 indicators show that 9 factors account for 80.4% of the variance and the first factor accounts for less than 50% of the total variance (21.9%). Hence, applying the Harman's single factor test for CMB, we conclude that CMB is not a serious issue in the measurement model.

The second method that we used to check for presence of CMB was an approach suggested by Podsakoff et al. (2003) following the procedure of Liang et al. (2007). As shown in Appendix F, the results revealed that the theoretical constructs were loaded highly significant while the CMB construct was loaded non-significant on all items in our measurement model. Therefore, CMB is unlikely to be present in our measurement model.

This study examined the path coefficients and R-square to assess the structural model. Path coefficient indicates the strength of the relationship between constructs and R-square shows the predictive power of the model. The results of the structural model assessment revealed that most of the hypothesized relationships are significant (See Figure 6). The results also revealed that the control variables were included in this study were non-significant (p > .05). Table 10 represents a summary of the results.



Note. * *p* < 0.05; ** *p* < 0.01; *** *p* < 0.001 (Two-tailed significance); NS: Not significant

Figure 6. Results of PLS analysis

Table 10
Summary of structural model assessment results

Hypothesis	Path coefficient	Result
H1: Protection motivation → Self-disclosure	-0.183*	Supported
H2: Privacy concern → Self-disclosure	-0.013	Not Supported
H3: Privacy concern→ Protection motivation	-0.376***	Supported
H4: Threat susceptibility → Privacy concern	+0.353***	Supported
H5: Threat severity → Privacy concern	+0.173*	Supported
H6: Assurance mechanisms efficacy → Privacy concern	-0.155*	Supported
H7: Self-efficacy → Privacy concern	+0.096	Not Supported
H8: Privacy assurance statement → Threat susceptibility	-0.327***	Supported
H9: Privacy assurance statement → Assurance mechanisms efficacy	+0.586***	Supported
H10: Privacy customization → Threat susceptibility	+0.042	Not Supported
H11: Privacy customization → Threat severity	+0.066	Not Supported
H12: Privacy customization → Assurance mechanisms efficacy	+0.178**	Supported
H13: Privacy customization → Self-efficacy	+0.536***	Supported

Note. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (Two-tailed significance)

Post-hoc Analysis

Because the structural model results revealed that the direct effect of privacy on self-disclosure is not significant, we examine the mediation role of protection motivation for the relationship between privacy concern and self-disclosure. Based upon recent critiques regarding (Zhao et al., 2010) the reliability of mediation test approach suggested by Baron and Kenny (1986), this study followed the approach developed by Preacher and Hayes (2008) to test the mediation effect of privacy concern. Table 11 summarizes the results of the mediation test.

Table 11

Preacher-Hayes mediation effect test results

Relationship	**95% Confidence Interval**		**Indirect Effect (t-value)**	***p*-value[a]**	**Supported**
	Lower	**Upper**			
Privacy Concern→Self-disclosure-Mediated by Protection Motivation	-0.135	-0.026	-0.112 (2.11)	0.013	Yes

Note. [a] $p < 0.05$ is significant

Discussion

The results of this study revealed that the privacy assurance statement affects privacy concern by decreasing the susceptibility of privacy threat and increasing perceived effectiveness of assurance mechanisms. Moreover, results of this study revealed that privacy customization features on SNSs do not have a significant influence on users' appraisal of the threat. One possible reason is that when SNS users use privacy customization features, they believe that there are some other threats such as threats from hackers, blackmails, and etc. that cannot be controlled by customizing privacy preferences. According to Xu et al. (2012), privacy customization is one of the technological approaches that is available on websites that enable users to protect their information. Xu et al. argue that there are several other approaches such as anonymous web surfing tools, cookie management tools, and etc. that enable website users to protect themselves about other types of threats. Therefore, these users perceive that some uncontrolled factors may still threat their privacy and privacy customization is not an appropriate mechanism to control these factors. The results of our study also support the positive influence of privacy customization features on the perceived effectiveness of assurance mechanisms and SNS users' self-efficacy. PMT postulates that people process available information in the environment to assess existing threats and their coping strength against these threats (Milne, Sheeran, & Orbell, 2000). Findings of this study support that assurance mechanisms on SNSs are considered as a source of information for users. These information enable users to evaluate privacy threats and their coping strength against them.

Additionally, our results posits a strong role for threat appraisal as an antecedent of privacy concern which is consistent with PMT point of view that suggests that fear results from threat appraisal (Rogers et al., 1983). Although the effectiveness of assurance mechanisms negatively affects privacy concern, there is no significant relationship between self-efficacy and privacy concern. The insignificant effect of self-efficacy is consistent with the results of previous studies in the online privacy concern literature (Youn, 2009). Furthermore, this paper found that privacy concern does not have a significant effect on self-disclosure. After we tested the mediator effect of protection motivation we found that protection motivation fully mediates the effect of privacy concern on self-disclosure. Finally, the results of this study revealed that age, gender, and past experiences does not matter in studying self-disclosure behavior in the context of SNS.

Implications

This study has implications for academia and practice. From a theoretical point of view, this study successfully applied PMT to investigate self-disclosure on SNSs. The PMT provided a theoretical lens for this study to conceptualize a model that explains the antecedents of self-disclosure on a SNS based on different assurance mechanisms that exist on that SNS. Moreover, the results of this study revealed that motivation protection mediates the effect of privacy concern on self-disclosure. Although prior researches have investigated the effect of privacy concern on protection motivation (Youn, 2009) and self-disclosure (e.g., Dwyer et al., 2007; Jiang, Chan, Tan, & Chua, 2010; Joinson, Reips, Buchanan, & Schofield, 2010), to the best of our knowledge this study is the first one that investigates the mediator effect of protection motivation on the effect of privacy concern on self-disclosure by applying PMT. Therefore, this paper makes novel contributions by extending PMT in the following ways. (1) This work is the first one that applied PMT to theoretically explain how privacy assurance mechanisms affect SNS users' privacy concern and ultimately their self-disclosure behavior. According to Bansal et al. (2015a) most of previous researchers studied privacy assurance mechanisms in the context of e-commerce. Hence, a contribution of our study is that this study investigates the effect of privacy assurance mechanisms on information disclosure in SNS by applying PMT. (2) this paper Introduced protection motivation as a mediator of the effect of privacy concern on self-disclosure which was overlooked by previous researches. (3) Our study introduced use of privacy customization features available on SNSs as a new construct that influences users' perceived effectiveness of privacy assurance mechanisms and their self-efficacy. The results of this study support the findings of previous studies (e.g., Xu et al., 2012) about the influence of self-protection approaches that exist on websites to enable users to protect their information. (4) Findings of our study showed that SNS users' privacy concern is the result a risk calculus process. In this process users perceive privacy concern based on the amount of risk that they perceive from privacy threat and their perceived effectiveness of privacy assurance mechanisms. This finding is an important contribution to previous studies that only focus threat appraisal component (e.g., Mohamed & Ahmad, 2012; Youn, 2005) of PMT. (5) According to Bansal et al. (2015a) most of previous researches studied privacy assurance mechanisms in the context of e-commerce. Hence, another contribution of our study is that this study investigates the effect of privacy assurance mechanisms on information disclosure in SNS by applying PMT. This study also provides several implications for practitioners. First, the findings of our study revealed that privacy assurance statement and privacy customization features on SNSs negatively influence users' privacy concern and consequently affect them to share more personal information. Thus, SNS website designers may apply findings of our study by empowering users to customize their privacy preferences more. Based on our findings, this empowerment motivates them to disclose their information. Moreover, SNSs can provide users with stronger privacy assurance statements as a tool to enhance users' perceived effectiveness of their assurance practices and consequently decrease their privacy concerns.

Limitations and Future Research

Like any other studies, this study has limitations. Although our conceptual model successfully explained the self-disclosure, there are some other factors that have not been investigated as the antecedents of self-disclosure behavior (Dinev & Hart, 2006). This affected our model power (R-square) since we just investigated risks of sharing personal information on the SNS. Future researches may investigate risks and benefits of sharing personal information on SNS. Additionally, using undergraduate students as our sample frame can be another limitation of this study. We believe that student data is a good sample for the study of social networking websites because it reflects a very high proportion of SNS users which are college students (Lenhart et al., 2010). Furthermore, our study lacks cultural diversity. We collected data from students of a university in United States. Different cultures may care about privacy differently (Wu et al., 2012). Thus, future studies may look at the differences in privacy concern among different cultures. Another possible limitation of this study is that personal trait was not studied in the research model. The reason that personal traits were not studied is that threat appraisal in this study is influenced by personal traits of the users (Junglas et al., 2008). In fact, assurance mechanisms have less influence on threat appraisal for those users who perceive more general privacy concern because of their personal traits and consequently these individuals have more privacy concern. Therefore, Future studies may consider the moderating effect of personal traits on the effect of assurance mechanisms on threat appraisal. Finally, this study does not captured the actual self-disclosure behavior of SNS users. As argued by Smith et al. (2011), the actual disclosure behavior of SNS users is a more predict measure than the intention to disclosure. In this study we address Smith et al. argument by measuring the disclosure behavior instead of the intention to disclosure. This study borrowed almost all of the measures from Koohikamali et al. (2015). They applied these items to measure actual behavior.

Conclusion

This study undertook the examination of the collective contributions of privacy assurance mechanisms on privacy concern and self-disclosure and the moderating effect of protection motivation. The PMT was applied as a theoretical lens for the conceptualization of the research model and interpretation of results. The results of the study revealed that privacy assurance mechanisms influence users' privacy concern by affecting their appraisal of a threat and the available coping mechanisms available on a SNS. This study also found that the effect of privacy concern is mediated by SNS users' protection motivation.

EPILOGUE

Online users' concerns affect their interaction with websites in different contexts such as electronic commerce, social networking websites, healthcare, and other contexts. This dissertation attempted to explore these concerns in electronic commerce and social networking websites and investigate how assurance mechanisms on website affect these concerns and users' behavior. The first essay examined the role of online privacy concern (OPC) by conducting a meta-analysis. The second essay investigated how web assurance mechanisms affect privacy, transaction security, and product and service concerns of online consumers. In addition, in this essay we focused on how these mechanisms affect consumers' purchase intention by influencing these concerns. Finally, the third essay studied how web assurance mechanisms influence social networking websites users' privacy concern and self-disclosure behavior.

In essay one we identified strong antecedents and consequences of OPC. Computer anxiety, interaction justice, disposition to privacy, privacy policy, perceived vulnerability, perceived anonymity of self, privacy control, perceived risks, reputation, regulations, familiarity, perceived anonymity of others, and negative experiences were identified as strong antecedents of OPC. Withholding, deflective behavior, protect, purchase intention, fabricate, risk, and trust were found to be strong consequences of OPC. We also found that although both users trust and perceived risk were studied as both antecedents and consequences of OPC, the results of meta-analysis indicated that these two variables are more likely to be antecedents of OPC.

The results of the second essay revealed that privacy and transaction security concerns negatively affect intention while product and service concerns are not significant indicators of intention to purchase. We also found that assurance statements cast an effect on consumers' purchase intention through privacy concern and transaction security concern, whereas third-party assurance seals affect consumers' purchase intention through transaction security concern only.

Finally, the third essay undertook the examination of the collective contributions of privacy assurance mechanisms on privacy concern and self-disclosure and the moderating effect of protection motivation. The PMT was applied as a theoretical lens for the conceptualization of the research model and interpretation of results. The results of the study revealed that privacy assurance mechanisms influence users' privacy concern by affecting their appraisal of a threat and the available coping mechanisms available on a SNS. This study also found that the effect of privacy concern is mediated by SNS users' protection motivation.

APPENDIX A

MEASUREMENT ITEMS - ESSAY II

Constructs	Item	Source
Assurance Statements	PAS1: I feel confident that the e-commerce website’s statements reflect their commitments to protect my transaction and personal information.	Xu, Dinev, Smith, and Hart (2011)
	PAS2: With the e-commerce website’s statements, I believe that my personal information will be kept private and confidential by my SNS.	
	PAS3: I believe that the e-commerce website’s statements are an effective way to demonstrate their commitments.	
Assurance Seal	AS1: The assurance seal makes me feel safe in online purchasing.	Lee, Choi, and Lee (2004)
	AS2: The assurance seal makes me feel comfortable toward the Web retailers.	
	AS3: The assurance seal is trustworthy.	
Privacy Concern	I am concerned that:	Chen, Han, and Yu (1996)
	PC1: This Website is collecting too much personal information from me.	
	PC2: This Website will use my personal information for other purposes without my authorization	
	PC3: This Website will share my personal information with other entities without my authorization.	
	PC4: I am concerned about the privacy of my personal information during a transaction.	
	PC5: This Website will sell my personal information to others without my permission.	
Product and Service Concerns	P&SC1: Purchasing from this Website would involve more product concern (e.g. not working, defective product) when compared with more traditional ways of shopping.	Kim, Ferrin, et al. (2008)
	P&SC2: Purchasing from this Website would involve more service concern (e.g. hard to refund, hard to return, poor delivery service, and …) when compared with more traditional ways of shopping.	
	P&SC3: How would you rate your overall perception of risk from this site?	McKnight et al. (2004)
	TSC1: This Website implements security measures to protect Internet shoppers	

Transaction Security Concern	TSC2: This Website usually ensures that transactional information is protected from accidentally being altered or destroyed during a transmission on the Internet	Chen et al. (1996)
	TSC3: I feel secure about the electronic payment system of this Website.	
	TSC4: I feel safe in making transactions on this Website.	Gefen (2000)
	TSC5: I am willing to use my credit card on this website to make a purchase	
Purchase Intention	PI1: I would consider buying this good from this website.	Jarvenpaa, Tractinsky, and Saarinen (1999)
	PI2: I will purchase this good from this website.	
	PI3: There is a strong likelihood that I will buy this good from this website.	

APPENDIX B

FACTOR LOADINGS - ESSAY II

	Mean	Std. Deviation	Assurance Statements	Assurance Seals	Privacy Concerns	Product & Service Concern	Transaction Security Concern	Purchase Intention
PAS1	5.45	1.33	**0.92**	0.45	-0.37	-0.28	-0.41	0.43
PAS2	5.55	1.20	**0.94**	0.45	-0.46	-0.23	-0.32	0.46
PAS3	5.68	1.56	**0.89**	0.41	-0.41	-0.21	-0.47	0.37
AS1	5.13	1.55	0.27	**0.93**	-0.23	-0.12	-0.51	0.34
AS2	5.10	1.47	0.37	**0.93**	-0.23	-0.08	-0.46	0.33
AS3	5.02	1.53	0.35	**0.85**	-0.24	-0.14	-0.45	0.34
PC1	3.52	1.53	-0.29	-0.12	**0.70**	0.36	0.17	-0.16
PC2	3.00	1.58	-0.36	-0.19	**0.88**	0.21	0.19	-0.29
PC3	3.09	1.62	-0.41	-0.23	**0.91**	0.26	0.24	-0.29
PC4	3.59	1.76	-0.32	-0.16	**0.73**	0.33	0.23	-0.2
PC5	2.92	1.58	-0.46	-0.29	**0.88**	0.30	0.35	-0.31
P&SC1	3.63	1.74	-0.13	-0.03	0.22	**0.79**	0.16	-0.13
P&SC2	3.65	1.78	-0.15	-0.06	0.26	**0.84**	0.20	-0.10
P&SC3	2.95	1.59	-0.30	-0.17	0.35	**0.91**	0.36	-0.24
TSC1	2.26	1.26	-0.57	-0.51	0.24	0.22	**0.87**	-0.55
TSC2	2.35	1.39	-0.54	-0.42	0.21	0.25	**0.85**	-0.47
TSC3	2.40	1.39	-0.52	-0.48	0.32	0.33	**0.92**	-0.51
TSC4	2.28	1.31	-0.42	-0.47	0.30	0.31	**0.92**	-0.50
TSC5	2.18	1.34	-0.56	-0.42	0.22	0.28	**0.85**	-0.47
PI1	5.79	1.38	0.44	0.37	-0.29	-0.21	-0.57	**0.93**
PI2	5.62	1.39	0.44	0.36	-0.31	-0.21	-0.53	**0.95**
PI3	5.57	1.56	0.40	0.29	-0.26	-0.13	-0.47	**0.89**

APPENDIX C

COMMON METHOD BIAS - ESSAY II

Constructs	Items	Substantive Factor Loading (R1)	$R1^2$	Method Factor Loading (R2)	$R2^2$
Assurance statements	PAS1	0.929***	0.863	0.014	0.000
	PAS2	0.925***	0.856	-0.013	0.000
	PAS3	0.895***	0.801	-0.001	0.000
Assurance Seals	AS1	0.933***	0.870	-0.004	0.000
	AS2	0.964***	0.929	0.042	0.002
	AS3	0.815***	0.664	-0.043	0.002
Privacy Concern	PC1	0.761***	0.579	-0.059	0.003
	PC2	0.917***	0.841	-0.069	0.005
	PC3	0.911***	0.830	-0.012	0.000
	PC4	0.743***	0.552	-0.002	0.000
	PC5	0.777***	0.604	0.135*	0.018
Product and Service Concern	P&SC1	0.900***	0.810	-0.091*	0.008
	P&SC2	0.931***	0.867	-0.071*	0.005
	P&SC3	0.751***	0.564	0.174**	0.030
Transaction Security Concern	TSC1	0.806***	0.650	0.067	0.004
	TSC2	0.916***	0.839	-0.079	0.006
	TSC3	0.866***	0.750	0.064	0.004
	TSC4	0.932***	0.869	-0.006	0.000
	TSC5	0.898***	0.806	-0.052	0.003
Purchase Intention	PI1	0.879***	0.773	0.061	0.004
	PI2	0.941***	0.885	-0.010	0.000
	PI3	0.952***	0.906	0.073	0.005

Notes. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; (Two-tailed significance).

APPENDIX D

MEASUREMENT ITEMS - ESSAY III

Constructs	**Items**	**Source**
Self-disclosure	SD1: How many times do you share information on Social Networking Site (SNS) each week?	Koohikamali et al. (2015)
	SD2: I share my information every time I use this SNS.	
	SD3: I rarely disclose my information when I use this SNS.	
	SD4: I am very likely to disclose my information on SNS.	New item
Protection motivation	PM1: I plan to protect my information against possible threats.	Johnston and Warkentin (2010)
	PM2: I predict I will protect my information on this SNS.	
	PM3: I intend to protect my information when I use this SNS.	
	PM4: I am sure that I will protect my information on this SNS.	Herath and Rao (2009)
	PM5: It is possible that I do something to protect my information.	
Privacy concern	PC1: I am concerned that this SNS is collecting too much information from me.	Kim, Ferrin, et al. (2008)
	PC2: I am concerned that this SNS will use my information for other purposes.	
	PC3: I am concerned that this SNS will share my information with other parties.	
	PC4: I am concerned that this SNS does not protect privacy of my information.	
Threat susceptibility	TSUS1: My information is at risk for being released to unauthorized people.	Johnston and Warkentin (2010)
	TSUS2: It is likely that my information will become available to unauthorized people.	
	TSUS3: It is possible that my Information will become available to unauthorized people.	
	TSUS4: It is likely that others get access to my information without my permission.	New items
	TSUS5: It is probable that others get access to my information without my permission.	
Threat severity	TSEV1: If my information released to unauthorized people, it would be very bad for me.	Johnston and Warkentin (2010)
	TSEV2: If my information released to unauthorized people, it would be a serious danger.	
	TSEV3: If my information released to unauthorized people, it would be significant danger.	
	TSEV4: If my information be available to unauthorized users, it would be risky.	New item
Assurance mechanisms efficacy	AME1: When this SNS uses privacy assurance mechanisms, my information are more likely to be protected.	Johnston and Warkentin (2010)
	AME2: I believe that the privacy assurance mechanisms that this SNS uses help me to keep my information private.	New items
	AME3: I think the privacy assurance mechanisms that this SNS uses are effective.	
Self-efficacy	SE1: It is easy for me to use privacy assurance mechanisms on this SNS.	Johnston and Warkentin (2010)
	SE2: It is convenient for me to use privacy assurance mechanisms.	
	SE3: I am able to use privacy assurance mechanisms without much effort.	Compeau and Higgins (1995)
	PAS1: I feel confident that this SNS's privacy assurance statement reflects their commitments to protect my information.	Xu et al. (2011)

Privacy assurance statement	PAS2: With this SNS's privacy assurance statement, I believe that my information will be safe.	
	PAS3: I believe that this SNS's privacy assurance statement is an effective way to demonstrate their commitments to privacy.	
Privacy customization	PCUST1: I customize my SNS privacy settings when I share my information.	New items
	PCUST2: I prefer to customize privacy settings before I share my information.	
	PCUST3: I usually use privacy customization feature.	
	PCUST4: I use privacy customization on this SNS to protect my information.	

APPENDIX E

FACTOR LOADINGS - ESSAY III

Item	**Mean**	**S.D.**	**SD**	**PM**	**PC**	**TSUS**	**TSEV**	**AME**	**SE**	**PAS**	**PCUS**
SD1	2.46	1.34	**0.74**	0.00	0.03	-0.12	-0.02	0.06	-0.04	0.00	0.01
SD2	2.72	1.72	**0.73**	-0.09	0.01	-0.05	-0.05	-0.05	0.14	0.34	0.03
SD3	3.55	1.79	**0.74**	0.09	0.03	0.02	0.05	0.00	-0.04	0.05	-0.01
SD4	3.35	1.61	**0.74**	-0.14	-0.03	0.08	-0.04	0.09	0.16	-0.01	0.02
PM1	5.60	1.21	-0.14	**0.79**	0.22	0.09	0.14	-0.03	0.07	-0.14	0.05
PM2	5.44	1.27	-0.04	**0.81**	0.21	-0.03	0.19	0.03	0.08	-0.04	0.09
PM3	5.73	1.16	-0.10	**0.86**	0.16	0.08	0.07	0.02	0.04	-0.02	0.23
PM4	5.31	1.38	-0.09	**0.83**	0.02	-0.08	0.05	0.08	-0.01	0.05	0.07
PM5	5.61	1.18	-0.02	**0.83**	0.09	0.09	-0.06	0.08	0.05	-0.04	0.18
PC1	4.73	1.56	0.04	0.15	**0.86**	0.18	0.04	-0.02	0.00	-0.07	0.04
PC2	4.82	1.60	-0.02	0.17	**0.92**	0.19	0.12	-0.08	0.00	-0.03	0.04
PC3	4.94	1.52	-0.08	0.19	**0.88**	0.22	0.12	-0.08	0.02	-0.04	0.07
PC4	4.64	1.55	0.03	0.19	**0.81**	0.27	0.15	-0.12	-0.03	-0.11	0.02
TSUS1	4.67	1.61	-0.04	0.05	0.23	**0.76**	0.16	0.00	-0.03	-0.17	-0.01
TSUS2	4.44	1.64	-0.02	0.00	0.17	**0.84**	0.17	-0.13	-0.03	-0.14	-0.05
TSUS3	4.88	1.49	-0.06	0.06	0.16	**0.89**	0.04	-0.03	-0.05	-0.12	-0.03
TSUS4	4.58	1.63	-0.03	0.02	0.14	**0.90**	0.09	-0.15	-0.04	-0.07	-0.08
TSUS5	4.66	1.61	-0.01	-0.02	0.13	**0.92**	0.05	-0.10	-0.03	-0.02	0.00
TSEV1	4.64	1.71	-0.04	0.18	0.13	0.17	**0.83**	-0.11	0.03	-0.04	-0.03
TSEV2	4.32	1.80	-0.04	0.07	0.08	0.05	**0.96**	-0.01	-0.02	0.01	0.00
TSEV3	4.24	1.81	-0.07	0.04	0.09	0.07	**0.95**	0.01	0.02	0.00	0.03
TSEV4	4.75	1.69	-0.02	0.06	0.09	0.16	**0.88**	0.09	-0.01	0.01	0.08
AME1	4.81	1.32	-0.01	0.06	-0.04	-0.09	-0.06	**0.85**	0.23	0.24	0.08
AME2	4.74	1.42	0.07	0.03	-0.15	-0.18	0.02	**0.84**	0.14	0.32	0.08
AME3	4.60	1.44	0.11	0.14	-0.14	-0.18	0.03	**0.80**	0.17	0.33	0.09
SE1	5.01	1.38	0.11	0.11	-0.01	-0.03	-0.01	0.14	**0.87**	0.09	0.29
SE2	4.96	1.45	0.08	0.06	-0.02	-0.06	0.01	0.15	**0.85**	0.14	0.37
SE3	4.93	1.40	0.14	0.05	0.01	-0.10	0.04	0.25	**0.82**	0.14	0.27
PAS1	3.87	1.70	0.04	-0.02	-0.09	-0.18	-0.04	0.24	0.06	**0.89**	0.03
PAS2	3.64	1.72	0.06	-0.13	-0.12	-0.14	0.00	0.30	0.12	**0.85**	-0.01
PAS3	4.11	1.71	0.05	-0.02	-0.03	-0.17	0.03	0.24	0.13	**0.82**	0.01
PCUS1	5.39	1.53	0.01	0.10	0.02	-0.01	-0.05	0.05	0.23	0.09	**0.80**
PCUS2	5.70	1.41	-0.08	0.19	0.12	-0.04	0.01	0.10	0.16	-0.06	**0.82**
PCUS3	5.61	1.53	0.12	0.12	-0.02	-0.04	0.11	-0.01	0.14	-0.02	**0.86**
PCUS4	5.74	1.39	0.01	0.17	0.05	-0.05	0.01	0.07	0.21	0.02	**0.87**

APPENDIX F

COMMON METHOD BIAS - ESSAY III

Construct	Indicator	Substantive Factor Loading (R_1)	R_1^2	Method Factor Loading (R_2)	R_2^2
Self-disclosure	SD1	0.709***	0.503	-0.013 NS	0.000
	SD2	0.754***	0.569	-0.099 NS	0.010
	SD3	0.756***	0.572	-0.052 NS	0.003
	SD4	0.790***	0.624	0.039 NS	0.002
Protection motivation	PM1	0.785***	0.616	0.172 NS	0.03
	PM2	0.851***	0.724	0.024 NS	0.001
	PM3	0.904***	0.817	0.018 NS	0
	PM4	0.868***	0.753	-0.166 NS	0.028
	PM5	0.867***	0.752	-0.058 NS	0.003
Privacy concern	PC1	0.954***	0.91	-0.096 NS	0.009
	PC2	0.992***	0.984	-0.043 NS	0.002
	PC3	0.942***	0.887	0.006 NS	0
	PC4	0.806***	0.65	0.134 NS	0.018
Threat susceptibility	TSUS1	0.735***	0.54	0.112 NS	0.013
	TSUS2	0.844***	0.712	0.075 NS	0.006
	TSUS3	0.928***	0.861	-0.018 NS	0.000
	TSUS4	0.944***	0.891	-0.017 NS	0.000
	TSUS5	1.029***	1.059	-0.138 NS	0.019
Threat severity	TSEV1	0.810***	0.656	0.144 NS	0.021
	TSEV2	0.985***	0.97	-0.054 NS	0.003
	TSEV3	0.979***	0.958	-0.053 NS	0.003
	TSEV4	0.908***	0.824	-0.025 NS	0.001
Assurance mechanisms efficacy	AME1	0.955***	0.912	0.079 NS	0.006
	AME2	0.916***	0.839	-0.051 NS	0.003
	AME3	0.917***	0.841	-0.025 NS	0.001
Self-efficacy	SE1	0.951***	0.904	0.045 NS	0.002
	SE2	0.952***	0.906	0.003 NS	0
	SE3	0.911***	0.83	-0.048 NS	0.002
Privacy assurance statement	PAS1	0.942***	0.887	-0.002 NS	0.000
	PAS2	0.909***	0.826	-0.045 NS	0.002
	PAS3	0.924***	0.854	0.049 NS	0.002
Privacy customization	PCUS1	0.832***	0.692	-0.063 NS	0.004
	PCUS2	0.870***	0.757	0.071 NS	0.005
	PCUS3	0.872***	0.76	0.003 NS	0
	PCUS4	0.917***	0.841	-0.011 NS	0.000

Note. *** $p < 0.001$ (Two-tailed significance).

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of the 1st ACM conference on Electronic commerce*: ACM.

Akhter, S. H. (2012). Who spends more online? The influence of time, usage variety, and privacy concern on online spending. *Journal of Retailing and Consumer Services, 19*(1), 109-115.

Al Kailani, M., & Kumar, R. (2011). Investigating uncertainty avoidance and perceived risk for impacting internet buying: a study in three national cultures. *International Journal of Business and Management, 6*(5), p76.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Oxford: Holt, Rinehart & Winston.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online information review, 31*(5), 661-681.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in human behavior, 45*, 93-98.

Bai, B., Law, R., & Wen, I. (2008). The impact of website quality on customer satisfaction and purchase intentions: Evidence from Chinese online visitors. *International Journal of Hospitality Management, 27*, 391-402.

Bansal, G. (2008). *Three research essays on examining online privacy concerns: The role of personal dispositions, context, and privacy-assurance features.* ProQuest.

Bansal, G., & Davenport, R. (2010). Moderating Role of Perceived Health Status on Privacy Concern Factors and Intentions to Transact with High versus Low Trustworthy Health Websites. *MWAIS 2010 Proceedings, 7*.

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., & Gefen, D. (2015a). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 1-21. http://dx.doi.org/10.1057/ejis.2014.41

Bansal, G., Zahedi, F., & Gefen, D. (2015b). The Role of Privacy Assurance Mechanisms in Building Trust and the Moderating Role of Privacy Concern. *European Journal of Information Systems, 24*(6), 1-21.

Bansal, G., Zahedi, F. M., & Gefen, D. (2008). *Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online*. Paper presented at the AMCIS 2008 Proceedings.

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. *Technology studies, 2*, 285-309.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Becker, L., & Pousttchi, K. (2012). *Social networks: the role of users' privacy concerns.* Paper presented at the Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*, 245-270.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems, 11*(3-4), 245-270.

Bhaiya, A. (2015, 03/25/2015). E-Commerce Sales Sweep the Globe: Here's How to Get in the Swing. *Huffingtonpost.com*. Retrieved from http://www.huffingtonpost.com/amit-bhaiya/ecommerce-sales-sweep-the_b_6903028.html

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On Risk, Convenience, and Internet Shopping Behavior. *Communications of the ACM, 43*(11), 98-105.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory *Predicting Health Behavior*. Buckingham, UK: Open University Press.

Bowman, G. D., & Stern, M. (1995). Adjustment to occupational stress: The relationship of perceived control to effectiveness of coping strategies. *Journal of Counseling Psychology, 42*(3), 294-303.

Boyd, D. M., & Ellison, N. B. (2010). Social network sites: Definition, history, and scholarship. *Engineering Management Review, IEEE, 38*(3), 16-31.

Brecht, F., Fabian, B., Kunz, S., & Mueller, S. (2011). *Are you willing to wait longer for internet privacy?* Paper presented at the ECIS.

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.

Brown, M., Pope, N., & Voges, K. (2003). Buying or browsing?: An exploration of shopping orientations and online purchase intention. *European Journal of Marketing, 37*, 1666-1684.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin, 56*(2), 81-105.

Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online information review, 31*, 583-603.

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7*(2), 117-141.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *Professional Communication, IEEE Transactions on, 52*(2), 167-182.

Chang, M. K., Cheung, W., & Lai, V. S. (2005). Literature derived reference models for the adoption of online shopping. *Information & Management, 42*, 543-559. doi: 10.1016/j.im.2004.02.006

Chang, T.-Z., & Wildt, A. R. (1994). Price, product information, and purchase intention: An empirical study. *Journal of the Academy of Marketing Science, 22*, 16-27.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*, 358-368.

Chen, J. Q., Zhang, R., & Lee, J. (2013). A Cross-Culture Empirical Study of M-commerce Privacy Concerns. *Journal of Internet Commerce, 12*(4), 348-364.

Chen, M.-S., Han, J., & Yu, P. S. (1996). Data mining: an overview from a database perspective. *Knowledge and Data Engineering, IEEE Transactions on, 8*, 866-883.

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems, 55*(3), 661-668.

Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: the case of Facebook users. *European Journal of Information Systems, 24*(1), 93-106.

Chen, Y.-H., Hsu, I., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research, 63*, 1007-1014.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research, 14*(2), 189-217.

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. 2nd edn. Hillsdale, New Jersey: L: Erlbaum.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences*: Routledge.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly, 19*(2), 189-211.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

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

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

Delgado-Márquez, B. L., Hurtado-Torres, N. E., & Aragón-Correa, J. A. (2013). On the Measurement of Interpersonal Trust Transfer: Proposal of Indexes. *Social Indicators Research, 113*(1), 433-449.

DeNale, R., Liu, X., & Weidenhamer, D. (2015). *Quarterly Retail E-Commerce Sales 2nd Quarter 2015*. Washington, D.C.

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

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

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*, 295-316.

Donthu, N., & Garcia, A. (1999). The internet shopper. *Journal of Advertising Research, 39*, 52-58.

Duh, R.-R., Sunder, S., & Jamal, K. (2002). Control and assurance in e-commerce: Privacy, integrity, and security at eBay. *Taiwan Accounting Review, 3*, 1-27.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.* Paper presented at the AMCIS 2007 Proceedings.

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.

Eroglu, S. A., Machleit, K. A., & Davis, L. M. (2001). Atmospheric qualities of online retailing: a conceptual model and implications. *Journal of Business Research, 54*, 177-184.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*: Addison-Wesley.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*, 601-620.

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.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior, 25*(1), 153-160.

Folkman, S. (1984). Personal control and stress and coping processes: a theoretical analysis. *Journal of Personality and Social Psychology, 46*(4), 839.

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

Forsythe, S. M., & Shi, B. (2003). Consumer Partronage and Risk Perceptions in Internet Shopping. *Journal of Business Research, 56*, 867-875.

Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research, 9*, 372-382.

Gauzente, C. (2004). Web Merchants' Privacy and Security Statements. *Journal of Electronic Commerce Research, 5*(3), 181-198.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*, 725-737.

Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The" science of the sophomore" revisited: From conjecture to empiricism. *Academy of Management Review, 11*(1), 191-207.

Greenberg, M. A., & Stone, A. A. (1992). Emotional disclosure about traumas and its relation to health: effects of previous disclosure and trauma severity. *Journal of Personality and Social Psychology, 63*(1), 75.

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., & William C, B. (1995). *Multivariate data analysis with readings*. New Jersy: Prentice Hall.

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.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*: Guilford Press.

Hedges, L. V., & Olkin, I. (1985). *Statistical Methods for Meta-Analysis*. Orlando, FL: Academic Press.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The Use of PLS Path Modeling in International Marketing. *Advances in International Marketing, 20*, 277-319.

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.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *The Information Society, 15*(2), 129-139.

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

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2005). *2005*.

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The Effects of Web Assurance Seals on Consumers' Initial Trust in an Online Vendor. *Decision Support Systems, 48*, 407-418.

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.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies. *Strategic management journal, 20*(2), 195-204.

Hunter, J. E., & Schmidt, F. L. (2004). *Methods for Meta-Analysis: Correcting Error and Bias in Research Findings* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Hwang, M. I., & Schmidt, F. L. (2011). Assessing moderating effect in meta-analysis: A re-analysis of top management support studies and suggestions for researchers. *European Journal of Information Systems, 20*(6), 693-702.

Ioinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet *The Oxford handbook of Internet psychology* (pp. 235-250).

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2).

Jiang, Z., Chan, J., Tan, B. C., & Chua, W. S. (2010). Effects of interactivity on website involvement and purchase intention. *Journal of the Association for Information Systems, 11*(1), 34-59.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (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.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.

Jung, E. J., Lankton, N., McKnight, H., & Jung, E. (2012). *Three Processes that Form Online Social Networking Post-Adoptive Use Intention.* Paper presented at the AMCIS.

Jung, E. J., McKnight, D. H., Jung, E., & Lankton, N. K. (2011). *The Surprising Lack of Effect of Privacy Concerns on Intention to Use Online Social Networks.* Paper presented at the AMCIS.

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*, 387-402.

Kalakota, R., & Whinston, A. B. (1997). *Electronic Commerce: a Manager's Guide.*: Addison-Wesley Professional,.

Kauffman, R. J., Lee, Y. J., Prosch, M., & Steinbart, P. J. (2011). A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Systems, 25*(2), 47-79.

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.

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.

Kim, D. (2008). Self-Perpcetion-Based Versus Transference-Based Trust Determinants in Computer-Mediated Transactions. *Journal of Management Information Systems, 24*(4), 13-45.

Kim, D., Sivasailam, N., & Rao, H. R. (2004). Information Assurance in B2C Websites for Information Goods/Services. *Electronic Markets, 14*(4), 344-359.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544-564.

Kim, D. J., Sivasailam, N., & Rao, H. R. (2004). Information assurance in B2C websites for information goods/services. *Electronic Markets, 14*(4), 344-359.

Kim, D. J., Steinfield, C., & Lai, Y.-J. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44*(4), 1000-1015.

Kimery, K., & McCord, M. (2002). Third-Party Assurances: Mapping the Road to Trust in E-Retailing. *Journal of Information Technology Theory and Application, 4*(2), 63-83.

Kimery, K. M., & McCord, M. (2002). Third party assurances: mapping the road to trust in eretailing. *Journal of Information Technology Theory and Application (JITTA), 4*, 7.

Ko, D.-G., Kirsch, L. J., & King, W. R. (2005). Antecedents of knowledge transfer from consultants to clients in enterprise system implementations. *MIS quarterly, 29*(1), 59-85.

Koohikamali, M., Gerhart, N., & Mousavizadeh, M. (2015). Location Disclosure on LB-SNAs: The Role of Incentives on Sharing Behavior. *Decision Support Systems, 71*, 78-87.

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

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*.

Kukar-Kinney, M., & Close, A. G. (2010). The determinants of consumers' online shopping cart abandonment. *Journal of the Academy of Marketing Science, 38*(2), 240-250.

Lala, V., Arnold, V., Sutton, S. G., & Guan, L. (2002). The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior. *International Journal of Accounting Information Systems, 3*, 237-253.

Lankton, N. K., & Tripp, J. F. (2013). *A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro Model.* Paper presented at the AMCIS.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social issues, 33*(3), 22-42.

Lazzarotti, J. (2014). Report Says Russian Hackers Stole 1.2 Billion Usernames and Passwords, But Don't Let "Breach Fatigue" Take Hold. *Workplace Privacy, Data Management & Security Report*. http://www.workplaceprivacyreport.com/2014/08/articles/written-information-security-program/report-says-russian-hackers-stole-1-2-billion-usernames-and-passwords-but-dont-let-breach-fatigue-take-hold/

Lee, L. T. (2000). Privacy, security, and intellectual property *Understanding the Web: Social, political, and economic dimensions of the Internet* (pp. 135-164): Ames: Iowa State University Press.

Lee, S. M., Choi, J., & Lee, S.-G. (2004). The impact of a third-party assurance seal in customer purchasing intention. *Journal of Internet Commerce, 3*, 33-51.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials *Pew Internet & American Life Project*: Pew Internet & American Life Project.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Li, Y. (2014a). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*, 343-354.

Li, Y. (2014b). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications, 13*(1), 32-44.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS quarterly, 31*(1), 59-87.

Lin, S.-W., & Liu, Y.-C. (2012). The effects of motivations, trust, and privacy concern in social networking. *Service Business, 6*(4), 411-424.

Lind, E. A., & Tyler, T. R. (1988). *The social psychology of procedural justice*: Springer Science & Business Media.

Lipsey, M. W., & Wilson, D. B. (2001). *Practical meta-analysis*: Sage Publications, Inc.

Liu, C., Marchewka, J. T., & Ku, C. (2004). American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce. *Journal of Global Information Management (JGIM), 12*(1), 18-40.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304.

Lo, J. (2010). *Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites.* Paper presented at the AMCIS.

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*, 163-200.

Lu, Y., Yang, S., Chaung, P. Y. K., & Cao, Y. (2011). Dynamics between the Trust Transfer Process and Intention to Use Mobile Payment Services: A Cross Environment Perspective. *Information & Management, 48*, 393-403.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*(2), 111-118.

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.

MacKinnon, D. P., Lockwood, C. M., & Williams, J. (2004). Confidence limits for the indirect effect: Distribution of the product and resampling methods. *Multivariate behavioral research, 39*(1), 99-128.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). *A model for information assurance: An integrated approach.* Paper presented at the Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital footprints: Online identity management and search in the age of transparency: Pew Internet & American Life Project.

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.

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.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS quarterly*, 5-12.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2000). Trust in e-commerce vendors: a two-stage model. *Proceedings of the twenty first international conference on Information systems*.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business. *Electronic Markets, 14*, 252-266.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations (JECO), 4*(1), 1-17.

Milne, G. R., & Culnan, M. J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US web surveys. *The Information Society, 18*, 345-359.

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.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of public policy & marketing, 12*(2), 206-215.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741-759.

Miyazaki, A., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs, 36*(1), 28-49.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of public policy & marketing, 19*(1), 54-61.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*(1), 27-44.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in human behavior, 28*(6), 2366-2375.

Morton, A. (2013). *Measuring Inherent Privacy Concern and Desire for Privacy-A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern.* Paper presented at the Social Computing (SocialCom), 2013 International Conference on.

Moscardelli, D. M., & Divine, R. (2007). Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal, 35*(3), 232-252.

Nemati, H. R., & Dyke, T. V. (2009). Do Privacy Statements Really Work/. *International Journal of Information Security and Privacy, 3*(1), 45-64.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory *Predicting Health Behavior*. London: Open University Press.

Psychometric theory, New York: McGraw-Hill (1978).

Nunnally, J. C., Bernstein, I. H., & Berge, J. M. t. (1967). *Psychometric theory* (Vol. 226): McGraw-Hill New York.

Odeyinde, O. B. (2013). *Information privacy concerns of undergraduate students in a nigerian university and their willingness to provide personal information to transact on the internet.* Wilmington University, ACM SIGMIS Database.

Ofcom. (2014). Ofcom Technology Tracker.

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

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology, 25*(2), 243-262.

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in human behavior, 49*, 324-332.

Otim, S., & Grover, V. (2006). An empirical study on web-based services and customer loyalty. *European Journal of Information Systems, 15*, 527-541.

Park, I. (2009). *The Study on the Relationship between Privacy Concerns and Information Systems Effectiveness.* Paper presented at the ICIS.

Park, I., Bhatnagar, A., & Rao, H. R. (2010). Assurance Seals, On-Line Customer Satisfaction, and Repurchase Intention. *International Journal of Electronic Commerce, 14*(3), 11-34.

Park, J., Lennon, S. J., & Stoel, L. (2005). On-line product presentation: Effects on mood, perceived risk, and purchase intention. *Psychology & Marketing, 22*, 695-719.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*, 101-134.

Peter, J. P., & Tarpey Sr, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research, 2*, 29-37.

Peterson, D., Meinert, D., Criswell, J., & Crossland, M. (2007). Consumer trust: privacy policies and third-party seals. *Journal of Small Business and Enterprise Development, 14*(4), 654-669.

Peterson, R. A., & Brown, S. P. (2005). On the use of beta coefficients in meta-analysis. *Journal of applied psychology, 90*(1), 175.

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.

Pingitore, G., Meyers, J., Clancy, M., & Cavallaro, K. (2013). Consumer Concerns About Data Privacy Rising: What Can Business Do? McGraw Hill Financial.

Plummer, M., Hiltz, S. R., & Plotnick, L. (2011). *Predicting intentions to apply for jobs using social networking sites: an exploratory study.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference on.

Poddar, A., Donthu, N., & Wei, Y. (2009). Web site customer orientations, Web site quality, and purchase intentions: The role of Web site personality. *Journal of Business Research, 62*, 441-450.

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

Posey, C., 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.

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior research methods, instruments, & computers, 36*(4), 717-731.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior research methods, 40*(3), 879-891.

Qureshi, I., Fang, Y., Ramsey, E., McCole, P., Ibbotson, P., & Compeau, D. (2009). Understanding online customer repurchasing intention and the mediating role of trust--an empirical investigation in two developed countries. *European Journal of Information Systems, 18*, 205-222.

Rainie, L., & Anderson, J. (2014). The Future of Privacy: Pew Research Center.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, Privacy, and Security Online: Pew Internet & American Life Project.

Raman, P., & Pashupati, T. K. (2004). *Online privacy: the impact of self perceived technological competence.* Paper presented at the American Marketing Association Educators.

Ranganathan, C., & Ganapathy, S. (2002). Key dimensions of business-to-consumer web sites. *Information & Management, 39*, 457-465.

Ratnasingham, P. (1998). Internet-based EDI trust and security. *Information Management & Computer Security, 6*, 33-39.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology, 91*(1), 93-114.

Rogers, R. W., Cacioppo, J. T., & Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation *Social psychophysiology: A sourcebook* (pp. 153-177).

Rogers, R. W., & Thistlethwaite, D. L. (1970). Effects of fear arousal and reassurance on attitude change. *Journal of Personality and Social Psychology, 15*(3), 227.

Rosenthal, R. (1984). *Meta-Analytic Procedures for Social Research* (Vol. 6). Beverly Hills, CA: Sage Publications.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems, 101*, 165-177.

Criteria for emotion-antecedent appraisal: A review 89-126 (Springer 1988).

Shawn F, C., Ryan T, W., & Ronald E, P. (2010). Employee information privacy concerns with employer held data: A comparison of two prevalent privacy models. *Journal of Information Privacy and Security, 6*(3), 47-71.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing, 19*(1), 62-73.

Singer, E., Hippler, H.-J., & Schwarz, N. (1992). Confidentiality assurances in surveys: Reassurance or threat? *International Journal of Public Opinion Research, 4*, 256-268.

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

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

Solomon, Z., Mikulincer, M., & Benbenishty, R. (1989). Locus of control and combat-related post-traumatic stress disorder: The intervening role of battle intensity, threat appraisal and coping. *British Journal of Clinical Psychology, 28*(2), 131-144.

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

Spake, D. F., Zachary Finney, R., & Joseph, M. (2011). Experience, comfort, and privacy concerns: antecedents of online spending. *Journal of Research in Interactive Marketing, 5*(1), 5-28.

Spreng, R. A., Harrell, G. D., & Mackoy, R. D. (1995). Service recovery: impact on satisfaction and intentions. *Journal of Services Marketing, 9*, 15-23.

Squicciarini, A., Paci, F., & Sundareswaran, S. (2010). *PriMa: an effective privacy protection mechanism for social networks.* Paper presented at the ACM Symposium on Information, Computer and Communications Security.

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

Stewart, K. J. (2003). Trust Transfer on the World Wide Web. *Organization Science, 14*, 5-17.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management, 8*, 349-411.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in human behavior, 27*(1), 590-598.

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

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research, 22*(2), 211-233.

Tanner Jr, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *The Journal of Marketing, 55*(3), 36-45.

Tao, Z. (2008). *The impact of privacy concern on m-commerce user acceptance.* Paper presented at the Grid and Pervasive Computing Workshops, 2008. GPC Workshops' 08. The 3rd International Conference on.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203-223.

TRUSTe. (2015). Privacy Assessments & Certifications.

Tsoi, H. K., & Chen, L. (2011). *From privacy concern to uses of social network sites: A cultural comparison via user survey.* Paper presented at the Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom).

Van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: contributions from technology and trust perspectives. *European Journal of Information Systems, 12*, 41-48.

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*, 415-444.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157-174.

Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing, 18*(1), 53-69.

WebTrust. (2015). Overview of Trust Services. from http://www.webtrust.org/overview-of-trust-services/item64420.aspx

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology, 12*(4), 324-333.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM, 10*(9), 533-537.

Whitener, E. M. (1990). Confusion of confidence intervals and credibility intervals in meta-analysis. *Journal of applied psychology, 75*(3), 315.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior, 28*(3), 889-897.

Wurtele, S. K., & Maddux, J. E. (1987). Relative contributions of protection motivation theory components in predicting exercise intentions and behavior. *Health Psychology, 6*(5), 453.

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. (2004). *Alleviating consumers' privacy concerns in location-based services: a psychological control perspective.* Paper presented at the ICIS, Charlottesville, Virginia.

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. (2005). *Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk.* Paper presented at the ICIS, Las Vegas, Nevada.

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.

Yang, H.-L., & Miao, X.-M. (2008). *Concern for information privacy and intention to transact online.* Paper presented at the Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on.

Yang, H. C. (2012). YOUNG AMERICAN CONSUMERS’PRIOR NEGATIVE EXPERIENCE OF ONLINE DISCLOSURE, ONLINE PRIVACY CONCERNS, AND PRIVACY PROTECTION BEHAVIORAL INTENT. *Journal of Consumer Satisfaction, Dissatisfaction & Complaining Behavior, 25*, 179-202.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database, 40*(1), 38-51.

Yao-Hua Tan, W. T. (2000). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*(2), 61-74.

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.

Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology, 24*(4), 259-274.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

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

Zhang, H. (2005). Trust-Promoting Seals in Electronic Markets. *Journal of Information Technology Theory and Applicatio, 6*(4), 29-40.

Zhang, H. (2005). Trust promoting seals in electronic markets: impact on online shopping decisions. *Journal of Information Technology Theory and Application (JITTA), 6*, 5.

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *The Journal of Computer Information Systems, 53*(4), 31.

Zhao, X. (2012). *Why we disclose differently: How social networking site affordances affect privacy concerns and disclosure practices in cross-cultural contexts.* Purdue University, ProQuest.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research, 37*(2), 197-206.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in human behavior, 37*, 283-289.

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.