2016

Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems

Patrick I. Offor
Nova Southeastern University, po125@nova.edu

Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems

by

Patrick Ikechukwu Offor

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2016

We hereby certify that this dissertation, submitted by Patrick Offor, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Tejay Gurvirender, Ph.D. — Date
Chairperson of Dissertation Committee

Ling Wang, Ph.D. — Date
Dissertation Committee Member

Timothy J. Ellis, Ph.D. — Date
Dissertation Committee Member

Approved:

Yong X. Tao, Ph.D., P.E., FASME — Date
Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University

2016

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Examining Consumers’ Selective Information Privacy Disclosure Behaviors in an Organization’s Secure e-Commerce Systems

by
Patrick I. Offor
November 2016

The study is an examination of the antecedents to the paradoxical changes in the consumers’ intended and actual personal information disclosure behaviors in online transactions or in e-commerce environments. The argument is that a consumer’s information privacy paradox is based on the consumer’s cognitive predisposition. The study adopted the conceptual underpinning inherent in the Privacy Regulation Theory (PRT) and translated them into information privacy context, as the consumer’s desired state of information privacy, information privacy self-interest, information privacy permeability, and information privacy equipoise constructs, to examine the causal relationship among the constructs and between a consumer’s selective personal information disclosure behavior variable. The theoretical model was advanced based on the conceptual framework in PRT and was validated using Structural Equation Modeling. In addition, the study conducted hypothesis testing and factor analysis using Confirmatory Factor Analysis in order to determine the existence of statistical significance and causality. The result indicates that the consumers’ willingness to transact online and disclose their personal information depend largely on the degree of their need signal (self-interest), and to some extent, their awareness and concern of the online merchant’s capacity to collect their personal information, irrespective of their previously declared or undeclared intent to transact and disclose personal information, or despite their desired natural state of information privacy. In other words, the existence of the information privacy paradox stems from the fact that a consumer’s intention to disclose personal information online depends on the person’s natural or desired state of information privacy, whereas the customer’s actual personal information disclosure behavior depends on his or her information privacy equipoise.

Acknowledgements

My first expression of gratitude goes to my advisor and dissertation committee chair, Dr. Gurvirender Tejay, for his understanding, guidance, and encouragement throughout this dissertation process.

Equally, my special thanks go to Dr. Ling Wang and Dr. Timothy Ellis, my dissertation committee members, whose reviews, feedbacks, suggestions, and questions helped in shaping the quality my research study.

My gratitude also goes to my colleagues and friends, whose support and help I have sought, cherished, and appreciated during this journey: Simon Cleveland Ph.D., John Gray Ph.D., Albert L. Harper, Fernando (Jose) Lopez, Osborne Obeng, Austin Ogwu-Chinuwa, and Zareef Mohammed.

I will forever be indebted to my family. To my wife Onyinyechukwu Obiageli Offor, I love you! I appreciate your understanding, unconditional love, and unequivocal support. To our children: Patrick Jr, MaryJane, and Elvis, your invaluable presence in my life and companionship have been instrumental to my pursuit of excellence and education. To our grandchild, Alaina Chizoba Offor, may you live and learn the power of the pen.

To my parents, Chief Cyprian U. Offor and Mrs. Emerenciana N. Offor, whose visions and insatiable desires for excellence and education sowed the seed and drove my *quality world*, I love you! I thank you for your love, inspiration, and adoration. You imbibed a sense of love and trust in God in me. In addition, your guidance had engineered my sense of integrity, courage, selfless service, perseverance, and diligence, which guides my path.

My special gratitude also goes to my siblings: Josephine Oragwu, whose support in life is priceless and with whom I truly endured the hardship of growing up; Esther Uwakwe, Nkeiru, Anastacia, Obiora, Anthony, and Catherine. Your love and support were and have been invaluable and remarkable to me!

To Geoffrey Owu and Elem Ude, words are not enough to express my gratitude to you and your family. Hence, I simple say, Thank you very much! My gratitude also goes to Fannie. Finally, to Emeka and Nneka Onyia, you were the connecting link, without which this may not have been possible…thank you for your friendship from the beginning.

Accepted Paper from this Research

Offor, P. I., & Tejay, G. (2016). Examining information privacy paradox through cognitive perspective. *Twenty-Fourth European Conference on Information Systems (ECIS), İstanbul, Turkey*.

Table of Contents

Chapters

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

1.1 Background

Organizations consider consumers’ personal information as a product, an asset, and as the substratum of online transaction processing (OLTP) in electronic commerce (e-commerce), electronic healthcare (e-healthcare), and in electronic government (Culnan & Armstrong, 1999; Gabisch & Milne, 2014; Kauffman et al., 2009; Smith et al., 2011; Ward & Krishnan, 2006). In addition, the Ericsson Report (2013) suggested that “companies such as Google and Facebook have business models built around collecting, aggregating, analyzing and monetizing personal information” (p. 4). On the other hand, consumers are apprehensive and ambivalent about sharing their personal information online because they are concerned about the security, and the use of their personal information by a third party, or beyond the stated reasons given for its initial collection (Hong & Thong, 2013; Lee et al, 2011).

Empirical evidence shows that organizations and consumers have divergent interests on personal information disclosure and collection during e-commerce (Corbett, 2013; Gabisch & Milne, 2014). Consequently, a consumer’s personal information disclosure behavior when transacting online is selective, deliberate, and dynamic, which is indicative of the gap between a consumer’s intended and actual disclosure of personal information online (Dinev & Hart, 2006; Norberg et al., 2007; Smith et al., 2011).

Despite the difference between organizations' and consumers' personal information disclosure interests, consumers' sharing of their personal information have become the cornerstone for the upward trend witnessed in sales and in e-commerce participations, in e-healthcare diagnosis interests, in e-government activities, in the social-media business model developments and participations, and has become a requisite for mobile computing, application downloads, and other services. For example, e-commerce sales are on the rise and had accounted for 4.7% of total sales in 2011, 5.2% of total sales in 2012, and 5.8% total sales in 2013 in the United States according to the U.S. Census Bureau (2014). In its 2014 quarterly retail sales report, the Bureau showed adjusted total e-commerce sales of $263.3 billion in 2013, which is an increase of 16.9% from 2012, and an increase of 36% from 2011. However, the Internet capable device ownership growth has surpassed the rate of OLTP use. According to Pew Research article, the ownership of tablet computers rose from 5% in 2010 to 50% in 2015, smartphone rose from 52% in 2011 to 86% in 2015, the e-book reader rose from 5% in 2010 to 18% in 2015, and the cellphone rose from 96% in 2010 to 98% in 2015 (Anderson, 2015).

The upward trend in online transactions or services is not unique to ecommerce alone. In electronic healthcare, about 71% of patients in Safety Net program who use email, which is about 60% in the U.S., had indicated their e-healthcare participation interests (Schickedanz et al., 2013). Electronic healthcare allows for a coordinated health care and requires the use of electronic health record (EHR), which is a digital copy of a patient's personal and medical history (Hoerbst & Ammenwerth, 2010). In addition, local, state, and federal governments are diversifying their capabilities and capacities to provide certain services online. Currently, e-government provides the citizens with online services, such as the renewal of driver’s license, renewal of vehicle registration, application for voter’s registration, application for international passport, conducting of information systems and information systems security training, and the payment for other government services.

Secondly, organizations consider consumers’ willingness to share their personal information online as a critical path necessary in achieving their online business objectives and in improving or maintaining their growth or their sales revenue. Conversely, consumers consider the risk of losing the control of their personal information after sharing them online. They are also worried about the obliviousness of not knowing how their personal information is used or shared, as such, they are concerned and consternated. This is important because although consumers’ personal information considerations, fears, concerns, anxieties are well documented in the literature (Dinev & Hart, 2006; Lee et al, 2011; Norberg et al., 2007; Smith et al., 2011), studies on organizations’ fair information practices (FIP) are scanty and have just begun to emerge (Lee et al., 2011). Suggestions in literature assume that consumers’ apprehensiveness and inconsistencies in disclosing personal information online are driven by lack of trust on firms’ ability to protect their personal information effectively and the risk associated with the loss of control of consumers’ information after they are disclosed online (Lee et al, 2011; Norberg et al., 2007; Smith et al., 2011). However, other studies argue that although consumers’ concerns and anxieties are real, their assessments of net gain in value mostly outweigh their consternations (Dinev & Hart, 2006).

Practically, organizations and consumers have opposing views in e-commerce or in an online personal information disclosure. Despite the dichotomy, the irony is that the consumers and organizations benefit relatively from the online personal information sharing. Largely, organizations benefit from online personal information disclosure by capturing consumers' information, which help them in conducting appropriate analysis on the consumer purchasing patterns, in target advertising, and in the information asset acquisition. Equally, consumers benefit by receiving monetary and other incentives in exchange for disclosing their personal information online, and by receiving specific discount opportunities. Hence, the truth is that although the benefits are relatively mutual, the risks, the controls, or the vulnerabilities are not. While a consumer may receive a one-time incentive for disclosing personal information online, an organization has endless access and control of the information, as long as the information remains valid. This means that an organization could share or sell a consumer's information, which is collected at one online transaction instance, as many times as it desires.

1.2 Research Problem and Argument

This study is an empirical examination of the antecedents to the paradoxical changes in the consumers' intended and actual personal information disclosure in an online transaction or in an e-commerce environment from cognitive predisposition perspective. Consumers' personal information is the cornerstone for an effective e-commerce, e-healthcare, or e-government activity. Inability of an organization to project or assess consumers' actual willingness to disclosure personal information in e-commerce may destabilize the organization's e-commerce activities, may upend the organization's e-commerce sales trajectory, may impede its market penetration or market expansion efforts, or may derail the organization's projected revenue and/or cash flow.

The need for further examination of this phenomenon in this study is supported in the literature (Bélanger & Crossler 2011; Keith et al., 2013; Mothersbaugh et al., 2012; Norberg et al., 2007; Smith et al., 2011). Bélanger and Crossler (2011) suggested that information privacy paradox, a gap between consumers' intended and actual personal information disclosure, requires further examination, despite studies that show that intentions lead to actual behavior. Norberg et al. (2007) found that there is a gap between consumers' intended and actual disclosure of personal information in e-commerce, but warned that the phenomenon needs adequate analysis. In addition, Smith, Dinev, and Xu (2011) submitted that researchers have concentrated in measuring intention rather than actual behaviors in the past, and that the associations between privacy concerns and stated intentions do not always reflect consumer actual personal information disclosure.

Incidentally, the inconsistency in the consumers' intended and actual behavior is not peculiar to information privacy discipline alone. The literature in the other social science disciplines had identified the variant in the consumers' intended and actual behaviors as well. Toulemon and Testa (2005) illustrated the disparity in intended and actual fertility in a five-year longitudinal survey designed to predict birth rate, with 2,624 sample subjects in France. Jamieson and Bass (1989) noted that although 70% to 90% of marketers use intention to purchase as the basis for their marketing prediction, evidence showed that actual purchase of materials depended on affordability, availability, or wanting to seek other people's opinion prior to purchasing.

Furthermore, although consumers' personal information disclosure concerns, behaviors, and paradox have been examined extensively, precursors to the inconsistency between the consumers' intended and actual disclosure have not been explored sufficiently (Berendt et al., 2005; Korzaan & Boswell, 2008; Malhotra et al., 2004; Son & Kim, 2008).

The research argument is that a consumer's discriminant or selective willingness to disclose personal information when transacting online is not solely economic-based or value-based, but cognitive predisposition-based as well. Economic-based or value-based information privacy assessment refers to cognitive risk-benefit or cost-benefit calculations (Dinev & Hart, 2006; Smith et al., 2011), whereas cognitive predisposition-based information privacy assessment refers to a consumer's personal information privacy disclosure tendencies based on mindset and perception, rather than on just reasoning and judgment.

Thus far, previous studies have discounted or failed to account for the effects of consumers' predispositions to information privacy paradox. Martin (2004) described consumer predisposition as "consumer's propensity to manifest the fantastic imaginary in consumption" (p. 143), and fantastic imaginary is evoked by "a desire for active participation in the fantastic imaginary setting" (p. 143). In information privacy context, it means that previous studies have not accounted for a consumer's avid desire to participate in e-commerce, regardless of the vulnerabilities or the amount of risks she faces when sharing personal information online or the level of trust she has on an organization's information privacy practices.

Additionally, cognitive predisposition assessment of the gap in information privacy paradox exposes the incompleteness in the current findings in the literature. The general consensus in literature is that the paradoxical gap in consumers' personal information disclosure behavior online is due to privacy calculus: risk-benefit analysis (Dinev & Hart, 2006), risk and trust considerations (Norberg et al., 2007), and the sensitivity of information (Moothersbaugh et al., 2012).

The supposition is that the contradiction between the consumers' intended and actual disclosure of personal information online is attributable to the consumers' electronic point-of-sale risk-benefit decisions, or consumers' perceived net value of information being requested. For example, the notion is that a consumer would always assess the cost-benefits of joining social network site prior to disclosing his personal information online. However, Awad and Krishnan (2006) noted that "consumers tend not to make a financial cost-benefit analysis of social contracts with unpredictable outcomes," because association of value is imprecise and making definite distinction between social exchanges is implausible. Therefore, this study postulates that information privacy disclosure paradox or disparity is attributable to consumers' predispositions as well.

Angst and Agarwal (2009) articulated similar position in a study of electronic health record. In the study, the authors defined attitude as a "complex mental state involving beliefs and feelings and values and dispositions to act in certain ways [sic]" (p. 346). Furthermore, Ajzen and Fishbein (1977) argued, "People's actions are found to be systematically related to their attitudes" (p. 888). Therefore, this study proposes that further examination of the antecedents to the privacy paradox is potent and crucial based on these aforementioned views in the literature.

1.3 Importance of Research Problem

The significance of this study is that a cognitive predisposition exploration and an empirical examination of the antecedents to the consumer's intended and actual personal information disclosure dichotomy in e-commerce would be invaluable to researchers, since current studies are economic and value based, which focused on the net benefit of the information privacy (Dinev & Hart, 2006; Smith et al., 2011). Besides, despite the extensive examination on the phenomenon in previous studies, researchers had warned that further examination of the privacy paradox is necessary (Bélanger & Crossler, 2011; Berendt et al., 2005; Keith et al., 2013; Mothersbaugh et al. 2012; Norberg et al., 2007; Smith et al., 2011).

For instance, Keith et al. (2013) was doubtful of the linkage between a consumer's intended and actual disclosure behavior. The paper stated, "It remains to be seen (1) whether, and to what degree, information disclosure intentions determine actual disclosure; and (2) how the practice of false information disclosure influences this relationship" (p. 1164). Furthermore, Mothersbaugh et al. (2012) suggested that prior studies had failed to account for the mediating effect of information sensitivity to a consumer's personal information disclosure. Yet, Berendt et al. (2005) evaluated consumers' stated preferences and actual behaviors, and found that whereas consumers' normative levels of privacy concerns were strong; their online interactive privacy behaviors were relatively weak.

Besides, previous studies did not account for a consumer's disposition to disclose personal information in e-commerce, regardless of whether the person is an information privacy fundamentalist, pragmatist, or unconcerned. Therefore, based on the belief that inquiry on the antecedents to the privacy paradox is not yet exhaustive, one of the aims of this study is to examine the phenomenon from cognitive predisposition prism. Additional goal of the study is to show that there are common personal information disclosure paradoxical influencers that are insensitive to our cultural, economic, or value differences. This is necessary because furtherance to empirical and anecdotal beliefs that information privacy paradox depend only on risk, trust, and value perceptions, privacy concern, and cultural differences (Bélanger & Crossler, 2011; Hui et al., 2007; Milberg et al., 2002), this study proposes to establish that consumers' predispositions have causal relationship with the consumers' willingness to share personal information online as well.

1.4 Definition of Key Terms

Although privacy and information privacy is interchangeable in this study, the focus of this study is on information privacy. Nevertheless, earlier studies on privacy were focused on *general privacy,* which is the right "to be let alone" (Warren & Brandeis, 1890). Early invasion of privacy stems from photographers taking pictures of influential people at their dullest hours, newspapers finding and publishing sensational information about people for readership and sales, neighbors gossiping about their neighbors, and businesses' carefree personal information collection and disposition. Later, the threat advanced to personal information solicitations, through junk mailing and telemarketing. Nowadays, it is the prying eye of the drones, Internet bots, information systems security attackers, hidden cameras, hidden microphones, and mobile and other hidden devices. In Gertler (2004), Justice Brandeis suggested that privacy is a protection to one's beliefs, thoughts, emotion, and sensation. The paper wrote, "They conferred as against the Government, the right to be let alone [as] the most comprehensive of the rights of man [or woman] and the right most valued by civilized men [or women]" (p. 5).

Information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Malhotra et al., 2004, p. 337). Son and Kim (2008) also described it as "an individual’s ability to control when, how, and to what extent his or her information is communicated to others” (p. 504). This study defines information privacy as an assurance of good stewardship of the consumers’ personal information, in terms of the collection, the use, and the security of the shared information, among individuals, groups, or organizations. The concern for information privacy is evolving and increasing, primarily because of the advances in information technology. It is also a reflective of the changes in the human knowledge and activities in the face of evolving technological changes. In addition, information privacy is interdisciplinary because it cuts across many disciplines: law, marketing, economics, healthcare, information systems, and e-commerce. However, central to information privacy despite its cross-discipline dimension, is the notion of the individuals’ abilities to have relative assurances or controls over the collection, the use, and the storage of their personal identifiable information (PII) or their protected health information (PHI).

Westin (1991) classified privacy behavior into three categories: the fundamentalist, the pragmatist, and the unconcerned. The paper equates a privacy fundamentalist as one with a high level of privacy concern, a pragmatist as one with an intermediate level of concern, and an unconcerned as one with limited concern for privacy. In this context, an information privacy fundamentalist is one who prefers to have a full control of his or her personal information to any associated or derived consumer benefit. A fundamentalist is always wary of an organization’s personal information collection and use, and advocates for the placement of more regulatory controls to information privacy collection and use. A pragmatist is one interested in assessing the cost-benefit of personal information disclosure or the net benefit, and is very attentive in the tradeoff in disclosing personal information online. Equally, an unconcerned, as the name implies, is always willing to disclose his personal information online with limited concern for what an organization will do with it (Kumaraguru & Cranor, 2005; Westin, 1991). Westin (1991) taxonomy is relevant to this study because it helps in identifying a consumer's natural or desired state of information privacy or predisposition prior to actual disclosure behavior.

The definition of ecommerce varies based on its scope (Belanger et al., 2002; GAO-02-404, 2002). In GAO-02-404 (2002, p. 82), the Organization for Economic Corporation and Development defined e-commerce as "the sale or purchase of goods or services conducted over computer-mediated networks; includes EDI (electronic data interchange); excludes Intranet transactions." Also in the report, the Gartner Group defined it as sales conducted over the Internet, EDI, e-marketplaces, and extranet, but not on proprietary networks. Yet, the U.S. Census Bureau's calculation of ecommerce activities involve "any monetary transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods and services, includes Internet, Intranet, Extranet, and EDI transactions" (GAO-02-404, 2002, p. 82). In Belanger et al. (2002), Conhaim (1998, p.13) articulated e-commerce as all "consumer-oriented storefronts, business-to-business applications as well as behind-the-scenes business functions like electronic payment systems and order management." In this study, e-commerce encompasses all frontend and backend electronic business-related sale transactions between individuals and businesses, between businesses, between governments and businesses, and between governments and their citizenry.

In this study, a *sector-based* information privacy law or regulation is one, which aims to protect the information privacy of one or more segments of businesses, groups, sectors, industries, or demographics (Schwartz, 2009), rather for the whole nation. For instance, unlike the European Union, the United State has sector-based privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which protects the patients' health records, and the Children's Online Privacy Protection Act (COPPA) of 1998.

1.5 Structure of the Papers

The rest of the paper is organized chronologically as follows: the literature review in Chapter 2; the research methodology, including the theoretical basis, theoretical model, research design, instrument development, research strategy, data collection and analysis, and analysis of empirical validation approach in Chapter 3. The summary of the hypotheses was also presented in Chapter 3.[1] The data collections, analyses, validations, and findings were reported in Chapter 4. Finally, the conclusion of the study, implication, limitations, and recommendations were meticulously delineated in Chapters 5.

[1] See Table 6 for the summary of the research hypotheses.

Chapter 2

Literature Review

2.1 Introduction

Until recently, scholars have conceptualized general privacy as a withdrawal process to avoid dealings with others, or as a mechanism to regulate access to the self, group, or organization (Altman, 1975). However, researchers have since distinguished between *general privacy* and *information privacy* although the terms are still being used interchangeably in literature and in our everyday discussions. Therefore, apart from the definition of the terms, any mention of privacy or information privacy in this study refers to information privacy.

The truth is that the difference between general privacy and information privacy is blurred, even in literature. Clarke (1999) illustrated the loss of confidence on privacy resulting from the growth of the Internet and the escalation in the use of surveillance systems. The paper suggested that privacy has four dimensions: privacy of a person, privacy of personal behavior, privacy of personal communication, and privacy of personal data. A closer examination of the dimensions indicates that privacy of personal behavior, privacy of personal communication, and privacy of personal data are centric to information privacy, whereas privacy of the person is more in alignment with the general privacy. In addition, Culnan and Bies (2003) define information privacy as the "ability of individuals to control the terms under which their personal information is required and used" (p. 326). Yet, consumers have limited control over their personal information online today, relatively speaking. Additionally, individuals have limited control over their private communications or their personal data because our private communication are readily available on demand from our Internet mail servers, employers' mail servers, or subject to both authorized and unauthorized surveillances (Gertler, 2004).

Information privacy paradox is a problem in information privacy discipline and is evidence in other disciplines as well. For illustration, this study used the concept of the *value of information* (VOI) to demonstrate the findings in previous studies and to show the ubiquitousness of studies on the phenomenon across academic disciplines, in order to strengthen the research problem and the research argument. Oostenbrink et al. (2008) used Markov Probabilistic Model to compare a 5-year cost and effect on patients with moderate to severe bronchodilators, which are tiotropium, salmeterol, and ipratropium. In the paper, Oostenbrink et al. (2008) stated, "Value of information analysis informs decision-makers about the expected value of conducting more research to support a decision" (p. 1070).

In this context, VOI will allow the study to judge the potency and value of further examination of information privacy paradox; i.e., to assess logically and make a decision of whether the study will add to the body of knowledge. The value of information is achieved through a thorough evaluation of previous academic work on a phenomenon. This is necessary because literature review allows a researcher to evaluate the validity of a research problem, and permits an estimation of known facts and assumptions, which are fundamental to problem solving (Baker, 2000).

Researchers and practitioners in a variety of disciplines, such as information privacy, information systems security, management information systems, healthcare, marketing and advertising, law and ethics, and economics have been examining the phenomenon of information privacy for many years. Nonetheless, the central theme in the body of work, despite variations in area of studies, has been the notion of a consumer's not having the ability to control how his or her personal identifiable information, or his or her protect health information is collected, used, stored, or shared. In a Harvard Law Review, Warren and Brandeis (1890) argued that the design of the law must be geared toward protecting an individual's information from society or from the public, especially the information an individual does not want to be made public or passed on to a third party. Ironically, in the United States, unlike in the European Union (EU) and other western countries, there is no comprehensive Act or regulation on data or information privacy.

Information privacy laws in the United States are sector-based, segmented, and industry driven. For example, in the healthcare sector, the Health Insurance Portability and Accountability Act (HIPPA) of 1996 was enacted to ensure the prevention of an unauthorized access (confidentiality) to patients' protected health information, which is an individual's identifiable health information. The Children's Online Privacy Protection Act (COPPA) of 1998 was enacted to allow parents to control the type of information a Website can collect from their children. While advocates, such as the Center for Democracy and Technology suggested that a comprehensive information privacy law in the United States would "minimize international regulatory conflicts about privacy" and harmonize current laws in the country, Schwartz (2009) warned that a preemptive information privacy law would be counterproductive, and may be far-reaching. The paper argued that a sector-based continuance or a bottom-up enactment of privacy law from the States in America would allow for experimentation of information privacy law prior to extending it to the federal level. In disagreement to the sector-based enactment of information privacy laws, Bellia (2009) argued that it is ill advised to ignore the impact of the federal influence on a state law, and that lack of federal law on the subject may be an inadvertent abdication of congressional responsibility. Congress and state legislatures have responsibility to enact laws for the federal government and the states respectively, and the judiciary at either of the two levels of government interprets the laws. Hence, competitive federalism in this context refers to the leadership competition between the states and the federal government for enactment of information privacy laws.

Additionally, in Table 1, this study categorizes chronologically and presents some interdisciplinary literature it considered to be relevant to the research argument, which is that a cognitive look at the research problem is warranted. Moreover, the study believes that incorporating literature from other disciplines would help in putting this study in perspective and would assure completeness in the study's capacity to assess and acknowledge previous works and findings. Hence, the study adapted privacy regulation theory for theoretical conceptualization and operationalization, and analyzed other literature, which dealt with information privacy paradox insights. In the literature review, the study assessed the impact of an obligatory passage point with respect to a consumer's ability to choose what kind of personal information he would share in an e-commerce environment and when to share it. The study also looked at information privacy risks and trust, current privacy regulatory provisions, and online personal information collection, use, and storage. In addition, the study deliberates on the dichotomy between information privacy and information systems security, and on information privacy concerns, information privacy paradox, and information privacy calculus.

Table 1. Information Privacy Literature Review

Information Privacy Perspective	Unit of Analysis	Interdisciplinary Areas	Literatures
Cognate-based Information Privacy	- Individual	- Information Systems	(Smith et al., 2011)
Provision of personal information as obligatory passage point (OPP)	- Individual - Groups - Organization	- IS Security Management - IS Security Policy - Privacy, Law, and Ethics	(Smith et al., 2011; Mager, 2009; Callon, 2007; Backhouse, Hsu, & Silva, 2006; Latour, 1987; Callon, 1986)
Information privacy risks and trusts	- Individual - Organization	- Information Privacy Management	(Smith et al., 2013; Norberg et al., 2007; Dinev & Hart, 2006; Sayre & Horne, 2000; Milne & Boza, 1999; Hoffman et al., 1999)
Information privacy regulation	- Individual - Organization	- Information Privacy Management - IS Security Management - IS Security Policy	(EPIC website, 2013; U.S. GAO-14-251T, 2013; GAO-13-663, 2013; Schwartz & Solove, 2013; Govtrack Website, 2013; Manolescu, 2012; Bellia, 2009; Schwartz, 2009; Warren & Brandeis, 1890)
Personal information collection, use, and storage	- Individual - Organization	- IS Security Management - Information Privacy	(Google Play Store, 2014; Häyrinen et al., 2008)
Information privacy and information systems security dichotomy	- Individual - Organization	- Information Privacy Management	(IGP Website, 2013; Symantec, 2010; Anderson & Agarwal, 2010; Son & Kim, 2008; Hui et al., 2007; Gertler, 2004; Grubbs & Phelps, 2003)
Information privacy concern	- Individual	- Information Privacy Management	(Dinev et al., 2013; Smith et al., 2011; Hui et al., 2007; Berendt et al., 2005; Jamal et al., 2005)
Information privacy paradox	- Individual - Organization	- Information Privacy Management	(Keith et al., 2013; Mothersbaugh et al., 2012; Smith et al., 2011; Norberg et al., 2007; Dinev & Hart, 2006; Berendt et al., 2005; Sayre & Horne, 2000; Milne & Boza, 1999; Hoffman et al., 1999)
Information privacy calculus	- Individual - Organization	- Information Privacy Management	(Lee et al., 2011; Xu et al., 2010; Li & Sarathy, 2007; Xu et al., 2009; Dinev & Hart, 2006; Dinev et al., 2006; Culnan & Bies, 2003; Culnan & Armstrong, 1999; Stone & Stone, 1990; Laufer & Wolfe, 1977)

2.2 Cognate-Based Information Privacy

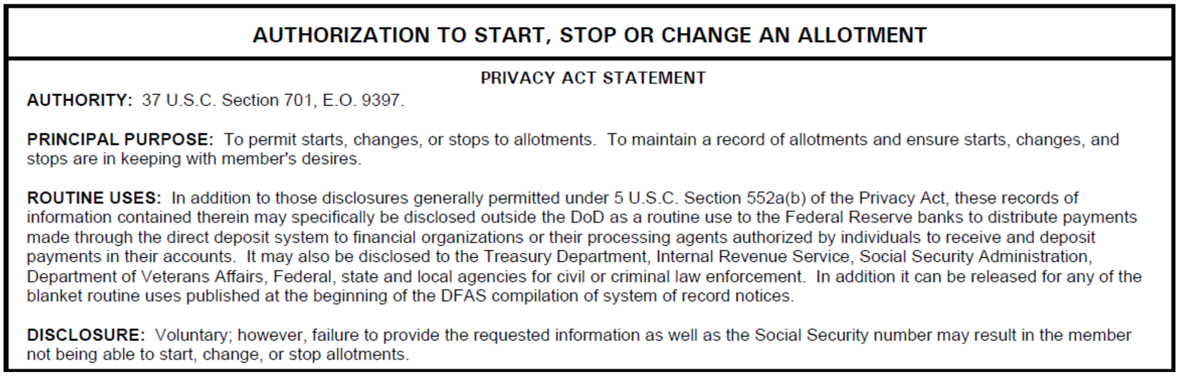
The review of literature has revealed that most assessments of the information privacy studies have been from the economic and value perspectives (Smith et al., 2011). The need for a different perspective attests to the potency of this study. A critical review of 320 articles and 128 books, Smith et al. (2011) revealed that the number of studies in information privacy from the cognitive standpoint is marginal (Smith et al., 2011); only 27 out of the 448 articles and books on information privacy were categorized as cognate-based. In addition, 23 out of the 27 studies treated privacy as a *control*, and only four treated it as a *state*. A treatment of privacy as a control refers to how an individual regulates access to the self, whereas a treatment of privacy as a state refers to the individual's nature or predisposition (Smith et al., 2011). Hence, the examination of information privacy paradox in this study is based on an individual's predisposition.

The analysis about the state of extant literature is important because existing studies had focused more on how individuals limit access to the self, and very little on the antecedents that drive their disclosure decisions. For instance, in explaining the scope of their study, Knijnenburg et al. (2013) stated, "This work does not define an overall measure of a person's rate of disclosure...this work typically also does not try to explain how disclosure behaviors come about, or how they can be influenced" (p. 1145). A pure economic or value evaluation presumes that individuals or consumers are always rational actors. However, empirical evidence showed that consumers are not always rational actors. Pink (2009) illustrated peoples' irrationalities by showing how a pursuit of fair play, a desire for revenge, or an irritation could override peoples' rationalities. [2]

[2] Complete scenario is in Section 2.10: "Suppose somebody gives me ten dollars and tells me to share it—some, all, or none—with you…" (Pink, 2009, p. 25)

2.3 Provision of Personal Information as an Obligatory Passage Point (OPP)

It is almost impossible today for a consumer to transact online without giving up some sort of his or her personal information compulsorily, even when such disclosure is deemed voluntary. In the context of information privacy, the position is that a data or information is an OPP if the provision of such data or information is deemed to be voluntary, but is actually indispensable or is required for completing an online transaction (Backhouse, Hsu, & Silva, 2006; Callon, 1986; Latour, 1987). The implication is that the absence of such information will cause the online transaction to be incomplete. For example, it is evident that an online merchant would need a customer’s name, address, and credit or debit card information in order to process a sales order, receive payment for goods or services, and ship the order to the right person, to the right place, at the right time, and in the right quantity. Hence, even when a merchant declares the provision of such information voluntary, in reality, it is mandatory; as such, the provision of the information would become an OPP. In another example, the U.S. Department of Defense uses DD Form 2558 (Sep 2002) shown in Figure 1 to start, change, or stop allotments for service members. The Privacy Act Statement on the form distinctively states, “Voluntary; however, failure to provide the requested information as well as the social security number may result in the member not being able to start, change, or stop allotments.” In effect, a social security number, in conjunction with other PII, is an OPP for the service expressed on the form. Therefore, the form should read *mandatory* rather than *voluntary*, because without that personal information, service member would not receive the required allotment service. With these examples, one can see how consumers’ personal information could inadvertently become an obligatory passage point. In fact, consumer disclosure of personal information is an obligatory passage point in electronic commerce. An electronic commerce is a market construction of actors who quit as soon as a transaction is complete, but never disentangled completely because of the data exchange (Callon, 2007).



AUTHORIZATION TO START, STOP OR CHANGE AN ALLOTMENT

PRIVACY ACT STATEMENT

AUTHORITY: 37 U.S.C. Section 701, E.O. 9397.

PRINCIPAL PURPOSE: To permit starts, changes, or stops to allotments. To maintain a record of allotments and ensure starts, changes, and stops are in keeping with member's desires.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act, these records of information contained therein may specifically be disclosed outside the DoD as a routine use to the Federal Reserve banks to distribute payments made through the direct deposit system to financial organizations or their processing agents authorized by individuals to receive and deposit payments in their accounts. It may also be disclosed to the Treasury Department, Internal Revenue Service, Social Security Administration, Department of Veterans Affairs, Federal, state and local agencies for civil or criminal law enforcement. In addition it can be released for any of the blanket routine uses published at the beginning of the DFAS compilation of system of record notices.

DISCLOSURE: Voluntary; however, failure to provide the requested information as well as the Social Security number may result in the member not being able to start, change, or stop allotments.

Figure 1. Excerpt from DD Form 2558 Privacy Act Statement.

Furthermore, the degree in which consumers' personal information has become an OPP is profound in electronic healthcare and in electronic government because of the sensitivity of the information and because of the need to maintain the integrity of the data or information. Since the review of literature has shown that consumers have limited or no control of their information upon their disclosure (Son & Kim, 2008; Tsai et al., 2011), consumers are left with the discretion or the decision to willingly disclose their personal information in an ecommerce environment.

To internalize this concept, it is crucial for us to look at this involuntary disclosure of personal information from the actor-network theory (ANT) perspective (Mager, 2009). For example, Google may be considered an obligatory passage point for Website providers because it serves as a major actor (provides maximum stability and maximum exposure for Website providers) and a primary search engine for Internet users; hence, Internet providers are forced to adapt Google's algorithm if they want to reach a greater number of consumers.

Actor-network theory is presented here to illustrate the relationships and the interdependencies among actors and not to show Google as a domineering power. Callon (2007) delineated that actors have variable competencies and forms, and could use them to foster their interest and establish an OPP (Backhouse et al., 2006). In information privacy context, organizations and Internet merchants require consumers' personal information for sales and delivery of goods and services. The key is that if a consumer fails to provide his or her personal information during such transaction, it may be impossible for the merchant to process the order or shipment. The implication is that a consumer who wants to place an order must provide all relevant personal information necessary to complete the transaction, including financial and shipping information. Therefore, the study argues that consumers constantly find themselves in this kind of situation, and that this is one of basis for the differences, we see in literature, in the hypothetical responses to personal information disclosure online and in the actual consumers' personal information disclosure behaviors.

Following the privacy calculus argument, a consumer's decision to transact online depends largely on her reasonable decision to provide the necessary information to the merchant. The question is to what degree does privacy calculus affect consumers' willingness to disclose personal information. Information privacy as obligatory passage point is relevant to this study because although we acknowledge the effect of privacy calculus, we argue that the consumer's disposition could override her privacy calculus. A counter argument is that consumers' hesitancy in using a particular Website could force an online merchant to improve the security of the site, display accreditation artifacts, and conspicuously exhibit information privacy policies and practices. Hence, consumers' reluctance in engaging a particular business outfit online could become an OPP as well (Smith et al., 2010).

2.4 Information Privacy Risk and Trust

Information privacy risk and trust have been identified in literature as antecedents to consumer personal information disclosure behaviors online (Milberg et al., 2000; Norberg et al., 2007; Smith et al., 1996). The relationships between Internet risk and trust have been examined extensively as well. Dinev and Hart (2006) found that Internet trust and personal Internet interest outweigh privacy risks, and affect an individual's decision to disclose personal information online. Malhotra et al. (2004) suggested that Internet users' information privacy concerns (IUIPC) affects trusting and risk beliefs. Additionally, Hoffman et al. (1999) had affirmed that consumers' mistrust of the Web providers and online merchants affect their personal information disclosure behaviors. Others studies had assessed the affect and the association between risk and trust to consumers' willingness to disclose personal information online as well. For example, Milne and Boza (1999) contended that trust influences behavior directly. Norberg et al. (2007) argued that the disparity between intended and actual disclosure of personal information is because risk considerations influence intention more, while trust considerations influence actual disclosure more. Dinev et al. (2013) suggested that perceived benefits of information disclosure, information sensitivity, information transparency, and regulatory expectation affect perceived risk, and that perceived risk affects perceived privacy. The paper argued that a net positive benefit would cause consumers to ignore or accept identified potential risks associated with personal information disclosure online. In addition, Sayre and Horne (2000) showed that there is a difference between perceived privacy violation apprehension prior to personal information disclosure and the indifference during actual disclosure.

Assessment of current the literature on the consumers' information privacy risk and trust is relevant to this study because there is a need for the study to control the effects of trust and risk constructs in order to ascertain the relationships between the underlying concepts in the privacy regulation theory and the variable of interest properly. Hoffman et al. (1999) suggested that the trust between consumers and online merchants could be attained by allowing consumers to transact online anonymously or pseudonymously. In addition, the paper advocated for recognition of consumers' right to data ownership in ecommerce, i.e., opt-in rather than opt-out, use of the informed consent policy, and the like. The point is that as more and more organizations strive to improve the security of their systems, and lean toward data management transparencies, consumers' concerns and risk valuation will dwindle. Therefore, the supposition is that as an organization's capacity to safeguard a consumer's personal information increases, the consumer's trusting of the organization's Website will increase and the consumer's risk concerns will decrease.

2.5 Information Privacy Regulation

The government accountability office (GAO-13-663, 2013) found that there is a gap in information privacy statutory framework in that the framework does not always reflect Fair Information Practice Principles (FIPP). The FIPP in Table 2 was developed by the Organization for Economic Co-operation and Development (OECD) in 1980 for the control of personal data within and outside a country (OECD Website, 2015). One of the problems in information privacy is the difficulty in having a single acceptable definition for personal information. Furthermore, there is variation in the definition of personal information even in the United States. For example, while California SB 1386 expanded the definition of personal information in 2011, by adding medical information and health insurance information as personal information data elements (Govtrack Website, 2013),

Table 2. Fair Information Practice Principles (adapted from OECD)

Principle	**Description**
Collection limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specific	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except 1) with the consent of the data subject, or 2) by the authority of law.
Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual participation	An individual should have the right: 1) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; 2) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; 3) to be given reasons if a request made under subparagraphs is denied, and to be able to challenge such denial; and 4) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures, which give effect to the principles stated above.

the 201 CMR 17.00 in Massachusetts does not. Similarly, while some argue that the definition of personal information is disjointed in the U.S., others feared that the EU’s definition is too broad.

According to U.S. GAO-14-251T (2013), there is “no overarching federal privacy law [that] governs the collection and [the] sale of personal information among private-sector companies, including information resellers” (p. ii) in the United States, however, specific laws have been enacted to govern the collection, the use, the sharing, and the protection of personal information (U.S. GAO-14-251T, 2013). The Government Accountability Office (GAO) is an independent government auditor that reports to the U.S. Congress on matters of great importance. Although the Fair Credit Reporting Act was enacted to restrict the use and the distribution of personal information for credit or employment determination eligibility, it did not limit the use or distribution of such information for marketing purpose (U.S. GAO-14-251T, 2013). In addition, the gaps noted in the report to congress is that (1) there is no federal law that grants consumers access to an organization’s information, (2) there is no available listing of organizations, which store and market consumers’ personal information to a third party.

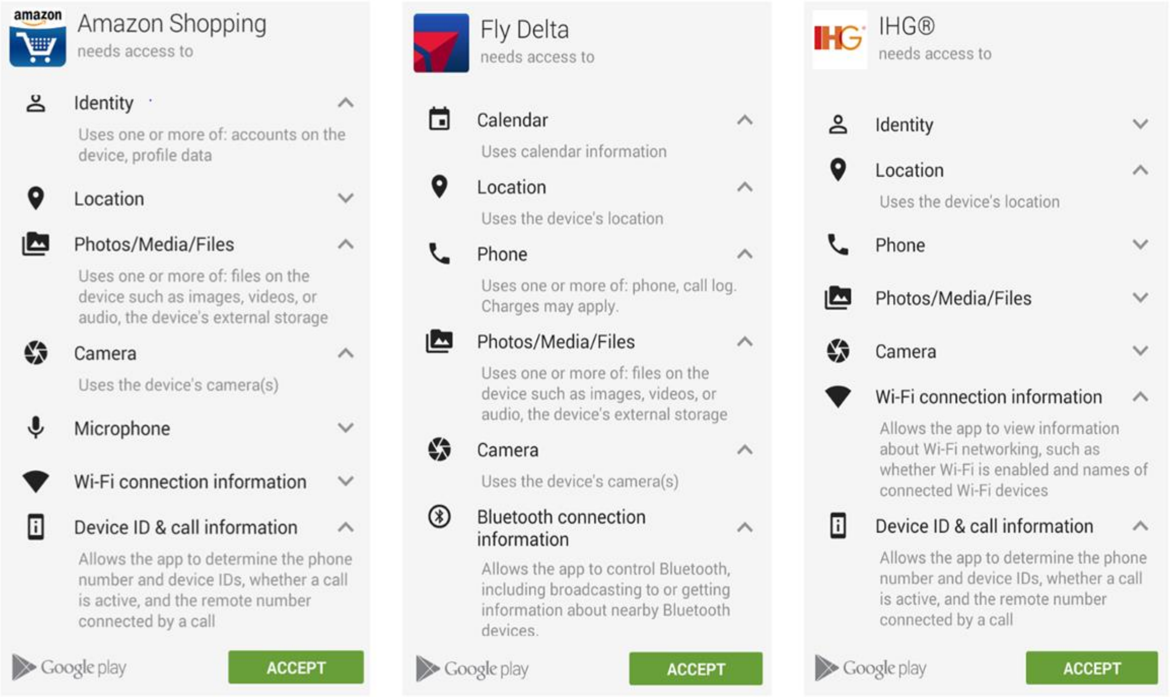
Unlike the European Commission Privacy Directives, information privacy law in the U.S. is sector-based. The Directive is a comprehensive information privacy law for members of the European Union. In the United States, there are two schools of thought regarding how inclusive information privacy law should be. While some information privacy advocates argue for a more comprehensive regulatory approach, others argue that a unitary approach is a recipe for ineptness, and would be cumbersome and inflexible (U.S. GAO-13-663, 2013). In the Yale Law Review, Schwartz (2009) argues that a comprehensive privacy law in the U.S., otherwise called the omnibus law will enhance the current state and federally sector-specific laws for adequacy, recognize and fill the statutory gap in current law due to technological convergence and ambiguity, and lessen the free flow of data issue like the EU Directive. Furthermore, supporters of a comprehensive information privacy regulation, including an estimated 20 U.S. consumers, privacy, and civil liberties groups sent letters to the European Parliament in 2013 in support of its new data protection law. Until the U.S. passes a comprehensive privacy legislature, the groups wrote, "The European Union offers the best prospect for the protection of Internet users around the globe" (EPIC website, 2013b).

The problem with information privacy initiatives in the U.S. is that it is not only sector-based; it is narrow in scope and industry centered. As a result, one of the drawbacks from this multi-echelon information privacy laws is the difficulty and the cost of keeping up with variances in the law at organizational level, especially those who have businesses across state lines. In the Harvard Law Review, Warren and Brandeis (1890) argued that the design of the law must be geared toward protecting individual’s information from society; especially the information an individual does not want to be made public or passed on to a third party. The notion of protecting individual personal information is not new. However, the ease at which information is collected and shared in recent times, due to advances in technology, is new and evolving. Secondly, the issue is not necessarily about the ease of personal information collection, but about the control and the effectiveness of the collection process, the storage, and the use of consumers’ personal information.

Supporters of an overarching federal privacy law argue there is a need for the U.S. to enact a comprehensive law to protect consumers' personal information. While advocates of this idea support the notion that perceived justice (interactional, procedural, and distributive justice) affects information provision (Son & Kim, 2008), others fear the impact of such law on the free flow of commerce online. In its report to congress, the Government Accountability Office found that industrial representatives in the U.S. fear that "restrictions on the collection and use of personal data would impose compliance costs, inhibit innovation, and reduce consumer benefits" (GAO-14-251T, 2013, p. 2). Secondly, opponents of a comprehensive privacy law in the U.S. argue that there are series of segmented and state laws in the United States on information privacy, even though there is no comprehensive law (GAO-13-663, 2013), unlike in the European Union. Therefore, the deduction from government's view regarding comprehensive privacy legislature seems to be relative to *mohist consequentialism* view (Ivanhoe & Van Norden, 2005), which is that the expected net outcome or the value of a consumer's personal information disclosure online, to the consumer and/or to the organization, should justifies a consumer's decision in disclosing personal information in ecommerce. Philosophically, *Mohist consequentialism*, otherwise called state consequentialism is a form of ethical theory, which evaluates the moral worth of an action based on its contributions or values to the state or the community (Ivanhoe & Van Norden, 2005).

2.6 Personal Information Collection, Use, and Storage

There are fundamental questions concerning consumers' personal information collection, use, and storage. For information collection, the questions are (1) whether consumers' personal information are collected in a legal and ethical manner, (2) whether consumers are aware of who, where, when, and which information are being collected, and (3) whether consumers' personal information disclosure are voluntary? Figure 2 presents Amazon, Delta, and Intercontinental Hotels Group (IHG) personal information requirements from consumers in exchange for the free use of their apps in their mobile devices (Google Play Store, 2014). Empirical and anecdotal evidence show that in e-healthcare, the following information may be required and collected: social security number, insurance policy number, home address, date of birth, personal and family medical history, food and drug allergies, social activity history, list of current medications and the like (Häyrinen et al., 2008). Similarly, in e-government, social security number, date of birth, sex, and place of birth are required for U.S. passport using DS-11 form, and for voter's registration or driver's license.



Amazon Shopping
needs access to

Identity
Uses one or more of: accounts on the device, profile data

Location

Photos/Media/Files
Uses one or more of: files on the device such as images, videos, or audio, the device's external storage

Camera
Uses the device's camera(s)

Microphone

Wi-Fi connection information

Device ID & call information
Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

Google play ACCEPT

Fly Delta
needs access to

Calendar
Uses calendar information

Location
Uses the device's location

Phone
Uses one or more of: phone, call log. Charges may apply.

Photos/Media/Files
Uses one or more of: files on the device such as images, videos, or audio, the device's external storage

Camera
Uses the device's camera(s)

Bluetooth connection information
Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

Google play ACCEPT

IHG®
needs access to

Identity

Location
Uses the device's location

Phone

Photos/Media/Files

Camera

Wi-Fi connection information
Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

Device ID & call information
Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

Google play ACCEPT

Figure 2. Online Merchants' Personal Information Requirements.

For personal information use, the questions are whether and how personal information is used beyond its initial intended use, and whether the information is being transferred to a third party in an appropriate manner. Additional question is what are the sell-resell implications of information privacy?

For information storage, the questions are about the security and accessibility of the information, the data authentication, and the communications between organizations and the consumers. Review of literature indicated that scholars around the globe have attempted to answer some of the aforementioned questions.

2.7 Information Privacy and Information Systems Security Dichotomy

The value of personal information is huge, so is the level of information systems (IS) security necessary to protect it. According to Gertler (2004), businesses use personal information to understand the market and develop new products and services, and governments use it to enhance services, track cyber criminals, test the effectiveness of new medical drugs, or track terrorist activities. In addition, healthcare providers use personal information to document patient care, medical history, and medical research trials, among others. Hence, the need to accumulate personal information to propagate e-commerce, e-government, and e-healthcare activities have engineered an unparalleled proliferation of database developments and the sharing of personal information. Similarly, the expansion in database management, including cloud computing, has expatiated information systems security vulnerability and threats in terms of data confidentiality, integrity, availability, authentication, and communication. Striking the balance between information privacy preservation and ensuring the security of the organizations and governments' information systems have been a subject of discussion in recent times, especially in the United States and other developed and developing countries.

Edward Snowden stealing of the state secrets from the National Security Administration (NSA) database has brought the exponential difficulty the problem poses to light, primarily because of his revelation of the NSA's overwhelming aggregation of citizens' metadata in the U.S. and elsewhere. The exposure of massive data collection, including personal information of prominent leaders around the world, resulting from the NSA debacle, has threatened the political and diplomatic relationships between the U.S. and other countries. For example, in 2013, Dilma Rousseff, President of Brazil and the directors of the five regional Internet Standard Registries called for an end to the U.S. Commerce Department oversight of the Internet Corporation for Assigned Names and Numbers (ICANN) during the Internet Governance Project meeting in Montevideo, Uruguay (IGP Website, 2013). The registries were established and charged with the responsibility to manage internet protocol (IP) addresses and the autonomous system (AS) number within their jurisdictions. The registries are the American registry for Internet numbers (ARIN) for Canada, Caribbean and North Atlantic Islands, and the United States; the Internet numbers registry for Africa (AFRINIC) and Indian ocean; the APNIC for Asia and portions of Oceania; the LACNIC for Latin America and the Caribbean; the RIPE NCC for Europe, Middle East, and Central Asia. The ICANN, through the Internet Assignment Numbers Authority (IANA), (1) manages Internet domain name, (2) coordinates recourses, and (3) assigns protocols and maintains address and routing parameter area (ARPA).

Empirical and anecdotal evidence have shown that information privacy and information systems security are intertwined because of the shared network resources, interconnectedness, and interdependences. Information privacy is at risk because users have unequal availability of security resources to deal with the home computer security issues and requirements, and unequal level of experience in dealing with software vulnerabilities and threat in the e-commerce marketplace (Anderson & Agarwal, 2010). In addition, users are worried about their personal information seepages to unauthorized persons due to the current upward trend in Web-based attacks (Symantec, 2010), as well as how organizations handle the information at their disposal (Hui et al., 2007; Son & Kim, 2008).

Recently, public debate has shifted to the question of what level of interdependency exits between information privacy and IS security, and the tradeoff between the two. While some believe that the relationship between the two is bidirectional, others think that the relationship is one directional, which means that although it is difficult to achieve a desirable level of information privacy without adequate IS security, achievement of IS security is not dependent on acceptable information privacy. Grubbs and Phelps (2003) evaluated information privacy and IS security policies and practices of 102 churches and found that although the Websites were collecting PII similar to that of the e-commerce sites, their awareness and practices in protecting their users personal identifying information were undesirable because they sometimes post their parishioners' PII online. The stealing of the data from the NSA databases, the hacking and wiping out of data from Sony Incorporation computer systems in December 2014, and the constant software attacks experienced by individuals and organizations have revealed how information systems security and information privacy are interwoven.

2.8 Information Privacy Concerns

The prevalence of information privacy anxiety experienced by consumers are not only with how organizations collect, use, or store their information, but about the security of their personal information on the network, as well as the information in the database. Smith et al. (2011) indicated that privacy experience, privacy awareness, personality and demographic differences, and culture are antecedents to privacy concern. Hui et al. (2007) evaluated the influence of privacy statement and privacy seal, monetary incentive, and the amount of information on personal information disclosure online. Although privacy statement proved to be significant, privacy seal was not. Although consumers' information privacy concerns are constant, the results from the empirical examination on how to tackle the problem have been inconsistence. For example, Berendt et al. (2005) found that the privacy statement has no significance to the consumers' personal information disclosure online, but Hui et al. (2007) found that privacy statement positively influenced consumers' personal information disclosure. Furthermore, Dinev et al. (2013) argued that the consumers' perception of risk based on perceived value of information, information sensitivity, information transparency, and regulatory expectations influence their personal information disclosure. Yet, Hui et al. (2007) found no significant influence between the information sensitivity and the online personal information disclosure behavior. The contrast is that the advances in information technology have created a very dynamic evolving marketplace, and have exponentially exacerbated the need for consumer personal information gathering and concerns.

Electronic commerce, electronic healthcare, electronic government, and the like have created an insatiable need for consumers' personal information, and the news of data breaches at organizations such as Target, Sony, and others in recent months and years have not helped matters. Secondly, organizations or online merchants want a consumer to register every electronic device the consumer purchases online. Understandably, some of the reasons for the registration requests are imperative; usually to allow for a quicker technical support in an event of a system failure, for service support, and for software updates. The issue is that soon after a registration, the consumer would start receiving sales solicitations and personalized advertisements directly to their physical address or to their email address, which is indicative that the consumer's information has been passed on to a third parties. A consumer may use a unique name and email address combination to find out the registration that caused a sales solicitation. Consumers are concerns and ambivalent because they have limited or no opportunity for redress since organizations, especially those in the United States have greater control of consumers' personal information, and there are limited federal legislative restrictions on how an online merchant or an organization uses consumer personal information EMC Website. (2015)

2.9 Information Privacy Paradox

The Information privacy paradox is the gap between consumers' intended and actual disclosure of personal information online or in e-commerce transactions (Awad & Krishnan, 2006; Norberg et al., 2007; Smith et al., 2011). Norberg et al., 2007 explored and found that information privacy paradox exists in e-commerce in a two-phased quantitative research study. Awad and Krishnan (2006) examined the relationship between information technology features and consumer sharing of personal information online from organizational perspective. Furthermore, Awad and Krishnan recommended that investment in online personalization should be geared more toward the information privacy of the unconcerned and the pragmatists rather than toward the fundamentalists (Westin, 1991). The recommendation stems from the fact that it may be a fruitless exercise to expend limited resources on convincing an information fundamentalist, and an organization may be better served if it invests on gathering personal information from the pragmatist and unconcerned. Other studies have also identified the paradoxical gap (Berendt et al., 2005; Smith et al., 2011). Sayre and Horne (2000) found that there is a difference between the consumers' perceived privacy violation apprehension prior to the personal information disclosure and their indifference during actual disclosure. Norberg et al. (2007) argued that the disparity between the intended and actual disclosure of personal information is because risk consideration influences intention more, while trust considerations influences actual disclosure more. Milne and Boza (1999) had contended that trust influences direct marketing usage behavior directly, and Hoffman et al. (1999) found that risk and trust influence intention and subsequently influence behavior.

In addition, Dinev and Hart (2006) found that Internet trust and personal Internet interest outweighs privacy risk, and influence individual's decision to disclose personal information online. Meanwhile, Berendt et al. (2005) also evaluated consumers' stated preferences and actual behavior, and found that while consumers' normative level of privacy concerns is strong, their online interactive privacy behaviors are relatively weak. The paper contended, "Users rely on legal protection, even though it is widely known that laws and regulations have difficulty responding to the fast changes in Internet communications." More recently, Keith et al. (2013) suggested that there is a continuous existence of information paradox because personal information disclosure intentions are not indicative of actual disclosure in a controlled experiment involving 1025 mobile device users. The paper emphasized that the accuracy of the personal information disclosed by a user is as important as the actual disclosure; otherwise, the efficacy of data or information interpretation may be skewed or jeopardized. Additionally, Mothersbaugh et al. (2012) suggested that the disparity between consumer intended and actual personal information disclosure could be a function of the sensitivity of information being requested, which was not considered in prior academic works. A look at Mothersbaugh et al. (2012) will prompt the question of why the sensitivity of the information was not a problem for the participants initially if a longitudinal data collection occurred.

2.10 Information Privacy Calculus

The concept and roles of information privacy calculus on consumer's preparedness to share personal information in an e-commerce environment has been examined extensively in the literature (Culnan & Armstrong, 1999; Culnan & Bies, 2003; Dinev et al., 2006; Dinev & Hart, 2006; Laufer & Wolfe, 1977; Lee et al., 2011; Li & Sarathy, 2007; Stone & Stone, 1990; Xu et al., 2010). In Culnan and Armstrong (1999), privacy calculus is described as an assessment by consumers that the personal information they shared online will be used fairly and that they would not be affected adversely. Privacy calculus is also described as an assessment of risks and benefits associated with information privacy protection by employing fair information practices (Dinev & Hart, 2006; Lee et al., 2011; Xu et al., 2009).

For a detail look at the phenomenon and for a better understanding of information privacy calculus, we looked at Laufer and Wolfe (1977) articulation of individuals' calculus of behavior, which was characterized in three major ways. The *first* is the presumption by individuals that they have control of their information, which allows them to minimize potential consequences. The *second* is the dynamic disclosure decisions individuals make because of the vagueness and unpredictability of how the information would be used. The *third* is the inability of individuals to predict future consequences of personal information disclosure. Thus, it is imperative that we ask ourselves whether the privacy calculus is real or imaginary. Although the conceptual principle of information privacy is real, the practicality seems unreal because consumers' assumption of control of their personal information after disclosure is a mirage. The illusion of control is real because consumers cannot make an informed assessment of how their information is used and they cannot project or predict future risks or consequences. This realism calls to question the justification of privacy calculus, as an antecedent to information privacy paradox.

While the study believes that information privacy calculus is related to information privacy paradox, it also argues that a consumer predisposition is related to information privacy paradox because of the nonexistence of the "hyper rational calculator-brained person" (Pink, 2009, p. 25). The following illustrates the fact that people are not always rational and that risk-benefit calculations expressed in privacy calculus may not always be related to information privacy paradox.

> Suppose somebody gives me ten dollars and tells me to share it—some, all, or none—with you. If you accept my offer, we both get to keep the money. If you reject it, neither of us gets anything. If I offered you six dollars (keeping four for myself), would you take it? Almost certainly. If I offer you five, you'd probably take that, too. But what if I offered you two dollars? Would you take it? In an experiment replicated around the world, most people rejected offers of two dollars and below. That makes no sense in terms of wealth maximization. If you take my offer of two dollars, you're two dollars richer. If you reject it, you get nothing. Your cognitive calculator knows two is greater than zero—but because you're a human being, your notion of fair play or your desire for revenge or simple irritation overrides it (Pink, 2009, p. 25).

From privacy calculus perspective, Smith et al. (2011), a review of 320 privacy articles and 128 books, noted that the salience of the individual risk-benefit tradeoff upon which consumers make online personal information disclosure decisions is based on expected net outcome. Additionally, Norberg et al. (2007) agrees with Milne and Boza (1999) that risk and trust considerations drive consumer information privacy paradox, but argues that the privacy paradox exists because risk considerations influence consumer intention to disclose personal information in an online setting more, while trust considerations affect actual disclosure more. Furthermore, Lee and LaRose (2011) argued that a consumer's personal information disclosure is based on the consumer's cognitive risk-benefit analysis, as well as the consumer's ability to overcome privacy invasions outcomes. The argument is in line with privacy calculus view because the paper found that personalized social cues immediacy affects personal information disclosure intention by triggering the self-regulatory mechanisms (Bandura, 1991) of information disclosure, and is mediated by social cognitive expectations of either a negative or a positive outcome. In cognitive theory of self-regulation, Bandura (1991) suggested that the self-regulative mechanism core principles are monitoring of one's behavior, monitoring of one's behavior determinants, and monitoring of the effects of the behavior.

Most studies on privacy calculus have used the individual as unit of analysis, and had ignored the fact that organizations have shared or greater responsibilities in preserving and protecting information privacy. Hence, Lee et al. (2011) cautioned that privacy calculus has not been evaluated from the organizational perspective; indicating that information privacy protection will increase if firms could mitigate price competition, minimize personalization scope or investment cost, increase consumers' participation in the personalization, and ensures that the consumer welfare and social welfare are at equilibrium.

2.11 Synopsis of Literature

Scholars in information privacy, information systems security, and other social science disciplines have examined the paradoxicalness of consumer personal information disclosure online. Thus far, the studies are economic and value based. While some of the literature is theoretical, others are atheoretical or reviews. Table 3 is a literature review reference summary, which provides pertinent information about some of the major works referenced in this study: author and the year, the research problem, the constructs or variables examine in the paper, the theoretical or conceptual framework, the data collection, the research methodology and the main findings of the study. Expanded literature review reference summary will be completed during the research proposal.

Table 3. Synopsis of Literature

Author (s) & Year	Research Problem	Constructs/ Variables	Theoretical Framework	Data Collection & Methodology	Main Findings
Norberg et al. (2007)	Examination of *Privacy Paradox* (disparity between intended and actual personal information disclosure)	Risk, Trust, behavioral intention, and disclose behaviors	Confirmation/ disconfirmation of previous studies	Two studies involving 43 Graduate students and 83 undergraduate students on a repeated-measure design. - Quantitative	1. Privacy paradox exits in information privacy. 2. Risk influences consumer online personal information disclosure intentions more, while Trust influences actual behaviors more.

Table 3. Synopsis of Literature (continued)

Author (s) & Year	Research Problem	Constructs/ Variables	Theoretical Framework	Data Collection & Methodology	Main Findings
Awad and Krishnan (2006)	An assessment of online information transparency on consumer's willingness to participate in online personalization for service and for advertising from Organization's perspective	Information transparency, previous online privacy invasion, privacy concern, and importance of privacy policy	Utility Maximization Theory	Survey from 400 online consumers -Hypothesis Testing	1. Consumers assign a different value to two outcomes based on benefit values, i.e., they are more willing to partake in personalization for online services than for advertising. 2. Consumers who value online transparency features are less likely to participate in personalization.
Bélanger and Crossler (2011)	Valuation of the current state of information privacy literatures	Theoretical classification of information privacy literature based Gregor (2006): Analyzing, Explaining, Predicting, Explaining and Predicting, and Design and Action	Review	Review of 500 information privacy articles - Thematic Analysis	1. Information privacy concept is interdisciplinary. 2. Research is generally theory based, student based, and U.S. centric.
Smith, Dinev, and Xu (2011)	Interdisciplinary assessment of information privacy literature	Development of APCO (antecedents → privacy concern → outcomes) Classification of general privacy: Value base (right and commodity) cognate based (state and control)	Review	320 Privacy articles and 128 books -Content Analysis Unit/Level of Analysis	1. There is need for empirical research in privacy. 2. The need for future research that targets other than individual level of analysis in privacy is warranted. 3. Focus on actual outcomes.

2.12 Summary

In the literature review section, this study used previous work to tell a story and to connect the dots from the past to the present that the threat to privacy or information privacy has been a constant. The section started with an introduction of the topic, which elaborated on the conceptualization of information privacy and how it relates to general privacy concepts from of old. Subsequently, the study showed how Smith et al. (2011) have classified information privacy studies as either valued-based (commodity and right) or cognate-based (control and state) and illustrated the gap in literature by focusing our evaluation of the phenomenon based on cognitive state. Furthermore, the study used the obligatory passage point concept to show that consumers have no real control of their personal information when transacting online, i.e., for the most part, consumers have limited control or an illusion of control (Backhouse et al., 2006; Smith et al., 2010). We went on to show the divergence in research findings on how the perceived risk or trust affects online users' willingness to disclose their personal information, despite the agreement or the consensus in the literature on the influence of privacy calculus.

Additionally, the review demonstrated the lack of universal privacy law and its impact in the U.S. as opposed to the European Union. We also analyzed the current studies on personal information collection, use, and storage practices, and sought to understand the dichotomy between information systems security and the information privacy. Finally, the review evaluated the relevancy of the information privacy concerns, paradox, and calculus to this study.

Chapter 3

Research Methodology

3.1 Introduction

This chapter provides the theoretical conceptualization and modelling of the consumers' selective personnel information disclosure, the information privacy constructs under examination, and the hypotheses. The chapter encompasses the details about the research design, instrument development and validation, measurement of the constructs, data collection, and data analysis. In addition, the chapter addressed the empirical validations, reliability, content validity, and construct validity approaches.

3.2 Theoretical Basis

The theoretical framework employed in this study was grounded on the *Privacy Regulation Theory* underpinnings or principles expressed in Altman (1975). A theoretical framework is a set of related concepts or constructs formulated based on a given theory to analyze, explain, predict, prescribe, and understand a phenomenon (Belanger & Crossler, 2011; Gregor, 2006; Lynham, 2002; Swanson & Chermack, 2013). Therefore, the aim of this study in employing the PRT theoretical framework was to explain and predict the information privacy paradox from the cognitive predisposition prism. Consequently, this study explained consumers' information privacy selective behaviors online and provided testable and casual predictions of the phenomenon.

3.2.1 Privacy regulation theory.

Altman (1975) defined privacy regulation theory as “the selective control of access to the self, involving dialectic, multimodal, and optimization processes” (p. 67). The paper argues that privacy regulation includes culturally universal and unique processes. Altman (1975) illustrated that privacy need is culturally universal and that the coping mechanism is culturally diverse. The notion is that the privacy regulation has dynamic, dialectic, and optimization characteristics as a culturally universal process and has multi-mechanism application characteristics as a culturally unique process.

Empirical and anecdotal evidences have shown that there is universality in privacy needs and uniqueness in the coping mechanisms. The universality is evidence in that the personal identifiable information and the protected health information are considered sensitive information in Europe, United States, United Kingdom, and in many other countries. The notion of universality was also illustrated by the uproar and condemnation, which followed the leak of the National Security Agency’s (NSA) information gathering scope and techniques around the world in 2013.

The uniqueness in the coping mechanism is obvious when you look at the information privacy laws and regulation in many states in the United States and in many countries. In a survey of 184 female resident students at the University of Utah, Harris et al. (1995) affirmed the universality of privacy need and the divergence of the cultural differences in the dialectic coping mechanisms. In addition, Smith et al. (2011), in a review of 320 privacy articles and 128 privacy books, noted that privacy is a culturally universal process due to its dynamic, dialectic, and optimization features, as well as a culturally unique phenomenon due to how individuals and groups regulate their social interactions.

In the context, the dynamic dialectic process, the multimodal process, and optimization process analyses implemented in this study are relative to the openness and closeness of how individuals engage in the electronic commerce or in online transactions, and how they exhibit their paradoxical personal information disclosure behaviors.

The privacy regulation theory has three core principles, including the state of the mind of the self, and they are relevant to this study. The principles are the dynamic dialectic process, the multimodal process, and the optimization process, according to Altman (1975). The relevancy of these principles emanated from the empirical quest to understand the paradox in the consumers' personal information disclosure behaviors in electronic commerce cognitively. Therefore, the followings are the delineations of the aforementioned principles.

The dynamic dialectic process principle explains the continuing interchangeable or contradicting opposing forces that urge people to want to be out of contact sometimes and want to be in contact at other times (Altman, 1975). The dialectic process has three important elements: the opposing need or urge, the unity of identity of the opposing forces, and the dynamic nature of the opposition (Altman, 1975; Foddy, 1984). The notion is that when such opposing forces exist, a person, a group, or an organization's reaction would naturally depend on the net strength of either of the forces. When the need to be open and accessible and the need to be closed and inaccessible are in conflict, the net strength would tilt toward being either accessible or inaccessible. Relative to information privacy and e-commerce, consumers have mixed feelings about engaging in e-commerce. On one hand, engagement in e-commerce makes consumers susceptible and vulnerable to the information privacy violations, and on the other hand, it provides some discount and personalization opportunities to the consumers. Hence, consumers are very selective in disclosing their personal information when they participate in an electronic commerce. In a critique of the Altman's definition of the privacy as a dialectic process, Foddy (1984) argues that privacy as a dialectic process must "clearly specify the elements in a unity of opposites" (p. 302) and must "clearly state how these elements are dynamically related so that the logic of change is made apparent." This study believes that the decision of whether or not to disclose personal information presents the unity of opposites. Besides, the information privacy paradox (Awad & Krishnan, 2006; Norberg, 2007) illustrated the dynamic logic of change, which shows the variations in the consumers' intended and actual personal information disclosure behaviors online.

Multimodal or multimechanism process involves "a network of behavioral mechanisms that people use to achieve desired levels of social interaction" (Altman, 1975, p. 67). It is a relational process through which a person or group of persons regulates access (openness and closeness) of the self to others, with changes in circumstances. It is also a verbal or nonverbal tactic, which allows an individual, or a group to achieve a variable level of privacy according Altman (1975). In information privacy context, individuals and groups aspire to have the ability to control how they deal with others and how they share their personal information online. However, in practice, it is impossible for an individual or a group to regulate access completely because sometimes consumers groggily share their personal information whenever the personal information becomes an obligatory passage point (Backhouse et al., 2006) in an e-commerce environment. At other times, consumers inadvertently and unknowingly share their personal information online. Altman (1975) defines privacy mechanisms as "the limits and boundaries of the self," and argues that an individual would develop a sense of individuality, competence, and self-worth "when the permeability of these boundaries is under the control of a person" (p. 68).

Optimization process is the concept of attaining an effective, compromised, or operative level of privacy over time as the dialectic characteristics of privacy changes because too much privacy is equally unsatisfactory as too little privacy. The goal of the optimization process is to achieve a balance in the interaction or to achieve privacy equilibrium, where the desired level of interaction is neither more contact nor less contact.

A rational assessment of the underlying core processes in the privacy regulation theory requires recognition of a fourth integral principle, which is the interaction between the actors in each process. In information privacy context, an act of privacy involves two actors, one whose information is being sought after and one who seeks the information. The actors could be an individual, a group, an organization, a state, or a country. Therefore, an instance of information privacy activity or the interaction between two or more actors is referred in this study as a *unit of privacy*. An interaction in itself may not be different from one another, all things being equally. However, the cognitive tendencies or predisposition of each actor involved during an interaction differentiates one interaction from another. The supposition is that the actors' states of information privacy would differentiate one interaction from another and would provide insight to the actors' privacy functions. Altman (1975) describes privacy functions as "(a) management of social interaction, (b) establishment of plans and strategies for interacting with others, and (c) development and maintenance of self-identity." To understand cognitive predisposition better, the study employed Westin (1970) classification of privacy: solitude, anonymity, reserve, or intimacy in order to make a cognitive predisposition assessment of the unit of privacy.

3.2.2 Rationale for privacy regulation theory.

The privacy regulation theory was chosen for this study because it provides the best theoretical premise upon which the study was able to examine the inconsistencies in the consumers' online personal information disclosure habits from the cognitive predisposition prism. This study also chose to examine the information privacy paradox with the privacy regulation theoretical framework because of the theory's fundamental principles described above and presented in detail in Table 4. The theory delineated how individuals deal with others, especially when they are receptive to communicating with them and when they are not. It also illustrated what happens when individuals are not fully in control of when and how to communicate with others. The underlying principles inherent in the theory are the dynamic opposition, the multimodal realism in application, and its optimizable capacity. Therefore, the study maintained that the use of the privacy regulation theory in explaining the phenomenon of the selective personal information disclosure online or the consumer privacy paradox was better. For example, a consumer may need to place an order for a textbook online at a lower price and yet worry about disclosing his or her personal information on an organization's Website at the same time. The underlying principles in PRT predicates on an individual's self-definition, which depends largely on the person's ability to regulate contact as desired (Altman, 1975). Furthermore, although there are divergent mechanisms available to individuals to regulate their contact with others, i.e., verbal or nonverbal communication, cultural or environmental practice, information permeability still occurs.

Finally, to demonstrate due diligence, this study considered the conceptual principles inherent in the *Self-Disclosure Theory* (Cozby, 1973; Derlaga & Berg, 1987; Joinson, 2001; Laurenceau et al., 1998) and in the *Expectations-Confirmation Theory* (Oliver, 1977; Oliver, 1980; Spreng et al. 1996) as well, in order to ensure that there is realism in the chosen theoretical concept.

3.2.3 Self-disclosure theory.

Joinson (2001) described self-disclosure as the “act of revealing personal information to others” (p. 178). The self-disclosure theory deals with the conscious or unconscious act of revealing more about oneself to others through one’s thoughts, feelings, aspirations, goals, failures, successes, fears, or dreams (Derlaga & Berg, 1987). Relative to information systems, Joinson (2001) noted that individuals tend to reveal more about themselves online, which could be a result of the pseudonymous illusion of information privacy and the intermediation of the Internet screens. The theory considers the basic parameters of disclosure: the breadth, the depth, and the time an individual spends detailing his information, and deals with the information disclosure reciprocity as well, based on trust (Cozby, 1973; Derlaga & Berg, 1987). Information privacy disclosure reciprocity refers to our eagerness and capacity to disclose information about ourselves to others largely on our perception and belief that others would share their own personal information with us as well.

This study chose not to use the self-disclosure theory because the theory assumes that the e-commerce information sharing may be a reciprocal in the information privacy context. In addition, a review of literature had demonstrated a lack of reciprocity in an online personal information collection and use (Culnan & Williams, 2009; Hong & Thong, 2013). Practically, online merchants or organizations vie for the consumers' personal information today more than ever, but they rarely provide consumers with comparable information relating to their lucrative personal information management strategy: collection, use, and storage (Dinev et al., 2013). Therefore, the study assessed that the theoretical examination of the phenomenon based on the self-disclosure theory was insufficient.

3.2.4 Expectation confirmation theory.

The expectation confirmation theory (ECT) posits that expectations, coupled with perceived performance, leads to post-purchase satisfaction (Oliver, 1977; Oliver, 1980). The theory has three main core principles, namely expectations, disconfirmation, and satisfaction. Expectation deals with a consumer's expected quality of a product or service prior to the purchase, which is evaluated only after a purchase has occurred based on the consumer's receipt of a positive or a negative disconfirmation. Oliver (1980) described consumer satisfaction as "a function of the expectation (adaptation) level and perceptions of disconfirmation" (p. 461).

Therefore, the motivation for the theory is on perceived expectation and post-purchase assessment, whereas the motivation for the phenomenon being examined was on the consumers' pre- and actual purchase behaviors online. Consumers' intended personal information disclosure decisions occur prior to an online purchase, and actual personal information disclosures occur during the purchases. Therefore, the study assessed that a theoretical examination of the phenomenon based on the expectation confirmation theory was not suitable.

Table 4. Theoretical Concepts and Information Privacy Constructs

PRT Concepts	Description of PRT Concept	Information Privacy Construct	Description of Information Privacy Construct	Reference
Access to the Self	Privacy involves the interaction between one individual and another, individual and group, or between groups. In any of these relationships, our reason for engaging or disengaging in a social unit depends on a need to satisfy any or a combination of the four natural states of privacy: intimacy, anonymity, reserve, or solitude.	Desired State of Privacy	Consumer's e-commerce personal information disclosure depends on the person's desired state of privacy: solitude (isolation of oneself), anonymity (concealing one's identity), reserve (very cautious and selective), or intimacy (eager to engage). The desire state is a natural state, and not a sought-after state.	(Altman, 1975; Westin, 1970)
Dynamic Dialectic Process	Dynamic dialectic process explains the continuing interchangeable opposing forces that urge people to want to be alone (out of contact) sometimes and want to be in contact (the need to hear, listen, talk, or be heard) at other times. The *net strength* is the *delta* between opposing forces; the need to be *open and accessible* and the need to be *close and inaccessible* changes over time.	Information Privacy Self-Interest	Information privacy self-interest is the need to be in contact—transact online or the need to be out of contact at a particular time and in a given situation or circumstance.	(Altman, 1975)
Multimodal or Multi-Mechanism Process	Multimodal or multi-mechanism process is a tactic through which individuals or groups achieve a variable level of privacy. It is a relational process through which a person or group of persons regulates access (openness and closeness) of the self to others with changes in circumstances.	Information privacy Permeability	Information privacy permeability refer to the fact that consumers do not always have total control of their information privacy boundaries; i.e., even if one is an information fundamentalist, pragmatist, or unconcerned, which means that mediating needs or conditions could cause changes to one's intended and actual personal information disclosure behavior.	(Altman, 1975; Westin, 1970)
Optimization Process	Optimization process is the notion of attaining an effective level of privacy, in which too much privacy is equally unsatisfactory as too little privacy. The goal is to achieve a state of balance in interaction, and privacy equilibrium, where a person desires neither more contact nor less contact.	Information Privacy Equipoise	Information privacy equipoise is the compromised or operative level of privacy at a given time and in a given circumstance. When the desired level of information privacy is high, people would feel violated, vulnerable, or overwhelmed if they receive more privacy. Conversely, when the desired level is low, they would feel isolated, insulated, or secluded if they receive less privacy.	(Altman, 1975)

3.2.5 Development of information privacy constructs.

The constructs in this study were developed based on the principles inherent in the privacy regulation theory. The concepts are access to the self, dynamic dialectic process, multimodal process, and optimization process and were translated into information privacy constructs of the desired state of privacy, information privacy self-interest, information privacy permeability, and information privacy equipoise respectively, as presented in Table 4. The essence of aligning PRT theory to the aforementioned constructs in this manner was to provide a cohesive and logical theoretical basis for this empirical study.

3.3 Theoretical Model

The information privacy disclosure behavior model developed in this study was based on the privacy regulation theoretical framework depicted in Table 4. A theoretical framework must be translatable, observable, and empirically testable in order to evoke trust and confidence in the research community (Lynham, 2002).

The hypothesized model was presented in Figure 3 and it shows that there is a relationship between a consumer's desired state of information privacy and the consumers' information privacy equipoise. The model also shows that the consumers' information privacy self-interest and the information privacy permeability have moderating effects on the positive relationship between the desired state of information privacy and the consumers' information privacy equipoise. Finally, the model shows that the information privacy equipoise, which is an intervening construct or variable, has a positive relationship with the consumers' selective personal information disclosure behaviors.

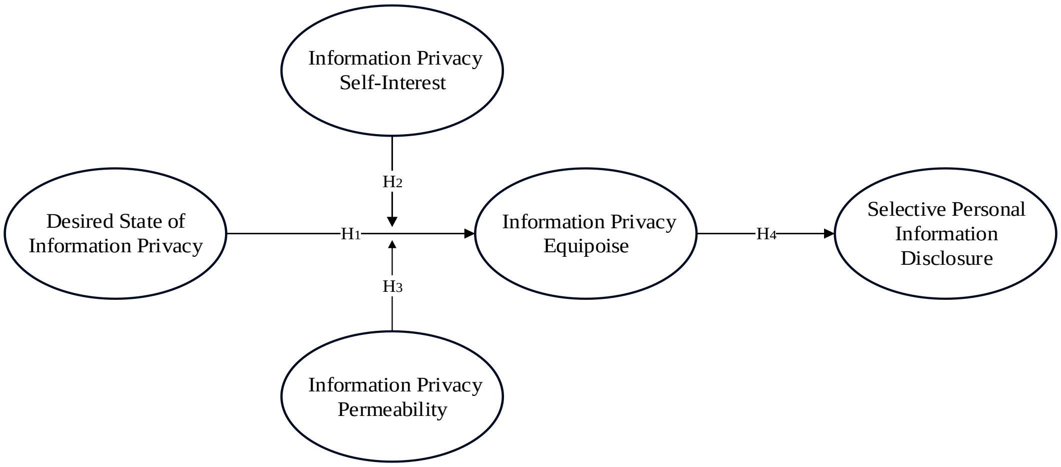

Information Privacy Self-Interest
H2
Desired State of Information Privacy
H1
Information Privacy Equipoise
H4
Selective Personal Information Disclosure
H3
Information Privacy Permeability

Figure 3. Selective Information Privacy Disclosure Theoretical Model

Following the definitions of the constructs below are details and contextual descriptions of each construct, which are the desired state of information privacy, the information privacy self-interest, the information privacy permeability, and the information privacy equipoise.

- The desired state of information privacy is a consumer’s online natural information privacy disclosure mindset and/or posture, i.e., a state of mind, in information privacy context, in which a consumer is usually comfortable or at ease with himself or herself. It is also a state of mind, in information privacy context, in which a consumer has a sense that he or she has reasonable control of his or her personal information. The four natural states of privacy, according to Westin (1970), are solitude (being very reluctant to engage in online transactions), reserve (willing to engage in an online transaction when it is practical), intimacy (always willing to transact online), anonymity (transacts online with pseudo identity).
- Information privacy self-interest is a consumer’s internal or external *need signal* to obtain an item or service online. The study defines need signal as a consumer’s cognition and gesture, action, or sound that something is required, useful, or desired

because it is crucial.

- Information privacy permeability is the collection of additional information from customers by an online merchant during a transaction with or without the consumers' knowledge. An online merchant could collect personal information from a consumer in two ways, (1) force the disclosure of the information as a condition for the completion of a transaction and/or (2) use technology to collection the information unbeknown to the consumer.
- Information privacy equipoise is the compromise one is willing to make to one's desired state of information privacy in order to transact online and disclose one's personal information. It is a state of mind in which an internal or external pressure forces a consumer to violate his or her desired state of information privacy in order to transact online and disclose his or her personal information.
- Selective personal information disclosure is the act of disclosing personal information in one online transaction setting and not disclosing it in another, regardless of whether the circumstances are the same or not.

3.3.1 Desired state of information privacy.

The original state of privacy was articulated based on general privacy; however, it is applicable and relevant to information privacy today. This study describes the desired state of information privacy as the *natural state* at which a consumer is naturally at ease with himself or herself, i.e., a state at which a consumer has a sense that he or she has reasonable control of his or her personal information. This study agrees with Smith et al. (2011) that "when privacy is viewed as a state…there must be a continuum of the states of privacy, from absolute to minimal" (p. 995). This view was articulated in Westin

(1970), where the fundamentalist was viewed as the absolute state and the unconcerned as the minimal. However, the study argues that there is a natural or desired state and a compromised or an operative state within the continuum. Therefore, an individual is considered to be at the natural or desired state when information privacy is not being sought-after or when other factors that could influence the desired state are constant, and at the compromised state when the sought-after goal is achieved. This means that at the desired or natural state of privacy, other factors, such as information privacy self-interest and permeability are presumed to be constant; whereas the factors are presumed to be at work when the individual is in a quest for an effective or operative level of information privacy. In addition, at a desired state, an individual may still need more privacy or less privacy, but at an equipoise state, neither more nor less privacy is tolerable. Therefore, in this study, an information privacy equipoise is a point at which more or less information privacy is unacceptable.

The following is an illustration of the desired state of information privacy situation. Imagine being asked by an acquaintance or a researcher to identify the types or the amount of information you would be willing to disclosure online. You may promise to disclose your personal information online at that point because you are aware that the questions are gaging your intent and that whatever answers you provide would be for a hypothetical exercise. In addition, you are aware that neither your personal information nor your financial is at stake at that point, that you have minimal or no risk estimates, and that there is no personal information disclosure need at work. Hence, you would naturally respond to the questionnaire with minimal pressure. On the contrary, your actual response may differ when you are actually transacting online because the disclosure would be real and may be consequential. Thus, the belief was that a consumer's intention to disclose personal information online depends on the person's natural or desired state of information privacy. The states of privacy used in this study are the solitude, anonymity, reserve, and intimacy (Westin, 1970). In the study, the solitude refers to removing oneself from ecommerce or from transacting online, the anonymity refers to concealing one's identity while transacting online, the reserve refers to being very cautious or pragmatic about personal information disclose during an online transaction, and the intimacy refers to embracing ecommerce and having limited or no concern for personal information disclosure while transacting online.

The postulation was that a consumer's natural or desired state of information privacy would influence his or her information privacy equipoise (operative level of information privacy). Therefore, the following hypothesis was posited:

H_1: A consumer's desired state of information privacy has a causal relationship with the consumer's information privacy equipoise.

3.3.2 Information privacy self-interest.

Dinev and Hart (2006) described interest as an "intrinsic motivation, a cognitive state or belief related to the self-fulfilling satisfaction derived from performing the activity" (p. 67). To gain a better understanding of the power of self-interest, the study explored the philosophical meaning of egoism. Moseley (2005) described egoism as "the theory that one's self is, or should be, the motivation and the goal of one's own action" (p. 1), and argued that individuals are motivated to act based on personal interest and desire, from descriptive or positive perspective. Hence, this study argues that a consumer's information privacy self-interest would affect the consumer's information privacy equipoise. Assessment of the information privacy paradox based on the PRT principles supported the argument that a consumer’s willingness to disclose his or her personal information in an e-commerce environment would be based on the individual’s information privacy self-interest. Therefore, the potency of the argument that an individual’s self-interest would affect the person’s information privacy equipoise is practical.

Furthermore, a consumer’s self-interest varies (Bellia, 2009) and could determine whether the individual wants to be in contact or out of contact, or whether the individual wants to transact online or not, from information privacy perspective. Extrapolating, Bellia (2009) suggested that an individual could have variable interests and commitments in an online personal information disclosure based on the type and nature of the online transaction. For instance, a person may have a need to purchase goods or services online and may be wary of the information being required by the online merchants at the same time. Equally, a person may have a need to purchase a medical service online or set up an appointment, yet worried about sharing some of his or her required medical history. Better yet, a person may be interested in participating in targeted advertising online, and still struggle with the idea of sharing his or her personal information online.

The notion is that an information privacy isolationist or an information privacy fundamentalist may still have a need to acquire materials from an online merchant. The need, therefore, would temporarily alter the person’s information privacy desired state, alter the degree of his or her information privacy permeability, or his or her information privacy expectation. Hence, such alterations would bring the individual to the information privacy equipoise. The implication of the aforementioned supposition is that a consumer’s decision to disclose his or her personal information online would be a function of a desire to satisfy a need, which would subdue or minimize the consumer’s concerns for information privacy and allow the consumer to reach the information privacy equipoise at a given time and in a given circumstance.

A consumer’s self-interest is a temporary condition, which may be triggered by internal or external events or pressures, or for a purpose. Besides, a consumer’s need is dynamic because it changes over time. It may cause a unit of change in a consumer’s information privacy posture, which allows the individual to satisfy his or her interest. Based on the above discussions, the study posited that a consumer’s self-interests would affect the person’s information privacy equipoise. Thus, the following hypothesis was postulated:

> **H_2**: A consumer’s information privacy self-interest moderates the relationship between the consumer’s desired state of information privacy and his or her information privacy equipoise.

3.3.3 Information privacy permeability.

Information privacy permeability is the information privacy seepages that occur despite the dialectic mechanism. Dialectic mechanism is a tactic through which individuals or groups achieve variable levels of information privacy (Altman, 1975). It is a relational process through which a person or group of persons regulates access (openness and closeness) of the self to others, with changes in circumstances. In an information privacy context, a consumer may still disclose his or her personal information in an e-commerce environment unknowingly even when the disclosure is against his or her desired state of information privacy or his or her self-interest. The postulation was that the degree with which information privacy permeates online affects information privacy equipoise.

The assumption was that it is not practical for consumers to have total control of their information privacy boundaries. Using the analogues of a social gathering event, empirical (Altman, 1975) and anecdotal evidences show that at some point during an event, one may want to be in contact with others, as well as want to be out-of-contact at other times. Yet, one's ability to stay in or out of contact depends not only on one's desires, but also on other actors. For example, assuming that a person does not want to be in contact in such a setting, he may ignore others, frown at people, or turn his back as others approach; however, his ability to maintain an out-of-contact posture depends largely on others as well, because other people may force their way into him. In an information privacy context, a consumer may not have the desire to transact online, yet participates in e-commerce due to a merchant's advertisement, mouth-to-mouth advertising from peers, or due to other external influencers. In addition, Petronio (2012) suggested that the "rules that control permeability are manifested in the depth, breadth, and amount of private information that is revealed" (p. 99). Hence, the following hypothesis was posited.

H_3: A consumer's information privacy permeability moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.

3.3.4 Information privacy equipoise.

Table 5 is an illustration of the *Information Privacy Equipoise* scheme developed in this study based on Altman (1975) privacy regulation principle and Westin (1970) classification of privacy. The position was that the variation in a consumer’s intended and actual personal information disclosure behavior online was a result of the changes in the consumer’s information privacy equipoise. Information privacy equipoise is a consumer’s operative or compromised level of information privacy at a given time and in a given circumstance. It is a point at which a consumer’s level of information privacy is at equilibrium. In other words, information privacy equipoise is a point at which there is a *cognitive symmetry* or *cognitive balance* between a consumer’s information privacy risk concerns, including the information privacy permeability, and the consumer’s desired state of information privacy and information privacy self-interest. Therefore, when a consumer achieves information privacy equipoise, he or she would need neither more nor less information privacy.

Table 5. Information Privacy Equipoise

Desired State of Privacy	**Privacy Self-Interest**	**Privacy Permeability**	**Information Privacy Equipoise**	
			Yes	**No**
Intimacy	High (open)	High	X	
	High (open)	Low	X	
	Low (close)	High	X	
	Low (close)	Low	X	
Anonymity	High (open)	High	X	
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low		X
Reserve	High (open)	High		X
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low	X	
Solitude	High (open)	High		X
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low		X

Cognition is a “process by which the system [or a consumer in information privacy context] achieves robust adaptive, anticipatory, autonomous behavior, entailing embodied perception and action” (Vernon et al., 2007, p. 151), and is individually constructed or structured (Tan & Hunter, 2002). Drawing from psychoanalysis, Takahashi et al. (2010) noted that symmetry “is one of the principles of the unconscious thinking” (p. 16). Therefore, this study surmises (see Table 5) that cognitive symmetry in information privacy or information privacy equipoise is achieved when a consumer, who is in intimacy state of information privacy, has high or low unfulfilled need signal, and has high or low information privacy permeability. Secondly, cognitive symmetry is achieved when a consumer, who is in anonymity state has high unfulfilled need signal, and has high or low information privacy permeability. Thirdly, cognitive symmetry is achieved when a consumer, who is in reserve state of information privacy, has high or low unfulfilled need signal, and has low information privacy permeability. Finally, cognitive symmetry is achieved when a consumer, who is in solitude state of information privacy, has high unfulfilled need signal, and has low information privacy permeability.

Therefore, a consumer *X* would achieve information privacy equipoise if he or she is in the intimacy or anonymity desired state of privacy, has high privacy self-interest (wants to be in contact), and is in a high or a low information privacy permeability situation. In contrast, while a consumer in intimacy state would be at equipoise whether or not his or her privacy self-interest or permeability is high or low, those at the anonymity state could feel violated, vulnerable, or overwhelmed if they have low or close privacy self-interest and low or high privacy permeability. Similarly, a consumer *Y* would achieve information privacy equipoise if he or she is in the reserve or solitude state of information privacy, has high or open information privacy self-interest and in a low privacy permeability situation. In contrast, the consumer would feel violated, vulnerable, or overwhelmed if he or she is in the reserve or solitude state of information privacy, has low or close information privacy self-interest and is in a high information privacy permeability situation.

To illustrate this point further, imagine that Elvis and MaryJane are student participants in an undergraduate and graduate mixer. While Elvis, an unconcerned or a pragmatist wants to talk to as many students as possible, MaryJane, a fundamentalist or a pragmatist does not. In this context, Elvis would achieve information privacy equipoise if other students are available for discussions as well, and he would not care if the content of the discussions were to be disclosed to others. Nonetheless, he would feel isolated, secluded, or insulated if other students were not available for discussions. On the other hand, MaryJane would achieve information privacy equipoise if other students were not available for discussions and would not want her discussion disclosed to others. She would feel violated, vulnerable, or overwhelmed, if other students are available, needing discussions, and would disclose their discussions.

The review of literature has shown that the previous examinations of the information privacy paradox have been from the value or economic perspective primarily. In an experimental study, based on the social cognitive theory, involving 126 participants, Doohwang and LaRose (2011) argued that the consumers' willingness to disclose personal information online is a function of the cognitive evaluation of the expected risk-benefit analysis. Additionally, in a hypothesis testing study involving 369 respondents, Dinev and Hart (2006) examined the effect of the contrary beliefs on a consumer's personal information disclosure online. The paper evaluated risk beliefs (internet privacy risk and concerns) and confidence and enticement beliefs (internet trust and personal interest), and argued that a consumer's personal information disclosure is based on the net expected outcome between the two. Furthermore, Dinev and Hart (2006) found that the confidence and enticement beliefs always tend to outweigh the risk beliefs in ecommerce, which may explain why ecommerce activities thrive, despite increased risk beliefs among the consumers. However, this study posited that the risk and enticement beliefs are not enough to explain the phenomenon of the information privacy paradox. Therefore, on the belief that a consumer's online personal information disclosure intentions occur at a natural state and the person's actual disclosures occur at the compromised or operative state, this study postulated as follows:

H_4: A consumer's information privacy equipoise is positively related to the consumer's selective personal information disclosure behaviors online.

3.3.5 Summary.

In this section, a distinction between the desired state of information privacy and the compromised state, otherwise called the information privacy equipoise was made in order to eliminate the ambiguity between the two, and to meet the internal validity objectives of the study. In addition, the study provided the detail information on each construct and the position taken by the study, which triggered each hypothesis. Therefore, Table 6 is the summary of the hypotheses in this study.

Table 6. Summary of the Research Hypotheses

	Hypothesis	Construct
H_1	A consumer's desired state of information privacy has a causal relationship with the consumer's information privacy equipoise.	Desired State of Information Privacy
H_2	A consumer's information privacy self-interest moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.	Information Privacy Self-Interest
H_3	A consumer's information privacy permeability moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.	Information Privacy Permeability
H_4	A consumer's information privacy equipoise is positively related to the consumer's selective personal information disclosure behaviors online.	Information Privacy Equipoise

3.4 Research Design

A cross-sectional survey research method was conducted for this study. A survey research is a type of research in which a structured or predefined written or oral questionnaire serves as the primary data collection instrument for a quantitative analysis from a given sample of a given population (Pinsonneault & Kraemer, 1993; Salkind, 2012). A cross-sectional method refers to a one-time data collection in response to answering a research question or solving a research problem (Salkind, 2012; Sekaran & Bougie, 2009; Vogt, 2005).

The study took the quantitative analysis approach. The quantitative analysis approach was necessary for this study because the study was predictive in nature and it evaluated the relationships among the constructs and the phenomenon. The additional import of the use of the quantitative analysis was that its allowance for behavior and attitude exploration (Dinev et al., 2013).

The use of the survey research approach by researchers in information privacy discipline is prevalent in the literature today (Dinev et al., 2013; Hong & Thong, 2013;

John et al., 2011). Considerations were also given to the issues relating to the population, sampling, questions, content, biases, and administration. According to Trochim (2000), population issues refer to matters relating to population enumeration, literacy, cooperation, geography and language. The paper saw sampling issues as those relating to data availability and sampling rate. The paper also saw question issues as those relating to whether there is a need for the screening of the questions and matters relating to item scaling and sequencing. In addition, the author suggested that the content deals with matters of whether respondents are familiar with the issue being examined. Finally, Trochim referred to biases as those issues relating to a researcher's prejudices, and administrative issues as those relating to cost, facility, time, and the like.

The unit of analysis for this study was individual (consumer). The unit of analysis is the entity, person, or thing being analyzed (Trochim, 2002; Vogt, 2005). The decision to examine the individual in this study was because the purpose of the study was to predict the factors, which contribute to the gap between an individual's intended and actual personal information disclosure behavior online.

3.5 Instrument Development and Validation

Many of the items or manifest variables used for this study, shown in Appendix A, were from the extant literature, although some were modified pertinently for appropriateness in the context. Adaption and/or modification of the observed variables adapted from the extant literature to suit the context of this study is consistent with many studies in the information privacy discipline (Culnan & Armstrong, 1999; D'Arcy et al., 2009; Dinev & Hart, 2006; Smith et al., 2011). Other items were developed by the study because there was no existing indicator variables or items or scale in the literature, that could be found, to examine some of the constructs. According to Lewis-Beck et al. (2004), a scale is “composed of a set of measurable items that empirically captures the essential meaning of the theoretical construct” (p. 998). Development of new items or scales based on the theoretical definitions, where none exists, is consistent with the extant literature (Dinev & Hart, 2006).

An interval scale was used for the study. The study used a seven-point Likert (Northouse, 2013) interval scale to capture the extent of respondents’ agreement to the questionnaire and employed multi-item indicators for the operationalization of the constructs. The use of a five-, seven-, or 11-point Likert scale is supported in the information privacy literature (Bansal et al., 2010; D’Arcy et al., 2009; Dinev & Hart, 2006). In a stratified survey research, which involved 735 participants (300 five-point, 250 seven-point, and 185 10-point), Dawes (2008) found that a five- and a seven-point interval scale had produced the same mean score, whereas the 10-point scale produced slightly lower mean score relatively. However, in a usability testing study, involving 172 Intel employees from 10 countries, Findstad (2010) suggested that a seven-point Likert item is better than a five-point if a researcher were to avoid response interpolation, especially for an electronically distributed and unsupervised survey. Interpolation refers to a participant’s inability to correctly choose a response between two discrete values, i.e., unable to choose a 3.5 value if the values are 3 and 4 (Findstad (2010).

An interval scale has three important properties, namely, “classification, logical order, and equal interval” (Newton & Rudestam, 1999, p. 180). Therefore, the main reason for using an interval scale was because it “groups individuals according to certain categories and taps the order of these groups…it also measures the magnitude of differences in the preferences among the individuals" (Sekaran & Bougie, 2009, p. 143). A *never* to an *always* response provided the classification or categorization property. In addition, an assignment of numbers 1-7 from a *never* to an *always* respectively provided the logical order and allowed for a quantitative calculation. Finally, the measures of the magnitude of differences were indicated with arithmetic mean and standard deviation. The study used multi-item indicators. The use of the multi-item indicators was necessary because they were suitable in measuring complex concepts and they allowed for the operationalization of a multidimensional phenomenon (Maxim, 1999).

3.5.1 The measure of the desired state of information privacy.

As a natural state at which a consumer is indeed at ease with him or herself and one in which information privacy is not sought after, the desired state of information privacy construct was examined using the scale adapted from Harris Interactive and Westin (2002), and Kumaraguru and Cranor (2005). The study aligned the four states of information privacy, solitude, reserve, intimacy, and anonymity (Westin, 1970), with the *Core Privacy Orientation Index* (Kumaraguru & Cranor, 2005), the privacy fundamentalists, pragmatists, and the unconcerned. The state of privacy has four components, whereas the index has three components, hence, it is importation to note that the additional state of anonymity has shown to have cut across the other three states of solitude, reserve, and intimacy (Bella et al., 2011; Joinson, 2001). The core privacy orientation index was originally proposed as the *General Privacy Concern Index* in Kumaraguru and Cranor (2005), involving 1255 survey elements. However, the paper did not account for the information privacy anonymity state in neither the core privacy orientation nor the privacy index. Therefore, the study added an additional indicator variable in measuring the desired state of information privacy, in order to account for the information privacy anonymity as one of the desired states.

In a field study in 2001, which involved 1529 sample subjects, Alan Westin and Harris Interactive classified the public into three categories. The first was the privacy fundamentalists, who were about 25% of the public; the second was the privacy pragmatists, who were about 55%; and the third was the privacy unconcerned, who were about 20%. To measure the consumers' desired state of information privacy, the study asked the survey participants to agree or disagree with the three statements used to categorize the public in the core privacy orientation index. In addition, a new statement was developed and added by the study in order to identify respondents, within the three classifications of the desired state information privacy, who have the anonymity state tendencies as well.

3.5.2 The measure of information privacy self-interests.

A consumer's information privacy self-interest is one in which an intrinsic or extrinsic motivator or need would trigger a change in the consumer or on the individual's information privacy posture, which then allows the person to transact online and disclose his or her personal information as a consequence. With the ubiquitous nature of the Internet capable devices, otherwise called the Internet of things, individuals have needs to purchase goods or services online from time to time, i.e., need to purchase books or items, apply for government services, renew registrations and licenses, register, receive, and update medical or dental information online, and the like.

Interest is described in Dinev and Hart (2006) as the "an intrinsic motivation, a cognitive state or belief related to the self-fulfilling satisfaction derived from performing the activity" (p. 67). Furthermore, personal interest, which is referred as self-interest in this study, was described in the paper as "a belief that reflects a level of enticement to transact" (p. 67). Therefore, the study adapted Dinev and Hart (2006) indicators for measuring the individual's Internet-interest as a good measure for the information privacy self-interest with some modifications for appropriateness in the context.

Scenario: I am an information fundamentalist and my natural state of information privacy is solitude, which means that I am one of those people who hate to transact online in order not to disclose my personal information. However, I am in need of a book, like yesterday, and my local bookstore does not carry the book or would not be able to provide the book to me in a timely manner if I order it from them. In addition, I learned that the nearest store that carries the book is about 75 miles away and I have no intention of driving that far for the book, especially when I know that I can get the book from an online merchant overnight.

Possible Outcomes: I have three courses of action in this case, (1) do not buy the book and bear the consequences, (2) travel 75 miles and back and buy the book, or (3) buy the book online. My information privacy posture will remain intact if I were to travel 75 miles to get the book, or decide not to buy the book at all and bear the consequences. However, there would be a change to my information privacy posture if I decide to buy the book online. The supposition is that my interest would have altered my natural information privacy (desired state) posture toward the compromised or the operative posture (equipoise) if I were to buy the book online.

3.5.3 The measure of information privacy permeability.

In this study, information privacy permeability was defined as a consumer's personal information collected during an online transaction unbeknown to the consumer and those known to the consumer, but collected because an online merchant designated them as required even though they were not critical to the completion of the transaction. Information privacy permeability may also be defined as the collection of additional information from a customer by an online merchant during a transaction with or without his or her knowledge. For example, a consumer may be forced to provide additional information, which may not be necessary for the transaction, but must be provided in order to complete the transaction. Likewise, an organization may use technology to collect additional information from a consumer during a transaction without the person's knowledge, i.e., the network IP addresses, previously visited sites, consumer's purchasing patterns, and the like. Information privacy permeation was classified into two in this study; permeation from a primary source and permeation from a secondary source.

The classification reflected the dimensions of information privacy concern presented in Smith et al. (1996). The online merchants collect consumers' personal information during the transactions, and the information may further be collected or shared internally or externally by either authorized or unauthorized secondary users. Therefore, permeation from the primary source refers to personal information collected during an online transaction, involving the gathering of a consumer's personal or private information. Permeation from the secondary source refers to any personal or private information collection that occurs after the initial collection online (Smith et al., 1996; Xu et al., 2012). Therefore, the study adapted some of the manifest variables from Smith et al. (1996) and modified them for suitability because only the permeation from primary source was relevant to this study.

3.5.4 The measure of information privacy equipoise.

Information privacy equipoise, as described earlier, is the consumer’s compromised state or the operative level of information privacy at a given time and in a given circumstance or situation. A consumer reaches the operative level of information privacy when he or she no longer needs more or less information privacy. Consumers will no longer need more or less information privacy when their desired or usual or natural state of information privacy, self-interest, and permeability at a given time and in a given circumstance or situation are in harmony with their sought-after information privacy posture, information privacy equipoise, as presented in Table 5. In other words, information privacy equipoise is a state of mind, from information privacy perspective, in which an individual moderates his or her concern or worry, in time and circumstance, about the risks and the vulnerabilities of transacting online because of his or her (1) need to purchase something online and (2) despite the awareness of the collection of his or her personal information by an online merchant.

The conceptual assumption is that a consumer’s decision to disclose his or her personal information online is based on his or her achievement of the information privacy equipoise. This means that the individual would have shifted from his or her desired or usual or natural state of information privacy posture to a sought-after or compromised state, which would have been moderated by the individual’s self-interest at the time, and the degree of information privacy permeation. Since a consumer’s information privacy equipoise is in a continuum and occurs intermittently, this study argued that a consumer’s information privacy equipoise at a time and in a given circumstance would prompt discriminative behavior in a consumer’s actual personal information disclosure, regardless of the person's previously declared or undeclared intended behavior.

An instance of information privacy activity online is referred to in this study as a unit of privacy, which is a function of a consumer's information privacy equipoise and the communicative act. In a psychological review, Newcomb (1953) noted, "Every communicative act is viewed as a transmission of [personal] information, consisting of discriminative stimuli" (p. 393). In the context, the stimuli were (1) disclose personal information online, (2) do not disclose, (3) disclose with pseudo identity, and (4) disclose only when it is rational. Going by this definition, the study argued that information privacy paradox is inherent in the consumers' online personal information disclosure behaviors. This view was supported in Miller (1951, p. 41), who stated, "A discriminative stimulus is a stimulus that is arbitrarily, symbolically, associated with some thing (or state, or event, or property) and that enables the stimulated organism to discriminate this thing from other things."

The notion of information privacy equipoise was not in existence in the information privacy discipline based on the extensive literature review conducted for this study. Therefore, adapting existing indicators for the construct was impractical. To overcome this difficulty, a review of the literature on clinical equipoise was undertaken since extensive work, in this regard, exists. Clinical equipoise lends itself to randomization or neutrality of choice based on reason. The randomization anchors in treatment effectiveness and patient's safety rather than in favoring one treatment over the other (Ashcroft, 1999, Freedman, 1987). Hence, Ashcroft (1999) stated, "Clinical equipoise is not simply preference neutrality" (p. 316), but a "state in which the physician has no reason to choose one treatment over the other" (p. 317). Therefore, in the information privacy context, a consumer who had achieved information privacy equipoise, would have no reason for more or less information privacy, as such would disclose personal information online.

3.5.5 Adaptation and development of measurement scale.

Table 7 is a depiction of the listing of the initial items adapted and developed for this study, although some were later modified or removed for suitability. The table also contains the constructs and the seven-point interval scale adapted from Northouse (2013). Moreover, in the reference column, a *yes* remark is indicative of an adapted item for the study, whereas the new items developed for the study are marked as *new* in the reference column as well.

Table 7. Measurement Scale

Construct		Items	Adapted?	Reference
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always				
Desired State of Information Privacy (DSIP)	DSIP1	Usually, I believe that consumers have lost control over how their personal information is collected and used by organizations.	Yes	(Kumaraguru & Cranor, 2005)
	DSIP2	Usually, I believe that most businesses handle the personal information they collect about consumers in a proper and confidential way.	Yes	(Kumaraguru & Cranor, 2005)
	DSIP3	Usually, I believe that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	Yes	(Kumaraguru & Cranor, 2005)
	DSIP4	Usually, I believe in concealing my personal information, to the maximum extent possible, when transacting online.	No	New
Information Privacy Self-Interest (IPSI)	IPSI1	I find that my interest in the goods or services that I want to obtain overrides my concerns for possible risks or vulnerabilities that I may have regarding the disclosure of my personal information online.	Yes	(Dinev & Hart, 2006)

Table 7. Measurement Scale (continued)

Construct	Items		Adapted?	Reference
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always				
	IPSI2	The greater my interest to purchase a certain good or service, the more I tend to suppress the risks or vulnerabilities of disclosing my personal information online.	Yes	(Dinev & Hart, 2006)
	IPSI3	In general, my interest in the goods or services that I want to purchase online is greater than my concern about disclosing my personal information.	Yes	(Dinev & Hart, 2006)
Information Privacy Permeability (IPP)	IPP1	It bothers me when an organization insists on getting certain personal information, especially when I believe the information to be unnecessary, before allowing me to complete an online transaction or purchase.	Yes	Smith et al. (1996)
	IPP2	I usually think twice before providing certain personal information online, whenever an organization asks for it, because I do not know who else will have asses to it and for what purpose.	Yes	Smith et al. (1996)
	IPP3	It bothers to know that organizations can collect my personal information, without my knowledge or approval, when I am transacting online.	No	New
	IPP4	It concerns me that organizations are using technology to collect my personal information, without my knowledge, whenever I am making an online transaction.	Yes	New
	IPP5	I am concerned that organizations are collecting too much personal information from consumers online whether they know it or not.	Yes	Smith et al. (1996)
Information Privacy Equipoise (IPE)	IPE1	I believe in sharing my personal information when purchasing an item or service online.	No	New
	IPE2	I believe in making an assessment of the information being requested before providing my personal information in an online transaction whenever an organization asks for it.	No	New
	IPE3	I believe that the use of a third-party payment service or method, such as Pay-Pal and other, to obtain goods or services online allows me to disclose my personal information online.	No	New
	IPE4	Although I dislike the idea of disclosing my personal information when transacting online, at times, I believe in disclosing my personal information in an online transaction without regard for any potential risk or vulnerability involved.	No	New
	IPE5	I believe in sharing my personal information when transacting online to obtain a particular good or service based on my need or interest at the time.	No	New

Table 7. Measurement Scale (continued)

Construct		Items	Adapted?	Reference
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always				
	IPE6	I believe that the need to obtain a certain good or service online diminishes my concern for personal information disclosure risks and vulnerabilities at the time.	No	New
	IPE7	I believe in disclosing my personal information online to obtain a good and service even when I think that an online merchant is using technology to collect additional formation from me at the time.	No	New
	IPE8	My concern of an organization collecting additional information from me when transaction online, knowing and unknowing, diminishes based on my belief that the organization's information privacy practices are in line with available laws and regulations at the time.	No	New
Selective Personal Information Disclosure (SPID)	SPID1	I have disclosed my personal information online during a purchase of goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information).	Yes	(Dinev & Hart, 2006)
	SPID2	I have disclosed my personal information online during a retrieval of information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates).	Yes	(Dinev & Hart, 2006)
	SPID3	I have disclosed my personal information online when I was conducting sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software).	Yes	(Dinev & Hart, 2006)
	SPID4	I have disclosed my personal information online during a retrieval of highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account).	Yes	(Dinev & Hart, 2006)
	SPID5	I have disclosed my personal information online when I am either registering, renewing, or updating highly personal and password-protected e-government information (e.g., using websites that allow me to access my voter registration, driver's license renewal, updating postal address, or the like).	No	New

3.6 Research Strategy

This study took a three-phase approach. The details of the three-phase approach or strategy for this empirical examination process are in the following sections. The phases consist of the data collection, the data analysis and interpretation, and the empirical validation. The use of this approach is consistence with the extant literature in the information privacy and information systems security studies (D'Arcy et al., 2009; Dinev & Hart, 2006; Norberg et al., 2007; Smith et al., 1996; Son & Kim, 2008).

3.7 Data Collection

The study undertook a three-phase approach for data collection as well. The data collection involved the data preparation and collection. In addition, the data collection was essential and fundamental in testing the hypotheses summarized in Table 6. The first phase involved the use of the *expert panel* (Lawshe, 1975), which involved the use of the substantive validity analysis and the content validity ratio (Anderson & Gerbing, 1991; Hinkin, 1998) to validate the survey instrument in order to ensure content validity. The second phase involved the piloting of the initial or preliminary study to assess the adequacy of the survey instrument and to refine the instrument, which was necessary and potent. Lastly, the third phase involved the actual data collection for the final analysis.

3.7.1 Phase 1.

The first phase of the data collection was from the expert panel. A team of professionals were used as the expert panel for this study. The use of a panel of expert judges to validate the observed variables or items is highly recommended in the information systems study because the positivist science still lacks a “clear consensus on the methods and means of determining content validity” (Straub et al., 2004, p. 387). The use of an expert panel is important in validating the survey instrument, especially for the newly developed or modified items in a study (Smith et al., 1996; Milne & Bahl, 2010).

The study received nine responses for the substantive validity analysis and 11 responses for the content validity ratio analysis even though it had sent the survey instrument to the same panel of 15 expert judges on both occasions during the first phase. The use of a small number of experts as judges is consistent with the extant literature in the information privacy and information systems security disciplines. In a 269-survey study on the users' awareness of security countermeasures, D'Arcy et al. (2009) used six professionals as an expert panel, and Smith et al. (1996) used three judges in streamlining 72 items designed to measure information privacy concern constructs. In comparing consumer and marketers' expectations for establishing and respecting privacy boundaries, Milne and Bahl (2010) used eight experts to validate the survey scenarios. In addition, the use of 12 to 30 participants has been deemed adequate as an expert panel (Anderson & Gerbing, 1991; Hunt et al., 1982).

The panel assessed whether the observed variables were appropriate and accurate in capturing the constructs or the latent variables based on the quantitative approach of the content validity ratio (CVR) espoused in Lawshe (1975). The quantification of the panelists' judgments was necessary in order to answer the question concerning the validity of the panel's judgment based on a quantifiable consensus. Lawshe (1975) evaluated expert panel consensus by asking the panelists to annotate whether each item in a questionnaire was *essential*, *useful but not essential*, or *not necessary*. This line of annotation criterion was replicated in this study.

The study used Lawshe (1975) one-tailed t-test and the CVR calculation for consensus analysis. The panelists were asked to assign numbers 3-1(*essential=3, useful but not essential=2, or not necessary=1*) to each item on the survey instrument based on their assessment of whether an item is a true representation of the content universe being measured. Equation 1 was used in calculating the CVR and the result was compared with the Lawshe (1975) one-tailed t-test table and the Wilson et al. (2012) two-tailed t-test table in Appendix C. The *first equation* was used to assess the ratio of the number of the experts who perceived an item as *essential* to the total number of experts. Here, the n_e is the number of experts with *essential* responses, and the *N* is the total number of experts (Lawshe, 1975; Wilson et al., 2012). Based on the aforementioned, the qualifying consensus and recommendations were followed (see the minimum values of content validity ratio tables in Appendix C):

> Any item, performance on which is perceived to be “essential” by more than half of the panelists, has some degree of content validity. The more panelists (beyond 50%) who perceive the item as “essential,” the greater the extent or degree of its content validity…when fewer than half say “essential,” the CVR is negative. When half say “essential” and half do not, the CVR is zero (Lawshe 1975, p. 567).

$$CVR = \frac{n_e - N/2}{N/2}. \tag{1}$$

Substantive validity analysis. The study used the substantive validity analysis to validate the observed variables and to validate the adequacy of the construct definitions (Anderson & Gerbing, 1991; Hinkin, 1998). The substantive validity analysis technique assesses two indices. One is the *proportion of substantive agreement*, which is “the proportion of respondents who assign an item to its intended construct” (Anderson & Gerbing, 1991, p. 734; Hinkin, 1998, p. 108). The proportion of substantive agreement is calculated by dividing the number of participants who correctly assign an item to its intended construct by the total number of participants. However, the shortcoming of this index is that it does not tell us the degree in which an item is reflected in other undesignated constructs, according to Anderson and Gerbing (1991). Hence, the second index, the *substantive validity coefficient* is preferred. The substantive validity coefficient is “the degree to which each rater assigned an item to its intended construct” more than other constructs (Hinkin, 1998, p. 108). To calculate the substantive validity coefficient, a researcher will subtract “the highest number of assignments of the item to any other construct in the set” (p. 734) from the number of participants who correctly assign an item to its intended construct, and divide the result by the total number of participants (Anderson & Gerbing, 1991).

The procedure for substantive validity analysis involves the provision of construct definitions, the provision of all items designated for validation in a randomized order without tying them to a particular construct, and asking participants to align the items to the constructs based on their understanding of the definition of the constructs. Since values for substantive-validity coefficient range from -1.0 to 1.0, larger values are indicative of a substantive validity. Secondly, a large, but negative number indicates substantive validity as well, but shows that the validity is for an unintended construct (Anderson & Gerbing, 1991). The underpinning in Anderson and Gerbing (1991) is that a revision of the item and/or the construct definition is warranted if an item fails to obtain sufficiently high substantive-validity coefficient.

3.7.2 Phase 2.

The second phase of data collection was with the pilot study. The review of the literature clearly recommended a pilot survey or pretest following items validation from the expert panel (Anderson & Gerbing, 1991; Hinkin, 1998; Milne & Bahl, 2010). The aim of the pilot study was to identify the issues and concerns relating to the sequencing of items, the method of administering the survey instrument (personal or phone interview, mail or email, and the like), the amount of time reasonable to complete the survey, and the issue of sample size (Anderson & Gerbing, 1991; Hunt et al., 1982). In addition, the pilot study was used to refine the measurement instruments (Boss et al., 2009).

The study used 55 participants for the pilot study. The use of this number of sample subjects is consistent with the extant literature. In a 269-survey study on users' awareness of security countermeasures, D'Arcy et al. (2009) used 54 computer-using professionals for the pilot test, and Norberg et al., (2007) used 43 graduate students for the pretest in examining the information privacy paradox. Furthermore, Smith et al. (1996) used 15 doctoral students and faculty members to refine the instrument in measuring information privacy concerns. Changes or modification were made to the survey instrument in this study as applicable post the pilot study.

The survey was administered to the participants via the email and the social network forum media. The sample subjects were given a week to respond to the survey. The study tallied and examined the participants' responses, and use them for the instrument refinement, the exploratory factor analysis (EFA), and the initial data analysis.

3.7.3 Phase 3.

The main data collection for this study took place in Phase 3. The study used the survey instrument developed in Phase 1, and refined in Phase 2 for the data collection. The study received 229 responses in this phase of the data collection, however, only 201 of them were valid. The sample subjects comprised of working professionals and respondents from the social network professional forums. According to Weston and Gore (2006), “there is no consensus [in sample size], except to suggest that missing or nonnormally distributed data require larger samples than do complete, normally distributed data” (p. 734). MacCallum et al. (1999) described the variation in the literature regarding the sample size calculation as the *N:p* ratio, where *N* is the minimum sample size and *p* is the number of the observed variables being analyzed. The paper stated that while some researchers believe that the ratio should range from 3:1 to 6:1, others argued that, at a minimum, the number of sample size ratio should be 5:1, 10:1, or 20:1. The ratio of the sample size to the number of items in this study was 12.6:1.

Meanwhile, while Gorsuch (1983) and Kline (1979) suggested that a receipt of 100 valid responses from the sample subjects is adequate for factor analysis, however, Cattell (1978) submitted that the minimum sample size should be 250 sample subjects or more. Furthermore, Comrey and Lee (1992) noted that a sample size of 200, 300, or 500 is fair, good, and very good respectively, as such adequate for factor analysis. For the structural equation modeling, a receipt of 200-400 valid responses is deemed adequate (Barrett, 2007), depending on the size, the characteristics, and the complexity of the model, including the desired statistical power and the null hypothesis being tested (Loehlin, 2004; MacCallum et al., 1999; Weston & Gore, 2006). The statistical power is the ability of a statistical test to detect the statistical significance relationships between variables or constructs, i.e., $(1 – \beta)$, where β (beta) is the probability of type II error—failure to reject null hypothesis when it is false (Park, 2008; Sekaran & Bougie, 2009). Vogt and Johnson (2016) recommended a minimal statistical power of 0.80 in a sample size selection in order to limit the probability of type II error to a maximum of 0.20.

The study used the sample subjects' responses for the hypothesis testing. The empirical test centered on evaluating the relationship between the desired state of information privacy and the phenomenon of the information privacy equipoise; the moderating effects of the information privacy self-interest and -permeability; and the mediating effect of the equipoise between the desired state and the selective personal information disclosure, as depicted in Figure 3. The states of information privacy were categorized and conceptualization based on the consumers' personal information disclosure behaviors in a cognate, coherent, and practical manner, based on the four states of privacy (Westin, 1970), and also based on the principles of the privacy regulation theory (Altman, 1975). The selective personal information disclosure behavior or the information privacy paradox is the inconsistency in the consumers' intended and actual personal information disclosure online.

3.8 Data Analysis and Interpretation

The study used the Structural Equation Modeling (SEM) and the Confirmatory Factor Analysis (CFA) for the data analysis and empirical validations. The structural package for social science (SPSS) and its specialized software, the analysis of moment structures (AMOS), were used for the SEM and CFA evaluations in this study because they are some of the most popular software used in the information privacy and in the information systems security studies (Bansal et al., 2010; Smith et al., 1996; Son & Kim, 2008).

The structural equation modeling is a "collection of statistical techniques that allow a set of relationships between one or more independent variables (IVs), either continuous or discrete, and one or more dependent variables (DVs), either continuous or discrete, to be examined" (Ullman & Bentler, 2001, p. 661). According to Albright and Park (2009), the SEM is a set of dependence relationships that link the hypothesized modelled constructs, and is used to answer the question of whether the estimated population covariance of a model is consistent with the sample or the observed variables' covariance matrix.

The structural equation modeling has two components, the measurement and the structural models (Albright & Park, 2009; Maxim, 1999). The measurement model links the manifest (observed) variables or items to the latent (unobserved) variable and the structural model assesses the latent variables' covariance via a series of recursive and non-recursive associations. Therefore, the study used the SEM because it allowed it to test the observed item linkages (see Appendix A) to the constructs and assess the covariance of the constructs depicted in Figure 3.

The CFA is "theory- or hypothesis driven" (Albright & Park, 2009, p. 3). It illustrates the constructs in a model, allows researchers to test the covariance of the variables or constructs in the model, measures the reliability of the factors, and certifies the factors' construct validity. This study used the CFA to test the hypotheses and assessed the model's goodness-of-fit based on the criteria shown in Table 8. The hypothesis testing tested if the hypotheses generated from privacy regulation theoretical framework hold true upon rigorous examination (Sekaran & Bougie, 2009).

The goodness-of-fit assessed the overall fit of the model to the observed data, the relative fit of the hypothesized model to the observed covariance matrix, and evaluated the residual between the empirical and the estimated covariance matrices (Maxim, 1999; Straub et al., 2004). In addition, the goodness-of-fit is usually examined in conjunction with other fit indices, such as the *two-index* presentation format suggested in

Table 8: Goodness-of-Fit Index, Description, and their Acceptable Threshold

Fit Index	Description	Acceptable Threshold	Reference
(χ^2/df)	Relative Chi-Square	≤ 2 (excellent) ≤ 5 (acceptable)	(Hong & Thong, 2013; Jackson et al., 2005)
RMSEA	Root Mean Square Errors of Approximation	< 0.01 (excellent fit) ≤ 0.05 (close fit) ≤ 0.08 (acceptable)	(Browne & Cudeck, 1993; Hong & Thong, 2013; Hooper et al. 2008; Jackson et al., 2005; MacCallum et al., 1996; Steiger, 2007)
SRMR	Standardized Root Mean Square Residual	≤ 0.08 (good) ≤ 0.10 (acceptable)	(Hong & Thong, 2013; Hooper et al. 2008; Hu & Bentler, 1999)
CFI	Comparative Fix Index	≥ 0.95 (recent view) ≥ 0.90 (acceptable)	(Bentler, 1990; Dinev & Hart, 2006; Hong & Thong, 2013; Hooper et al. 2008; Jackson et al., 2005)
NNFI (TLI)	Non-Normed Fit Index (Tucker-Lewis Index)	≥ 0.95 (recent view) ≥ 0.90 (acceptable)	(Hong & Thong, 2013; Hooper et al. 2008; Jackson et al., 2005)
PNFI	Parsimony Normed Fit Index	Value around 0.50 or greater	(Hooper et al. 2008; Kacmar & Carlson, 1997; Mulaik et al., 1989; Osman et al., 1997)

Hooper et al. (2008), and in Hu and Bentler (1999). The use of the two-index concept is necessary because each index reflects an aspect of a model fit. The notion of combining and/or presenting two indices is to avoid the temptation of picking and presenting only fit indices that indicate the best fit and those commonly cited in the literature (Hooper et al., 2008). Therefore, based on the Hu and Bentler's (1999) two-index presentation strategy, the study presented the fit indices depicted in Table 8.

According to Hu and Bentler (1999), the Standardized Root Mean Square Residual (SRMR) should always be presented in conjunction with the Non-Normed Fit Index (NNFI) or Tucker Lewis Index (TLI), the Root Mean Square Errors of Approximation

(RMSEA), or the Comparative Fix Index (CFI). Following Hu and Bentler (1999) suggestion, Hooper et al. (2008) advocated the salience of presenting additional fit indices and recommended the inclusion of chi-square statistics and one of the parsimony fit indices, i.e., Parsimony Normed Fit Index (PNFI).

3.8.1 Goodness of fit definitions and reporting rationale.

Relative Chi-Square. The study reported the chi-square (χ^2) and the relative chi-square (χ^2/df) because they assessed the overall fit of the model (Hooper et al., 2008). In SPSS AMOS software, the relative chi-square is presented as the *CMIN/DF,* and is the minimum discrepancy of the default model and its degree of freedom respectively. According to Bentler (1990), researchers use the chi-square to evaluate the adequacy of a structural model in order to accept or reject the null hypothesis. The chi-square "assesses the magnitude of discrepancy between the sample and the fitted covariances matrices…the product of the sample size minus one and the minimum fitting function" (Hu & Bentler, 1999). Barrett (2007) suggested that the chi-square is the only statistical test that aligns the SEM model fit to the data by testing a hypothesis for statistical significance to the goodness of fit (Albright &Park, 2009; Barrett, 2007).

Furthermore, the relative chi-square is an improvement to the chi-square because it diminishes the effect of the sample size and the effect of the size of the correlation in a model since smaller sample size and larger correlations poorly affect model fit (Barrett, 2007; Bollen & Long, 1993). The relative chi square is calculated by dividing the chi-square fit index by the degrees of freedom (Bollen & Long, 1993).

Root Mean Square Errors of Approximation. The RMSEA was reported because it helped in measuring or in determining how well the theoretical model fits the data without a baseline model (Hooper et al., 2008). Since the RMSEA is an absolute fit statistic, it assesses the wellness of priori model fit to the data (Hooper et al., 2008). A root mean square errors of approximation of 0.01 is considered an excellent fit; 0.05, a close fit; however, a RMSEA of 0.08 is acceptable (Browne & Cudeck, 1993; Hong & Thong, 2013; Hooper et al. 2008; Jackson et al., 2005; MacCallum et al., 1996; Steiger, 2007).

Nonetheless, Barrett (2007) questioned the predictive accuracy in using fit approximation in testing model fit. The paper argued for 0.01 fit and suggested that researchers are oblivious of the consequence of accepting a model with model fit of 0.05 or 0.08 since the criterion used for the fit is an abstract concept in structural equation modelling. Although Steiger 2007 acknowledged Barrett's argument that the SEM indices have no accommodation or measurement for model misfit, the paper noted that the notion of measuring misfit may be illusive because in the SEM, discrepancies are collapsed into a single measure, which makes it hard to identify the actual causes of a misfit. In addition, the author noted that the construction of a latent variable could disallow a direct observation of the variable, as such creates a weak predictability of a behavior in relationship to an expected outcome (Steiger, 2007).

Standardized Root Mean Square Residual. This SRMR was reported because it assessed the sample size, the model misspecification, and the distribution, and a value of 0.08 or lower is acceptable (Hooper et al., 2008; Hu & Bentler, 1999). The SRMR is an absolute measure of fit with values ranging from 0.0 to 1.0. It is the "square root of the difference between the residuals of the sample covariance matrix and the hypothesised covariance model [sic]" (Hooper et al., 2008, p. 54). The root mean square residual

(RMR) is similar to the SRMR, but its shortcoming stems from its calculation, which is based on the scales of each indicator to a latent variable. The SRMR is preferred to the RMR because the interpretation of the RMR is difficult, especially when dealing simultaneously with indicators with varying number of points, i.e., five-point, seven-point, and the like (Hooper et al., 2008).

Comparative Fix Index. The study reported the CFI because it compared the sample covariance of a model with its null model by measuring the difference in mean deviations (Hooper et al., 2008). It is a revision of the Normed Fit Index. The CFI performs well with a small sample size by avoiding the underestimation of fit commonly found in small sample sizes (Bentler, 1990; Hooper et al., 2008). The comparative fix index has a statistical value ranging between 0.0 and 1.0, and a value greater than 0.90 is acceptable (Dinev & Hart, 2006; Hong & Thong, 2013; Hooper et al. 2008; Jackson et al., 2005). The CFI is a very popular index in the extant literature, according to Hooper et al. (2008), because the sample size has limited effect on its measurement.

Non-Normed Fit Index (Tucker-Lewis Index). The Non-Normed Fit Index, also known as the Tucker-Lewis Index, was reported because the fit index assessed the model by comparing the chi-square value of the model to the chi-square of the null model (Hooper et al., 2008). The Non-Normed Fit Index is an improvement to the Normed Fit Index (NFI). The NNFI was reported because the NFI is very sensitive to sample size and underestimates a fit (Hooper et al., 2008). However, the NNFI is said to be difficult to interpret at times when its value is above 1.0 because of its nature of non-normed (Hooper et al., 2008). An NNFI value equal or greater than 0.90 was recommended as acceptable (Hooper et al., 2008; Jackson et al., 2005), however Hu and Bentler (1999) advocated for an acceptance value equal or greater than 0.95.

Parsimony Normed Fit Index. The study also reported the Parsimony Normed Fit Index because the PNFI adjusted for the loss of degrees of freedom based on the normed-fit index (Hooper et al., 2008). The parsimony is the ratio of degrees of freedom between a model and the null model or “the number of covariances below the main diagonal in the variance/covariance matrix,” according to Marsh and Hau (1996, p. 368). Although there is no consensus on the acceptable threshold for PNFI, a value around 0.50 or greater is acceptable (Hooper et al. 2008; Kacmar & Carlson, 1997; Mulaik et al., 1989; Osman et al., 1997).

3.8.2 Testing for moderating variable.

Sharma et al. (1981) defined moderator variable as “one which systematically modifies either the form and/or strength of the relationship between a predictor and a criterion variable” (p. 291). A predictor variable could also be characterized as the independent variable and the criterion variable as the dependent or the outcome variable (Sharma et al., 1981). Wu and Zumbo (2008) stated, “Moderator modifies the strength or direction (i.e., positive or negative) of a causal relationship” (p. 370).

There are two moderator variables in this study as shown in Figure 4a, the IPSI and IPP. The DSIP is the independent variable, while the IPE is the dependent variable. In Figure 4b, the regression coefficient *β1* is the effect of the independent variable, DISP, on the dependent variable, IPE; the *β2* is the effect of the moderator variable, IPSI, on the IPE; and the *β3* is the moderating effect of the product of the DSIP and IPSI on the IPE. In Figure 4c, the *β1* is the effect of the DISP on the IPE; the *β2* is the effect of the IPP on the IPE; and the *β3* is the moderating effect of the product of the DSIP and IPP on the

IPE. The one-way arrow is indicative of the direction of impact from one variable to another, as such, it is the structural regression coefficient (Byrne, 2013).

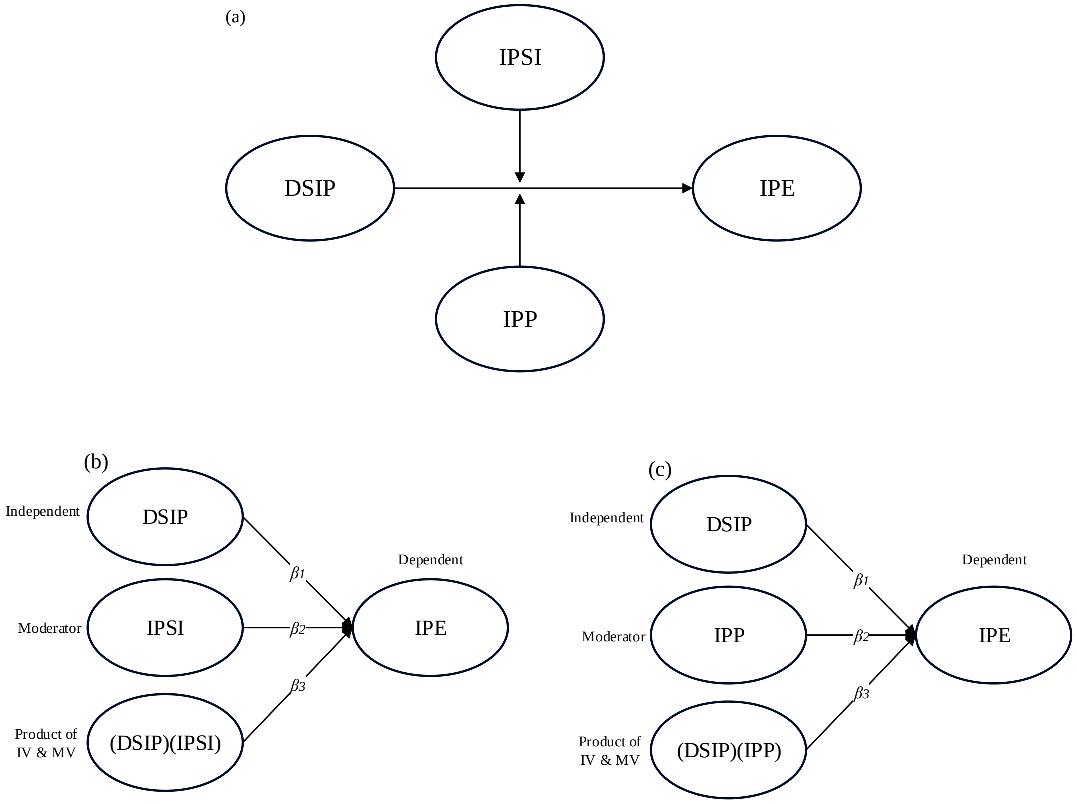


Figure 4. Moderator Model for Selective Personal Information Disclosure

Following Fairchild & MacKinnon (2008), the study evaluated the moderating effect of information privacy self-interest by using *Equation 2* for Figure 4b and *Equation 3* for Figure 4c. The intercept of the equation is the β_0, the residual is the *e*, the coefficient of the DSIP to the IPE when the IPSI is zero is the β_1, and the coefficient of the IPSI to the IPE when the DSIP is zero is the β_2. Hence, the regression coefficient of the β_3 provided an estimated moderation effect of the interaction. The test for interaction effect in this study is consistent with the extant literature, which requires a causal theory and design behind the data for estimation of causal interaction effect (Wu & Zumbo, 2008). A statistically significant of the β_3 from zero indicated that there is a significant moderation effect on the relationship between the DSIP and the IPE in the data.

$$\text{IPE} = \beta_0 + \beta_1 DSIP + \beta_2 IPSI + \beta_3 (DSIP)(IPSI) + e. \tag{2}$$

$$\text{IPE} = \beta_0 + \beta_1 DSIP + \beta_2 IPP + \beta_3 (DSIP)(IPP) + e. \tag{3}$$

3.8.3 Testing for mediation.

The study conducted simple linear regressions and a multiple linear regression analyses to test for the mediating or intervening effect of the information privacy equipoise on the relationship between a customer's desired state of information privacy and his or her selective personal information disclosure (Baron & Kenny, 1986; Judd & Kenny, 1981). A mediating variable is one, which "surfaces as a function of the independent variable, and helps in conceptualizing and explaining the influence of the independent variable on the dependent variable" (Sekaran & Bougie, 2009, p. 441). The mediation is causal in nature, according to Wu and Zumbo (2007), because it explains the *why* and how a cause-and-effect occurs.

Following these definitions, the study identified the information privacy equipoise as a mediating variable. Judd and Kenny (1981) argued for a demonstration of a mediation if a mediating variable exists in a hypothesized model. Therefore, this study tested the mediation of the information privacy equipoise. The regression analysis was used rather than the ANOVA because the regression test is better since ANOVA is limited in hypothesis testing for mediation, as suggested in the extant literature (Baron & Kenny, 1986; Fiske et al., 1982).

The rationale for the testing of the mediation affect in the model was to ensure that there are linkages among the independent variable (IV), the mediator variable (MV), and the dependent variable (DV). This is necessary because Baron and Kenny (1986) had noted, “Mediators represent properties of the person that transform the predictor or input variable [DSIP] in some way” (p. 1178). The paper identified the three properties necessary for mediation, which include a show of the existence of effects between the IV and the MV, between the MV and the DV, and between the IV and the DV.

Therefore, based on the hypothesized model, the predictor variable, DSIP, affects the outcome variable, SPID—path *c* in Figure 5; the predictor variable, DSIP, affects the mediator variable, IPE—path *a*; and the IPE affects the outcome variable, SPID—path *b*. Based path *a*, *b*, and *c*, and Steps 1-3 in Table 9, the aim was to establish the existence of a zero-order relationship among the constructs (Newson, 2014). A “zero-order relationship measures the magnitude or strength of an association between two variables, without controlling for any other factors” (Knoke et al., 2002, p. 213).

Newsom (2004) suggested that a lack of significance in one or more of the simple regressions in Step 1-3 would call to question the existence of mediation. Full mediation is achieved when DISP exerts no effect upon SPID when IPE is controlled, and partial mediation is one in which DISP exerts some effect upon SPID when IPE is controlled (Judd & Kenny, 1981). In the context, the study tested for significant of the direct and indirect effects in paths *a*, *b*, and *c*. The test for full or partial mediation, path *ć* (Step 4), is depicted in Figure 5 and in Table 9 (Newsom, 2014; Wu & Zumbo, 2008). The simple linear regression tests that the conditional mean of the SPID depended on the DSIP and IPE in Steps 1 and 3, Table 9 respectively, and that the conditional mean of the IPE depended on DSIP in Step 2 (Carvalho, 2015; Fairchild & MacKinnon, 2008).

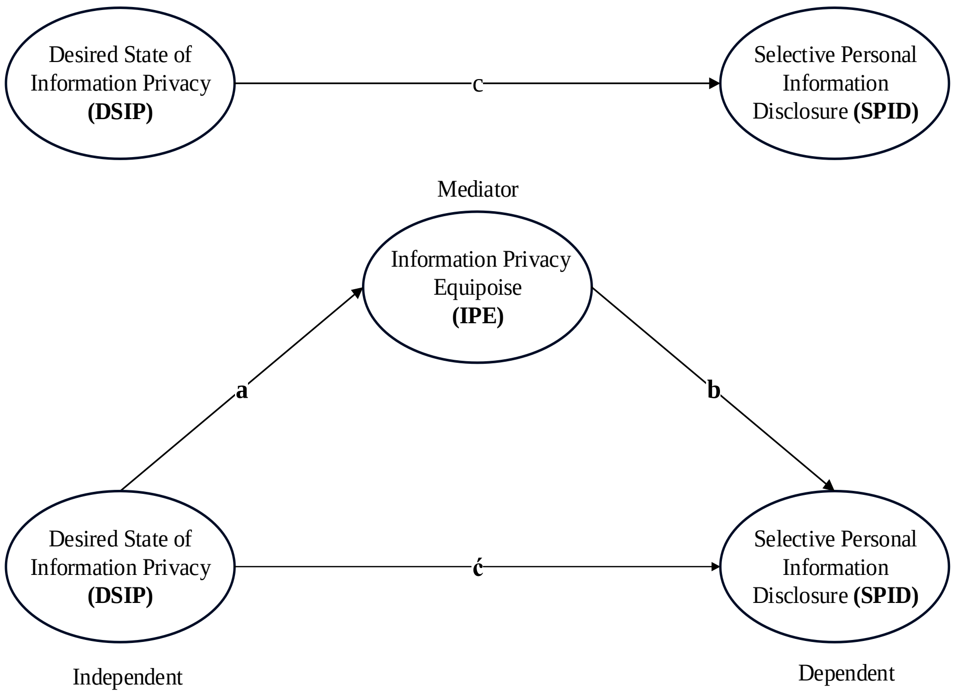
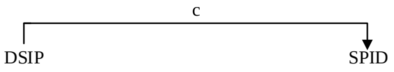
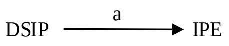
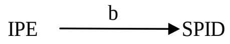
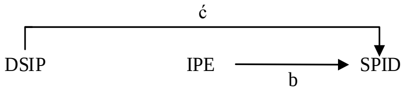

Desired State of Information Privacy (DSIP)
c
Selective Personal Information Disclosure (SPID)
Mediator
Information Privacy Equipoise (IPE)
a
b
Desired State of Information Privacy (DSIP)
ć
Selective Personal Information Disclosure (SPID)
Independent
Dependent

Figure 5. Mediator Model for Selective Personal Information Disclosure

In Figure 5 and in Tables 9, 10, and 11, the *c* is the total effect of the DSIP on the SPID; the *ć* is the effect of the DSIP on the SPID when the IPE is controlled; the *b* is the effect of the IPE on the SPID; the *a* is effect of the DSIP on the IPE; the B_0 is the equation intercept; and the *e* is the residual (Fairchild & Mackinnon, 2009).

Table 9: Test for Mediation—Causal-Step Approach (Baron & Kenny, 1986)

	Description	**Depiction**
Step 1	For path *c*, conduct simple regression analysis in which DISP would predict SPID: $\text{SPID} = B_0 + B_1 DSIP + e$	
Step 2	For path *a*, conduct simple regression analysis in which DISP would predicts IPE: $\text{IPE} = B_0 + B_1 DSIP + e$	
Step 3	For path *b*, conduct simple regression analysis in which IPE would predicts SPID: $\text{SPID} = B_0 + B_1 IPE + e$	
Step 4	For path *ć*, conduct multiple regression analysis in which DISP and IPE would predict SPID: $\text{SPID} = B_0 + B_1 DSIP + B_2 IPE + e$	

The alternatives to the Baron and Kenny (1986) *causal-steps approach*, depicted in Table 9, are the indirect test or the *difference of coefficients* presented in Table 10 (Judd & Kenny, 1981) and the indirect test or the *product of coefficients* in Table 11 (Sobel, 1982). The regression coefficient for the indirect effect signifies the change in SPID for every unit of change in DSIP, which is mediated by IPE (Newsom, 2014). In Table 10, the difference of coefficients is calculated by subtracting the partial regression coefficient value in Model 1 from Model 2. In Table 11, the product of coefficients is calculated by multiplying the partial regression coefficient value in Model 1 and Model 2.

Table 10: Indirect Test for Mediation—Difference of Coefficients (Judd & Kenny, 1981)

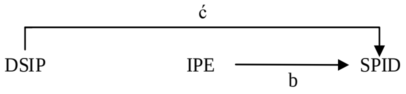
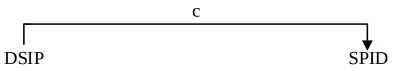
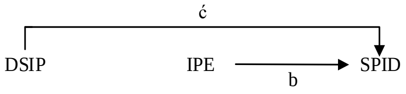
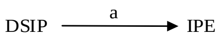
Description		Depiction
Model 1	$\text{SPID} = B_0 + B_1 DSIP + B_2 IPE + e$	
Model 2	$\text{SPID} = B_0 + B(DSIP) + e$	

Table 11: Indirect Test for Mediation—Product of Coefficients (Sobel, 1982)

Description		Depiction
Model 1	$\text{SPID} = B_0 + B_1 DSIP + B_2 IPE + e$	
Model 2	$\text{IPE} = B_0 + B(DSIP) + e$	

3.9 Empirical Validation

The reliability and validity tests were conducted for empirical validation in this study. The reliability of the survey instrument was tested because the measurement accuracy or the internal consistency of the instrument and the data were critical to the findings of the study. Reliability is the assurance that the measuring instrument will produce the same result when subjected to the same measurement (Straub et al., 2004).

Secondly, the validity test was conducted because of the potency in ensuring that the observed variables would converge and that the latent variables would discriminate. Sekaran and Bougie (2009) described validity as an "evidence that the instrument, technique, or process used to measure a concept does indeed measure the intended concept" (p. 447). In addition, Vogt (2005) stated that validity is the "extent to which a measure is free of systematic errors" (p. 335).

3.9.1 Reliability.

The Cronbach's alpha (*a*) and the construct or composite reliability (CR) estimates inherent in CFA were used to validate the reliability of the measurement instrument in the study. The Cronbach's alpha of each latent variable was measured and presented in Chapter 4. Cronbach's alpha presumes that the scoring scale of the items for each latent variable is the same (Straub et al., 2004). The use of the Cronbach's alpha reliability test has been accepted in the social science research, especially in the information privacy discipline (Awad & Krishnan, 2006; Malhotra et al., 2004). Researchers use reliability to find the "proximal measures of the true score that perfectly describe the phenomenon" (Straub et al., 2004). Carmines and Zeller (1979) suggested that true score is the average score obtainable from measuring a person on a variable for an infinite number of times. A reliability coefficient of 0.70 or greater is considered as good and a coefficient of 0.60 – 0.70 is acceptable (Awad & Krishnan, 2006; Paswan, 2009; Shadfar & Malekmohammadi, 2013; Straub et al., 2004).

In addition, in CFA, the reliability of a latent variable is said to be valid if the CR is greater than the average variance extracted (AVE). The calculation for the AVE was with *Equation 4* and the calculation for the CR was with *Equation 5*. The AVE "measures the percent of variance captured by a construct by showing the ratio of the sum of the variance captured by the construct and measurement variance" (Straub et al., 2004, p. 424). The CR is calculated by dividing the squared sum of the factor loading for each construct, by the squared sum of the factor loading for each construct and the sum of the error variance for each construct (Paswan, 2009).

3.9.2 Validity.

The content validity and construct validity were employed and tested in this study because they were relevant to the potency of the research findings. Therefore, the following paragraphs provide detail information on the definitions and types of the content and construct validity tests used in the study.

Salkind (2012) described content validity as "the extent to which a test fairly represents the universe of all possible questions that might be asked" (p. 392). Content validity is also described as "a matter of expert judgment…the ability of a group of measured variables to estimate a latent variable," according to Vogt (2005, p. 59). The judgment of the experts and the adaptation of items from the extant literature were used to validate the survey instrument in this study. To be specific, expert judgements were used to validate the indicators, especially those developed in this study, i.e., the information privacy permeability and information privacy equipoise, because the constructs were new, as such, require new definitions (Straub et al., 2004; Vogt, 2005).

Sekaran and Bougie (2009) described construct validity as one that "testifies to how well the results obtained from the use of the measure fit the theories around which the test was designed" (p. 436). Vogt (2005) noted that construct validity measures the extent to which the constructs or the variables under examination are operationalized. In other words, construct validity tests how well the chosen items in a research study fit together within a latent construct and captures the essence of the construct, and how well the latent variables in a study discriminate among themselves. Therefore, the followings are the delineation of the two types of construct validity used in this study, convergent and discriminant validity.

Convergent validity was used to measure how the measurement items or observed variables converged to their designated latent variable. It measured how well the observed variables measured the latent variable (Offor, 2013). The AVE and CR were used in measuring the convergent validity.

The AVE (see Equation 4) is calculated as the sum of the squared standardized factor loading (communalities) for each item in the construct, divided by the number of the items in the construct (Paswan, 2009). In addition, the CR (see Equation 5) is calculated as the sum of the factor loadings for a construct, squared, divided by the sum of the factor loadings for the construct, squared and the sum of the error variances of the construct (Paswan, 2009). The error variance for each item in a construct is calculated as 1.0 minus the squared standardized factor loading of the item in the construct. For the equations, the λ is the standardized factor loading, the i is the number of items, the δ is the error variance. Adequate convergent validity is established if the standardized factor loadings for the items are equal or greater than 0.60; if the AVE is equal or greater than 0.50; and if the CR is equal or greater than 0.70 for the latent variables (Malhotra et al., 2004;

Paswan, 2009).

$$AVE = \frac{\sum_{i=1}^{n} \lambda_i^2}{n}. \tag{4}$$

$$CR = \frac{(\sum_{i=1}^{n} \lambda_i)^2}{(\sum_{i=1}^{n} \lambda_i)^2 + (\sum_{i=1}^{n} \delta_i)}. \tag{5}$$

Discriminant validity measures how the latent variables discriminate among each other. It demonstrates the distinctiveness of each construct in a study. Under discriminant validity, a construct is said to be valid if the inter-construct correlations between the constructs are discriminant. To be discriminant, a construct's average variance extracted would need to be greater than its associated squared inter-construct (SIC) correlations (Paswan, 2009). In other words, the "correlations between two constructs that are greater than the square root of AVE are indicative of poor discriminant validity between the constructs involved," according to Boss et al. (2009, p. 157).

3.10 Summary

This chapter addressed the theoretical framework and the research method approach used in this study.

The theoretical framework contains the analysis of the underlying principles inherent in the privacy regulation theory and the construction of the latent variables under examination. The framework also provided the descriptions of the constructs, the hypotheses, the research model, and the philosophical position of this study.

The research approach covered the research design, the instrument development and validation, the research strategy, the data collection, the data analysis and interpretation, and the empirical validations. The research design discussed the rationale for the cross-sectional survey research and the unit of analysis. The instrument development and validation section presented the logical reasoning behind the adaptation of indicators in the extant literature and the creation of new ones. The research strategy was the avenue of approach in conducting this research. The data collection section contains a three-phase approach to the data collection process for effectiveness. The current and acceptable measures of goodness of fit were discussed in detail in the data analysis and interpretation section. In the empirical validation section, the pathway used in testing the reliability and the construct validity of the result were stipulated.

Chapter 4

Result

4.1 Introduction

This chapter provides the result of the data collections and analyses, the research findings, and the summary of the research result. In other words, the chapter presents the result of the study based the proposed theoretical framework, the research model, the research design, the research strategy, the data collection and data analysis methods, and the validation and interpretation approaches presented in the previous chapters.

4.2 Data Collection and Analysis

The data collection and analysis were broken into three stages in order to reflect the three phases of the data collection approach presented in Chapter 3. The first stage describes the result of the data collected from the expert panelists who validated the survey instrument. The content validation was completed through the application of the substantive validity analysis and the content validity ratio. The second stage describes the result of the pilot test. Finally, the third stage is a complete presentation of the final result of the data collection, analysis, validation, and interpretation.

4.2.1 Expert panel.

The expertise of the knowledgeable judges was sought longitudinally at two different times during the Stage 1 of the data collection and analysis for (1) the substantive validity analysis and (2) the content validity ratio. The segmentation of the surveys was necessary because the objectives of the outcome of the substantive validity analysis and the content validity ratio were different. For instance, while the objective of the substantive validity analysis was to provide suitable definition[3] for each construct in the study relative to the reflectiveness of the construct in the proposed items, the objective of the content validity ratio was to validate the relevance[4] of each observed variable to its associated construct.

The surveys for the substantive validity analysis and the content validity ratio were sent to the same 15-member expert panelists three weeks apart. The first survey was for the substantive validity analysis and the second was for the content validity ratio. The thought was that it is better to obtain the suitable definitions of the constructs first and then evaluate their relevancy to their associated indicator variables. The response rates for the substantive validity analysis and the content validity ratio were 0.60 and 0.73 respectively.

4.2.1.1 Substantive validity analysis.

The result of the substantive validity analysis was mixed. Twenty-five percent of the observed variables were appropriately allocated to their intended constructs. However, only 50% of the 25% correct selections were completed by the one-half of the total number of participants. The detail result of the substantive validity analysis is in Appendix F. The major takeaway from the substantive validity analysis was the value of the recommendations obtained from the panelists. Some of judges cited the wordiness and how technical some of the definitions were, others recommended for the simplification of the definitions and the provision of examples whenever possible in order to provide the respondents with the most suitable context.

[3] See the introductory letter to the participants in Appendix E., p. 159.

[4] Ibid., p. 160.

Therefore, based on the expert panelists' recommendations from the substantive validity analysis survey, the definitions of the constructs were reworded, especially for the *new* and the *modified* items. The revision centered mostly on those items associated with the information privacy equipoise construct. The focus on the information privacy equipoise construct was to ensure that the items were able to project a *state* (a condition or an acceptance of a belief at a particular time), rather than an *act* (a deed) as the initial items seem to have indicated.

4.2.1.2 Content validity ratio.

Table 12 is a presentation of the result of the content validity ratio. The table contains 25 items, which are unevenly divided among the five constructs depicted in the research model in Figure 1.

Table 12: Summary Result of the Content Validity Ratio

Item #	***N***	**# of *Essential***	**# of *Useful but not essential***	**# of *Not necessary***	**Percentage of *essential* selection**	**The Study's CVR = n_e-(N/2)/N/2**
Q1	11	**8**	1	2	**0.73**	0.45
Q2		**6**	2	3	**0.55**	0.09
Q3		4	5	2	0.36	-0.27
Q4		**8**	2	1	**0.73**	0.45
Q5		**8**	2	1	**0.73**	0.45
Q6		**10**	0	1	**0.91**	**0.82**
Q7		**8**	1	2	**0.73**	0.45
Q8		**8**	1	2	**0.73**	0.45
Q9		**6**	4	1	**0.55**	0.09
Q10		**9**	0	2	**0.82**	**0.64**
Q11		**8**	2	1	**0.73**	0.45
Q12		**9**	1	1	**0.82**	**0.64**
Q13		5	4	2	0.45	-0.09
Q14		4	1	6	0.36	-0.27
Q15		5	4	2	0.45	-0.09
Q16		**7**	1	3	**0.64**	0.27
Q17		**8**	2	1	**0.73**	0.45
Q18		**9**	1	1	**0.82**	**0.64**
Q19		5	2	4	0.45	-0.09
Q20		5	2	4	0.45	-0.09
Q21		**8**	1	2	**0.73**	0.45
Q22		**8**	1	2	**0.73**	0.45
Q23		**7**	1	3	**0.64**	0.27
Q24		**10**	0	1	**0.91**	**0.82**
Q25		**8**	1	2	**0.73**	0.45

For clarity, the questions on the table were aligned with their associated construct. The desired state of information privacy is the independent variable (Q1-Q4), and the information privacy self-interest and the information privacy permeability are the moderating variables (Q5-Q7 and Q8-Q12 respectively). In addition, the information privacy equipoise is the mediating variable (Q13-Q20) and the selective personal information disclosure is the dependent variable (Q21-Q25).

Seventy-six percent of the items were rated as being *essential* by one half or more of the expert panelists, and 0.79 of the 0.76 essential ratings were greater than 0.70. Therefore, 76% of the items have some degree of content validity (see Table 12) based on the assumptions in Lawshe (1975), and the statistic linearity of reporting of the *essential* rating by the panelists (Wilson et al., 2012). According to Lawshe (1975), when all members of an expert panel rate an item as being *essential*, then the CVR for that item is 1.0, although it is usually adjusted to 0.99 for ease of manipulation. In addition, the paper suggested that if an item receives an *essential* rating by 0.50 or more from the participating panelists, then it is perceived that the item has some level or degree of content validity. However, the extent or degree of the content validity for an item depends largely on the number essential rating for that item beyond 0.50 (Lawshe, 1975). Hence, Appendix C contains the detail information on the content validity ratio.

Although most of the items demonstrated content validity beyond 0.50, only 0.2 exceeded the 0.59 threshold of the CVR recommended for an 11-member panelist (Lawshe, 1975; Wilson et al., 2012). Consequently, the items for the desired state of information privacy and the information privacy equipoise constructs were revised extensively because of their low CVR. The study retained items with CVR of 0.45

because the difference between the items being above or under the threshold is by one panelist's essential selection, and because Lawshe (1975, p. 568) suggested, "It should be pointed out that the use of the CVR to reject items does not preclude the use of a discrimination index or other traditional item analysis procedure for further selecting those items to be retained in the final form of the test."

Table 13 is a presentation of the demographic statistics of the expert panelists for the construct validity ratio.

Table 13. Demographics Characteristic of the Content Validity Ratio

Characteristics	Frequency	Percentage
Gender		
Male	9	0.82
Female	2	0.18
Age		
20 years and under	0	0.00
21—30 years	1	0.09
31—40 years	2	0.18
41—50 years	4	0.36
51—60 years	3	0.27
61—and over	1	0.09
Highest level of education (degree) completed		
High school	0	0.00
Associate Degree	0	0.00
Bachelor Degree	0	0.00
Graduate-Professional Degree	8	0.73
Other (Ph.D.)	3	0.27
Employment category		
Self-employed	1	0.09
Private organization	1	0.09
Government agency	4	0.36
Public organization	4	0.36
Non-government organization (NGO)	0	0.00
Other (Full-time student)	1	0.09
Years of work experience		
None	1	0.09
One year and under	0	0.00
Two—three years	0	0.00
Four—five years	0	0.00
Six—seven years	0	0.00
Eight—nine years	0	0.00
10 years and over	10	0.91

4.2.2 Pilot test.

The survey for the pilot test was sent to 68 participants using the Survey Monkey audience. However, 13 out of the 68 sample subjects started the survey, but did not complete it. In other words, although the study received the 68 responses, only 55 of them were valid. Therefore, the pilot test had 0.81 response rate, which is in line with the recommendations [5] in the extant literature (Sivo et al., 2006).

4.2.2.1 Exploratory factor analysis.

The EFA was used in determining the capacity and the number of observed variables to measure the constructs in this study or in detecting the patterns in the data (Albright & Park, 2009; Allen & Meyer, 1990; Fabrigar et al., 1999). In addition, the EFA was conducted to ensure that the constructs, factors, or latent variables in the study would be adequately reflected in the sets of the observed variables adapted by the study and those it developed (Allen & Meyer, 1990; Vogt & Johnson, 2016).

Table 14 is the demographic description of the pilot test. In addition, in the descriptive statistics in Appendix I, the *Analysis N* is equal to the 55 cases for each observed variable. The responses with missing data were excluded from this analysis and the *exclude cases listwise* was selected from the *factor analysis options* to eliminate the inclusion of missing data in the analysis. The use of the 55 cases in the pilot test for the factor analysis is in line with the suggestion in the extant literature. Winter et al. (2009) submitted, "EFA is generally regarded as a technique for large sample size (N), with *N* =

[5] Sivo et al. (2006) wrote, "Among the selected research in which data were gathered using questionnaires, the average response rate ranged from 22% to 59.4%. More specifically, for JAIS, the average was 22%, ranging from 10.2% to 37%; for ISR, the average was 42% ranging from 7% to 93.3%; for MISQ, the average was 38.5% ranging from 5.7% to 100%; for EJIS, the average was 29.3% with a wide range from 3% to 100%; for MS, the average was 59.4% with a range from 38.1% to 88%; and for JMIS, the average was 37.8%, ranging from 16% to 86%" (p. 356).

50 as a reasonable absolute minimum" (p. 147).

Table 14. Demographic Characteristics for the Pilot Test

Characteristics	Frequency	Percentage
Gender		
Male	23	0.42
Female	32	0.58
Age		
18 - 20 years	4	0.07
21 - 30 years	17	0.31
31 - 40 years	16	0.29
41 - 50 years	9	0.17
51 - 60 years	4	0.07
61 years and over	5	0.09
Highest level of education (degree) completed		
High school or its equivalent	15	0.27
Associate Degree	12	0.22
Bachelor Degree	17	0.31
Graduate/Professional Degree	11	0.20
Other	0	0.00
Employment category		
Student	8	0.15
Self-employed	10	0.18
Private Organization	16	0.29
Governmental Organization	7	0.13
Public Organization	9	0.16
Non-Government Organization	5	0.09
Other (Disabled)	0	0.00
Years of work experience		
None	2	0.04
1 year and under	3	0.05
2 - 3 years	4	0.07
4 - 5 years	6	0.11
6 - 7 years	5	0.09
8 - 9 years	5	0.09
10 - 20 years	19	0.35
21 years and over	11	0.20

The correlation matrix for the pilot study, presented in Appendix H, was 1.004E-7. The *determinant* of the correlation matrix for this pilot test was met because the determinant was not equal to zero and could be explained by linear combinations (Beavers et al., 2013), however, the determinant was less than .00001, which is another criterion for measuring determinant (Beaumont, 2012). Beavers et al. (2013) stated, “The determinant of a matrix is a single value calculated using the values within a square matrix, revealing the presence or absence of possible linear combinations within the matrix” (pp. 3-4). The paper suggested that when a determinant is equal to zero, it is presumed to be a singular matrix without possibility of linear combinations. Conversely, when a determinant is not equal to zero, it could be explained by linear combinations.

Furthermore, the *Bartlett’s Test of Sphericity*, a test for the determinant value (Beavers et al., 2013), was statistically significant with *p-value* = .000—see Table 15, which indicated that the pilot test correlation matrix was statistically different from an *identity* matrix (Dziuban & Shirkey, 1974). An identity matrix is one in which all, but the main diagonal are zeros, or one in which the correlation between the observed variables are zeros (Gantmakher, 2000), or “a square matrix in which all the elements of the principal diagonal are ones and all other elements are zeros” (Sun et al., 2015, p. 2079).

The correlation matrix in Appendix H expressed how the observed variables relate to one another, the strength of the relationships, and their linearity (Beavers et al., 2013). Normally, evidence of the commonality is demonstrated when a correlation is greater than .30 (Beavers et al., 2013). While the majority of the observed variables in the matrix revealed high correlations, above 0.50, a few of them showed lower correlations, below 0.30, which could potentially affect their loadings relative to their constructs.

The Kaiser-Meyer-Olkin (KMO) test for the pilot test was 0.673 as shown in Table 15. Vogt and Johnson (2016) recommended a 0.70 threshold for KMO and assumes that a KMO below 0.70 indicates that there may not be enough items for some of the factors. The KMO for the main data collection was 0.768. Further discussion concerning the number of items is contained in the rotated component matrix section. The KMO is affected by the sample size and is "an indicator of the strength of the relationships among [the] variables in a correlation matrix…by calculating the correlations between each pair of variables after controlling for the effects of all other variables" (Vogt & Johnson, 2016, p. 220).

Table 15. KMO and Bartlett's Test for the Pilot Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.673
Bartlett's Test of Sphericity	Approx. Chi-Square	754.667
	df	171
	Sig.	.000

4.2.2.2 Principal component analysis.

The overview of the pattern in the data is well-defined in Table 16. The rotated component matrix indicated that most of the items have high factor loadings, except those items that cross-loaded. During the principal component analysis (PCA), the study elected to exclude factor loadings that were less than |.40| for clarity. In table 16, the items with the highest loadings are at the top of the hierarchy for each factor, i.e., for factor 1, the IPP2 is on top because it has a loading of .945 and the DSIP2 is at the bottom because it has the lowest loading of .509 within the factor. Meanwhile, Factor 5 has only two indicators because IPE1 (.478) and IPE2 (.450) cross-loaded to the second and the third factors respectively. In addition, while the DSIP2 (.509) cross-loaded to Factor 1, it has a higher loading of .515 in Factor 4. Finally, DSIP4 cross-loaded to Factor 1 (.553), instead of aligning itself with Factor 4 like the rest of the DSIP items.

Table 16. Extraction Method: Principal Component Analysis

Rotated Component Matrix[a]

	Component				
	1	2	3	4	5
IPP2	.945				
IPP3	.922				
IPP4	.896				
IPP1	.777				
DSIP4	**.553**				
SPID2		.880			
SPID4		.864			
SPID3		.853			
SPID1		.761			
IPE1		**.478**			
IPSI1			.876		
IPSI2			.860		
IPSI3			.852		
IPE2			**.450**		
DSIP1				.833	
DSIP3				.811	
DSIP2	**.509**			**.515**	
IPE3					.892
IPE4					.865

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]
a. Rotation converged in 6 iterations.

One of the implications is that the DSIP2 is measuring Factor 1 and Factor 4 above a loading greater than 0.5, which could pose a multicollinearity problem. Nonetheless, the study decided to retain the items for the final data collection because the sample size for the pitot test was smaller (Beavers et al., 2013).

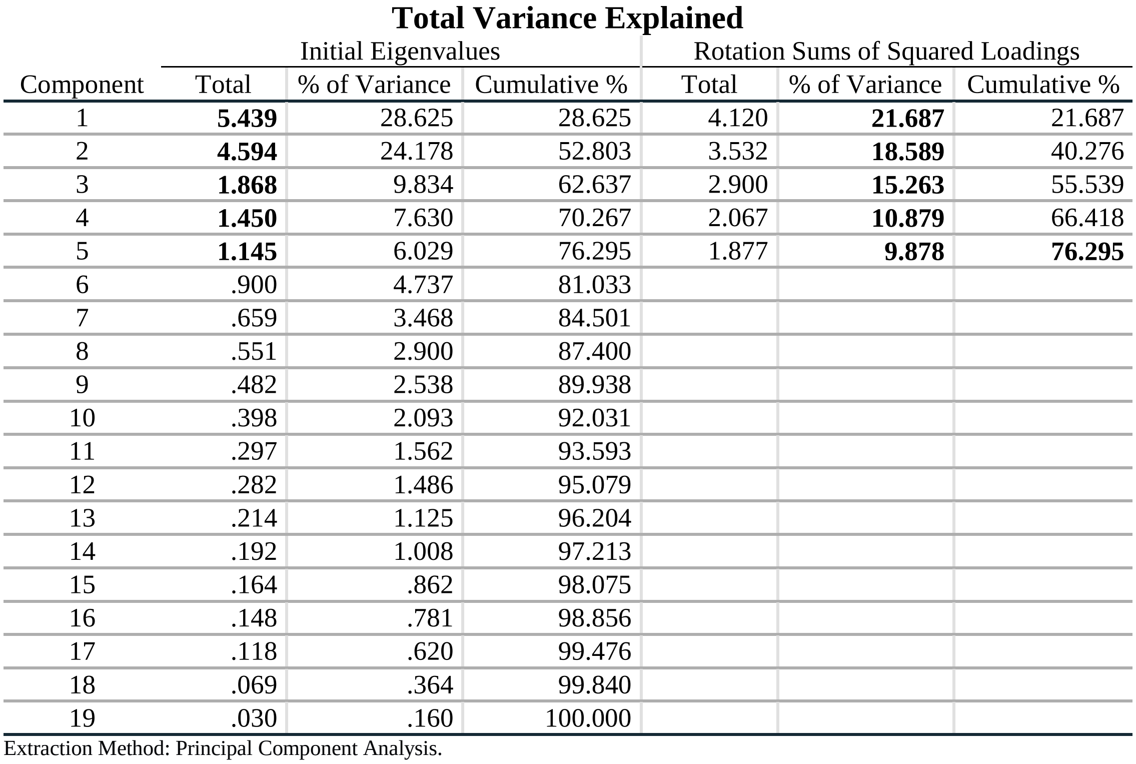
The principal component analysis was conducted with the Varimax rotation to measure the clustering of the observed variables. Vogt and Johnson (2016) described the principal component analysis as “methods for undertaking a linear transformation of a large set of observed correlation variables into a smaller set of uncorrelated latent variables…[which] makes analysis easier by grouping data into more manageable units and eliminating problems of multicollinearity” (p. 339). The data from the pilot test showed tight factor groupings, as previously stated and expressed in Table 16. Likewise, in Table 17, the Total Variance Explained produced the same result, when the *fixed number of factors* was select and pegged to five (5) and when it wasn't, using the SPSS statistics software selection option for the factor analysis extraction.

Table 17 illustrates the total variance explained for the pilot test. The table is a presentation of the degree of variance accounted for by each factor. In the pilot test, Factors 1-5 accounted for 21.687%, 18.589%, 15.263%, 10.879%, and 9.878% of the variability in the 19 observed variables respectively, which amounted to a 76.295% of the total variance. During the test, the *eigenvalue* was set to 1.0, which means that the total factor *rotation sums of square loadings variance* for a component must be greater than 1.0 to be considered significant (Vogt & Johnson, 2016). The result indicated that 5 out of 19 possible factors exceeded the eigenvalue (5.439, 4.594, 1.868, 1.450, and 1.145), which represents the five factors under consideration (Albright & Park, 2009). Vogt and Johnson (2016, p. 138) defined the eigenvalue as "a statistic used in factor analysis to indicate how much of the variation in the original group of variables is accounted for by a particular factor." The notion of the 19 possible factors indicate that when the eigenvalue is less than 1.0, "the component accounts for less variance than a single variable" would have been explained (Floyd & Widaman, 1995, p. 291).

4.2.3 Final data analysis.

First, the study prepared the data by performing the data screening. Secondly, the study conducted the confirmatory factor analysis and the structural equation modelling to assess the measurement and structural model. Thirdly, the reliability and the validity of the instrument and the constructs were tested, analyzed, and interpreted. Finally, the study tested the effects of the moderator and the mediator variables.

Table 17. Principal Component Analysis for the Pilot Test



Total Variance Explained

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	**5.439**	28.625	28.625	4.120	**21.687**	21.687
2	**4.594**	24.178	52.803	3.532	**18.589**	40.276
3	**1.868**	9.834	62.637	2.900	**15.263**	55.539
4	**1.450**	7.630	70.267	2.067	**10.879**	66.418
5	**1.145**	6.029	76.295	1.877	**9.878**	**76.295**
6	.900	4.737	81.033			
7	.659	3.468	84.501			
8	.551	2.900	87.400			
9	.482	2.538	89.938			
10	.398	2.093	92.031			
11	.297	1.562	93.593			
12	.282	1.486	95.079			
13	.214	1.125	96.204			
14	.192	1.008	97.213			
15	.164	.862	98.075			
16	.148	.781	98.856			
17	.118	.620	99.476			
18	.069	.364	99.840			
19	.030	.160	100.000			

Extraction Method: Principal Component Analysis.

4.2.3.1 Data screening.

The data screening includes the assessment of the response rate, the descriptive statistics, the missing data, the response set, the outliers, and the normality.

4.2.3.1.1 Response rate.

Out of about 500 surveys sent to the targeted sample subjects through the email invitation, survey audience, and web link for the final data collection, only 229 responses were received from the respondents. However, only 201 out of the 229 responses were valid because of some missing data. Within the 201 valid responses, only 200 have valid descriptive statistics information. Hence, the response rate for this study is at 0.40. The receipt of a 40% response rate is in line with the recommendations in the extant literature (Sivo et al., 2006).

Table 18. Demographics

Characteristics	Frequency	Percentage
Gender		
Male	103	0.52
Female	97	0.48
Age		
18 - 20 years	2	0.01
21 - 30 years	6	0.03
31 - 40 years	55	0.27
41 - 50 years	83	0.41
51 - 60 years	43	0.22
61 years and over	11	0.06
Highest level of education (degree) completed		
None	2	0.01
High school or its equivalent	11	0.06
Associate Degree	31	0.15
Bachelor Degree	88	0.44
Graduate/Professional Degree	68	0.34
Employment category		
Student	5	0.03
Self-employed	11	0.05
Private Organization	26	0.13
Governmental Organization	129	0.64
Public Organization	11	0.06
Non-Government Organization	18	0.09
Years of work experience		
None	1	0.01
1 year and under	4	0.02
2 - 3 years	1	0.01
4 - 5 years	3	0.01
6 - 7 years	5	0.03
8 - 9 years	2	0.01
10 - 20 years	61	0.30
21 years and over	123	0.61

4.2.3.1.2 Descriptive statistics.

Table 18 is a presentation of the descriptive statistics of the sample subjects. The statistics indicates that 52% of the respondents were male and 48% were female. It also showed that most of the respondents in the study were between 31 and 50 years of age. In addition, the indication was that most of the respondents have bachelor or higher degrees and are gainfully employed in the governmental organizations. Finally, about 91% of the respondent have worked for 10 years or more.

Another descriptive statistic of great importance in this study is the degree of the respondents' access to the Internet at home and/or at work. This is necessary in order to control for the capacity or Internet accessibility. In Table 19, about 91% of the respondents have extensive access to the Internet. In addition, about 88% of the sample subjects have the capacities and the capabilities to transact online at home to a large extent. The only drawback to the Internet access is that about 21% of the respondents have little or no access to transact online at work, outside their job requirements, with their workstations or their Internet capable devices.

Table 19. Access to the Internet

Characteristics	Frequency	Percentage
Regular Access to the Internet		
Somewhat	2	0.01
To a moderate extent	16	0.08
To a large extent	182	0.91
Access to the Internet at Home and/or Work		
Somewhat	4	0.02
To a moderate extent	13	0.07
To a large extent	183	0.91
Freedom to Transact Online with Home or Personal Mobile Device		
Very little	2	0.01
Somewhat	6	0.03
To a moderate extent	16	0.08
To a large extent	176	0.88
Freedom to Transact Online with Work or Personal Mobile Device		
Not at all	24	0.12
Very little	17	0.09
Somewhat	33	0.16
To a moderate extent	36	0.18
To a large extent	90	0.45

4.2.3.1.3 Missing data.

From the planning perspective, efforts were made to mitigate the issue of the missing data in this study. For instance, the online survey was designed not to allow a respondent to submit a survey without answering all the questions. However, the subjects' responses were also designed to save on-the-fly because the notion was to allow respondents to take breaks intermittently while taking the survey, as needed, prior to the final submission. As a result, the receipt of incomplete data was practically unavoidable.

Additionally, the study appealed to the participants, through the cover letter, to complete the survey by explaining the criticality and the essence of completing the whole survey. Nonetheless, the study was unable to receive completed responses from all the participants due to abandonment. Thus, the study visually removed the 27 responses with missing data using the SPSS statistic software.

4.2.3.1.4 Response set.

There was no evidence of response set in the remaining data points used for the final analysis. However, a visual at the all the 229 responses the study received indicated that some of the subjects who exhibited the propensity for response set also abandoned the survey, as discussed in the preceding section. A response set is "a tendency of subjects to give the same type of answer to all questions rather than answering questions based solely on their content" (Vogt & Johnson, 2016, p. 384).

4.2.3.1.5 Outliers.

The test for outlier was conducted, which resulted in the removal of one extreme case, number 102, from the data set. Using the *histogram* and the *explore* (stem-and-leaf plot) in the descriptive analyzer in the SPSS software, the study identified the extreme case. In addition, the univariate outlier was used to test the data in order to ensure that the *z* score is within the acceptable +/-3.29 threshold, and the multivariate linear regression was used as well, which yielded the same result (Tabachnick & Fidell, 2007). A few cases were found to be high for IPP2, but did not meet the extreme case criterion (Hoaglin & Iglewicz, 1987).

4.2.3.1.6 Normality.

The skewness and the kurtosis were used to measure the distribution of the variables. The normality distribution threshold of < 3.0 for skewedness and 10.0 for kurtosis were met (Offor, 2013; Weston & Gore, 2006) based on the review of the histograms (see Appendix M) and the assessment of normality result from the analytic software, SPSS AMOS. The skewness is a measure of the asymmetric or the symmetric normality distribution of a variable, and the kurtosis measures the peak and tail of the distribution (Offor, 2013). In a critical review of kurtosis, Balanda and MacGillivray (1988) provided a vague definition of kurtosis as "the location- and scale-free movement of probability mass from the shoulders of a distribution into its center and tails" (p. 111).

4.2.3.2 Confirmatory factor analysis.

The confirmatory factor analysis was used to evaluate the measurement model, the reliability, and the construct validity (Maxim, 1999). Figure 6 is the initial CFA model specification.

The measurement model assumes that the operationalization of a model is without any cross-loading in order to ensure the convergence of the observed variables and the discriminant of the latent variables. The CFA was conducted using the SPSS AMOS structural equation modelling software. The overall goodness-of-fit of the initial confirmatory factor analysis presented in Figure 6 was acceptable based on the relative chi-square of 2.28. However, a couple of fit indices were marginal when compared with recent recommendations in the extant literature, i.e., the indices for the model in Figure 6 are GFI = .856, AGFI = .808, CFI = .904, TLI = .884, RMSEA = .080, SRMR = .200, and PNFI = .700.

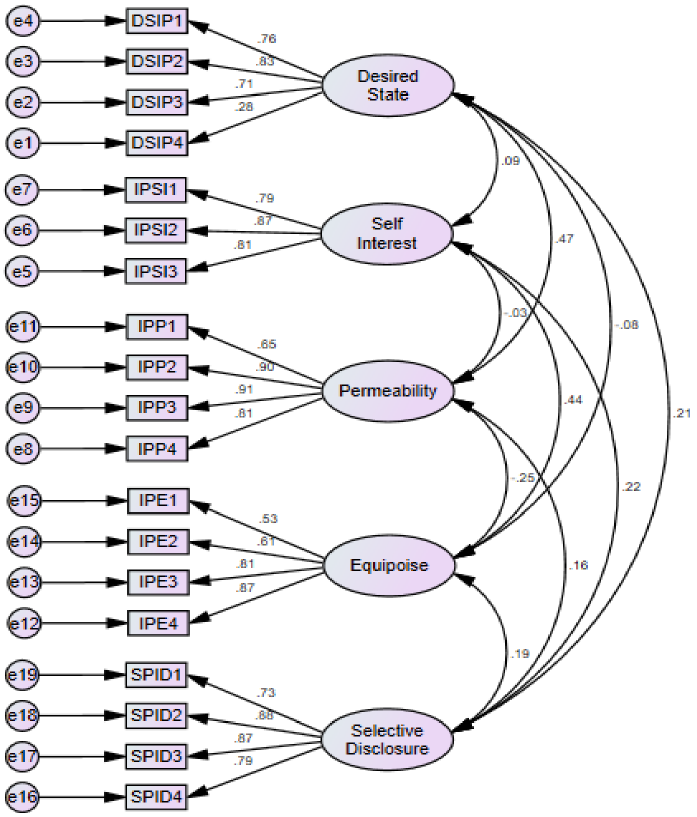


Figure 6. The Initial Hypothesized CFA Model

Consequently, the model was re-specified as presented in Figure 7. Hooper et al (2008) recommended for the removal of indiscriminant items because although they may improve the model, they may not have major theoretical repercussions. In addition, following the modification indices recommendation in the covariances table, items such as the DSPI4, IPE3, and IPE4 were deleted. According to Jöreskog and Sörbom (1984), a correct model is one in which most of the standardized residual estimates are less than two in absolute value. The residual covariance is the difference between the sample and the model-implied covariances (Jöreskog & Sörbom, 1984).

The overall goodness-of-fit of the CFA final hypothesized model in Figure 7 is excellent and acceptable because the relative chi-square (χ^2/df), which assesses the overall fit of a model (Vogt & Johnson, 2016) is at 1.636 (χ^2/df—148.91/91). In addition, since

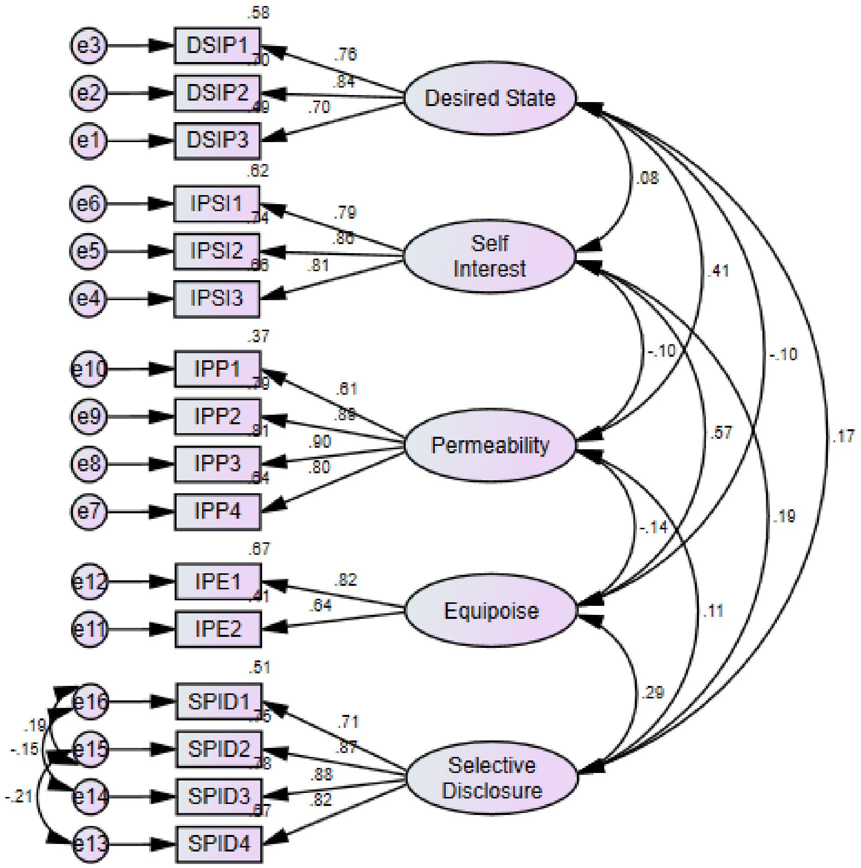


Figure 7. The Final Hypothesized CFA Model

goodness-of-fit is usually examined in conjunction with other fit indices (Hooper et al. 2008; Hu & Bentler,1999), Table 20 presents the detail result of the study's hypothesized CFA model. Therefore, the rest of the goodness-of-fit indices of the measurement model for the study is as follows: GFI = 0.919, AGFI = 0.879, RMSEA = 0.056, SRMR = 0.107, CFI = 0.964, NNFI (TLI) = 0.952, and PNFI = 0.692.

The study presented the initial and the finalized goodness-of-fit results in order to avoid the conflict between the interpretability and goodness-of-fit characteristics of the models since "the interpretability of a model can be judged only subjectively and is not amenable to the application of statistical methods" (Bollen & Long, 1993, p. 136).

Table 20. The Goodness-of-Fit Index

Fit Index	Threshold	Study
Absolute Fit Measures		
Relative Chi-square (χ^2/df)	< 5	1.636
GFI	≥ 0.90	0.919
AGFI	≥ 0.90	0.879
RMSEA	≤ 0.08	0.056
SRMR	≤ 0.10	0.107
Incremental Fit Measures		
CFI	< 0.95	0.964
NNFI (TLI)	≥ 0.95	0.952
NFI	≥ 0.90	0.913
Parsimonious Fit Measures		
PNFI	≥ 0.50	0.692
PCFI	≥ 0.50	0.731

Table 21 is a presentation of the factor loadings for the study based the CFA hypothesized model in Figure 7. In the SPSS AMOS software, it is the standardized regression weight estimate. All the factor loadings for each observable variable are equal or greater than 0.60.

Table 21. The Factor Loadings for the Study

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
DSIP3	<---	Desired State	0.69741
DSIP2	<---	Desired State	0.83580
DSIP1	<---	Desired State	0.76200
IPSI3	<---	Self Interest	0.81189
IPSI2	<---	Self Interest	0.85929
IPSI1	<---	Self Interest	0.78515
IPP4	<---	Permeability	0.79860
IPP3	<---	Permeability	0.89843
IPP2	<---	Permeability	0.89013
IPP1	<---	Permeability	0.60930
IPE2	<---	Equipoise	0.64089
IPE1	<---	Equipoise	0.81804
SPID4	<---	Selective Disclosure	0.81816
SPID3	<---	Selective disclosure	0.88038
SPID2	<---	Selective disclosure	0.86714
SPID1	<---	Selective disclosure	0.71138

4.2.3.2.1 Reliability.

The reliability of the proximal measure of the true score that describes the variable flawlessly (Straub et al., 2004) in the study yielded a good result. A test for the Cronbach Alpha, presented in Table 22, using the SPSS software reliability scale resulted in a 0.805 reliability coefficient for the desired state construct, 0.856 for the self-interest, 0.866 for the permeability, 0.687 for the equipoise, and 0.886 for the selective disclosure. In the extant literature, reliability coefficient equal or greater than 0.70 is considered as good and acceptable (Awad & Krishnan, 2006; Paswan, 2009; Shadfar & Malekmohammadi, 2013; Straub et al., 2004).

Table 22. Cronbach Alpha for Construct Reliability

Reliability Statistics									
Desired State		**Self-Interest**		**Permeability**		**Equipoise**		**Selective Disclosure**	
Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items	Cronbach's Alpha	N of Items
0.805	3	**0.856**	3	**0.866**	4	**0.687**	2	**0.886**	4

Furthermore, the Excel Stats Tools Package (Dawson, 2016), which was based on the calculations in *Equations 4* and *Equations 5*, was used in calculating the construct or composite reliability (CR) as well, and the result was good (see Table 23). For instance, based on *Equation 4*, the AVE for the desired state is equal to $0.697^2 + 0.836^2 + 0.762^2 \div 3 = 0.589$, and based on the *Equation 5*, the CR is equal to $(0.697+0.836+0.762)^2 / ((0.697+0.836+0.762)^2 + (0.514+0.301+0.419)) = 0.810$. Malhotra et al. (2004) stated, “A scale is said to be reliable if the CR > 0.70 and the AVE > 0.50” (p. 345). In addition, a CR coefficient well above 0.60 is considered a “rule of the thumb of acceptability” (Smith et al., 1996, p. 187).

Table 23. The Reliability and Validity Table for the Study

	CR	AVE	MSV	MaxR(H)	Permeability	Desired State	Self Interest	Equipoise	Selective Disclosure
Equipoise	0.698	0.540	0.320	0.731	**0.735**				
Desired State	0.810	0.589	0.171	0.881	-0.098	**0.767**			
Self Interest	0.860	0.671	0.320	0.932	0.566	0.077	**0.819**		
Permeability	0.880	0.652	0.171	0.960	-0.141	0.414	-0.099	**0.808**	
Selective Disclosure	0.892	0.676	0.086	0.971	0.294	0.175	0.193	0.106	**0.822**

4.2.3.2.2 Construct validity.

Construct validity is a test of the convergence of the observed variables to a designated latent variable in the CFA and a test of the discriminant of the latent variable from other latent variables in a study.

A construct has convergent validity if its AVE is greater than 0.50 (Hair et al., 2011). The result indicated that all the constructs in the study have convergent validity greater than 0.50 as expressed in Table 23. The CR for each construct is equal or greater than 0.698. Each construct's CR is greater than its associated AVE estimate (Malhotra et al., 2004). Convergent validity is an assessment of the factor loadings, the average variance extracted and the reliability (Paswan, 2009). The objective was to have the standardized loadings estimates that are 0.60 or greater, the AVE(s) that are 0.50 or greater, the reliability measurements that are equal or greater than 0.70 (Malhotra et al., 2004; Paswan, 2009).

In addition, convergent validity exists if the AVE(s) is greater than its associated maximum shared square variance (MSV) for each construct in the study (Malhotra et al., 2004; Paswan, 2009). The result indicates that each construct's AVE is greater than its associated MSV. In Table 23, the AVE for Equipoise = 0.540 (MSV = 0.320), desired state = 0.589 (MSV = 0.171), self-interest = 0.671 (MSV = 0.320), permeability = 0.652 (MSV = 0.171), and the selective disclosure = 0.676 (MSV = 0.086).

The discriminant validity was determined by comparing the AVE estimate of a construct and the highest associated constructs' squared inter-construct correlation. The notion is that a construct has discriminant validity if the AVE is greater than its highest associated squared inter-construct correlation (Boss et al., 2009; Hair et al., 2011; Paswan 2009; Smith et al., 1996). The AVE for each construct presented in Table 23 is greater, with good margins, than the construct's associated squared inter-construct correlation in Table 24, which is indicative of very strong discriminant validity.

Table 24. The Squared Inter-Construct Correlation

Correlations: (Group number 1 - Default model)

			Inter-construct Correlation (IC)	**Squared Inter-Construct Correlation (SIC)**
			Estimate	
Desired State	<-->	self Interest	0.07672	0.006
Desired State	<-->	Permeability	0.41397	0.171
Desired State	<-->	Equipoise	-0.09831	0.010
Desired State	<-->	Selective Disclosure	0.17488	0.031
Self Interest	<-->	Permeability	-0.09927	0.010
Self Interest	<-->	Equipoise	0.56566	0.320
Self-Interest	<-->	Selective Disclosure	0.19278	0.037
Permeability	<-->	Equipoise	-0.14093	0.020
Permeability	<-->	Selective Disclosure	0.10620	0.011
Equipoise	<-->	Selective Disclosure	0.29374	0.086

4.2.3.3 Structural equation model.

The structural equation modeling was used to test the structural model of the study. First, the study presented the final hypothesized structural model and its goodness-of-fit. Secondly, the moderation and mediation effects of the hypothesized model were tested. Finally, the hypotheses were evaluated and the final theory of the study was articulated.

Figure 8 presents the final structure of the hypothesized model. The structural model has one independent variable (the desired state of information privacy), two moderator variables (the information privacy self-interest and the information privacy permeability), one mediator variable (the information privacy equipoise), and one dependent variable (the selective personal information disclosure). In summation, the model has 20 endogenous variables (16 observed indicators and four (4) unobserved constructs: self-interest, permeability, equipoise, and selective disclosure), and 21 unobserved exogenous variables (the desired state of information privacy construct and the 20 measurement errors). The five-step recommendation (Bollen & Long, 1993) in the application of SEM were followed: model specification, identification, estimation, testing of fit, and re-specification.

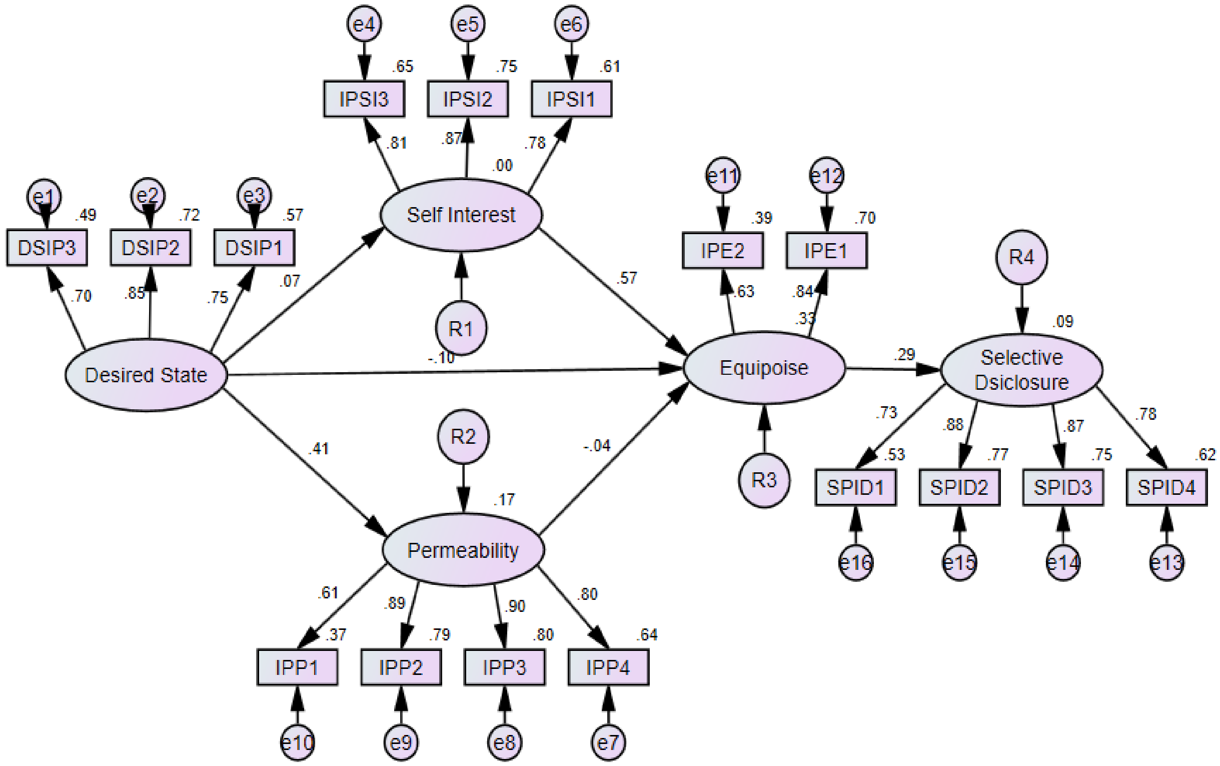


Figure 8. The Hypothesized Structural Model for the Study

The detail result of the statistical relationships of the hypothesized model is in the excerpt of the regression weights in Table 25.

Table 25. Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P
Self Interest	<---	Desired State	.07662	.09826	.77970	.43557
Permeability	<---	Desired State	.37612	.07901	4.76030	***
Equipoise	<---	Desired State	-.08124	.07791	-1.04276	.29706
Equipoise	<---	Permeability	-.03325	.07724	-.43047	.66686
Equipoise	<---	Self Interest	.39398	.07612	5.17554	***
Selective Disclosure	<---	Equipoise	.42957	.12985	3.30833	***

Sig. ****p* $\leq$ *.001*

The information in the table indicates that the regression weight for the desired state in the prediction of the permeability is statistically significant (different from zero) at p-value 0.001, two-tailed. However, the regression weight for the desired state in the prediction of the self-interest or the equipoise is not statistically significant (not different from zero) at 0.05 level, two-tailed. In addition, the regression weight for the self-interest in the prediction of the equipoise is statistically significant at 0.001 level, two-tailed, and the regression weight for the equipoise in the prediction of the selective disclosure is statistically significant at 0.001 level, two-tailed, as well. The standardized estimate of the model is in Appendix J.

Table 26. The Goodness-of-Fit Index for the Structural Model

Fit Index	Threshold	Study
Absolute Fit Measures		
Relative Chi-square (χ^2/df)	< 5	1.800
GFI	≥ 0.90	0.907
AGFI	≥ 0.90	0.872
RMSEA	≤ 0.08	0.063
SRMR	≤ 0.10	0.164
Incremental Fit Measures		
CFI	< 0.95	0.951
NNFI (TLI)	≥ 0.95	0.939
NFI	≥ 0.90	0.897
Parsimonious Fit Measures		
PNFI	≥ 0.50	0.732
PCFI	≥ 0.50	0.776

Table 26 is the presentation of the goodness-of-fit for the structural model. The overall goodness-of-fit, using the relative chi-square (χ^2/df—176.41/98), was 1.800, indicative of an excellent fit. In addition, the AGI = 0.907, AGFI = 0.872, RMSEA = 0.063, SRMR = 0.164, CFI = 0.951, TLI = 0.939, NFI = 0.897, PNFI = 0.732, and the PCFI = 0.776.

4.2.3.4 Analysis of the hypotheses.

Rather than analyze the causal effects or the effects of the mediation and moderation variables in isolation or in silos, the belief was that it makes a better sense to analyze the causal, mediating, and moderation effects among the latent variable within the context of the hypotheses. Therefore, this section is an evaluation of the hypotheses based on the research methodology suggested in Chapter 3.

The study was concerned with four hypotheses. The first hypothesis (H_1) was concerned with the evaluation of the causal effect of the desired state information privacy in the prediction of the information privacy equipoise. The second and the third hypotheses (H_2 and H_3) were to measure the moderation effect of the information privacy self-interest and information privacy permeability on the relationship between the desired state of information privacy and the information privacy equipoise. Finally, the fourth hypothesis (H_4) was a measurement of the mediation effect of the information privacy equipoise on the relationship between the desired state of information privacy and the consumers' selective personal information disclosures.

For H_1, the following is the proposed hypothesis:

> *H_1: A consumer's desired state of information privacy has a causal relationship with the consumer's information privacy equipoise.*

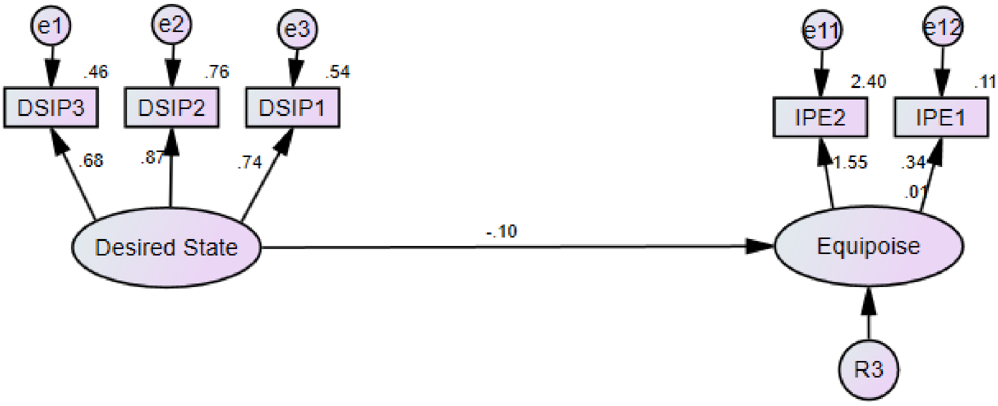


Figure 9. Standardized Effect of the Desired State on the Equipoise

The regression weight for the desired state in the prediction of equipoise is statistically significant from zero at 0.05, two-tailed, with *p-value* = 0.038. In the standardized regression weight estimate, when the desired state goes up by 1.0 standard deviation, the equipoise goes down by 0.103, and in the unstandardized regression weight estimate, when the desired state goes up by 1.0, the equipoise goes down by 0.214 (see Appendix J). Therefore, H_1 is supported. In addition, the structural model in Figure 9 has an excellent fit. The relative chi-square (χ^2/df) is 0.195, GFI = 0.998, AGFI = 0.994, RMSEA = 0.000, SRMR = 0.022, TLI = 1.031, CFI = 1.000, NFI = 0.997, PNFI = 0.399, and the PCFI = 0.400.

4.2.3.4.1 Moderation.

The following is the result of the tests for moderation of the information privacy self-interest and information privacy permeability variables on the relationship between the desired state of information privacy and the information privacy equipoise.

For the information privacy self-interest:

> *H_2: A consumer's information privacy self-interest moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.*

Following the moderation test strategy described in Chapter 3 and *Equation 2*, the structural model in Figure 10 provides an illustration of the result of the test for the moderation effect of the information privacy self-interest on the relationship between the desired state of information privacy and the information privacy equipoise. The structural model has an excellent fit because the relative chi-square was 1.619, SRMR = 0.016, GFI = 0.998, AGFI = 0.981, CFI = 1.000, TLI = 1.006, NFI = 0.998, RMSEA = 0.000, and the PNFI = 0.200.

The H_2 is supported because the regression weight for the product of the coefficient of the desired state and the self-interest, DSIP x IPSI, in the prediction of the equipoise is statistically significant from zero at the 0.05, two-tailed, with *p-value* = 0.018. Furthermore, the desired state of information privacy is statistically significant in the prediction of the selective disclosure at 0.01, two-tailed, with *p-value* = 0.005. Besides, the regression weight of the self-interest is statistically significant in the prediction of the equipoise with *p-value* = 0.001, and the equipoise is statistically significant in the positive prediction of the selective disclosure with *p-value* = 0.001.

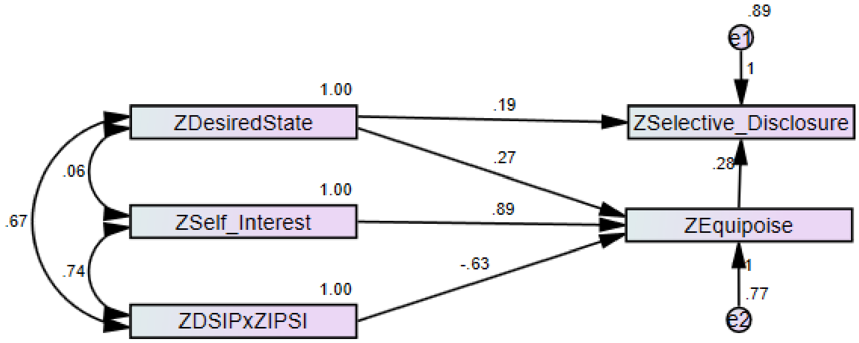


Figure 10. The Moderation Effect of the Self-Interest

From another perspective using the linear regression in the SPSS software, the interaction between the desired state, self-interest, and the product of DSIP and IPSI (see

Table 27, Model 2) accounted significantly more variance than the desired state and self-interest by themselves, where R = .452 in Model 1 changed to R = .475 in Model 2; R^2 changed from .204 to .022; and *p*-value in both models equal to .000 and .020 respectively.

Table 27. Self Interest Moderation Model Summary

				Std. Error	Change Statistics				
		R	Adjusted R	of the	R Square	F			Sig. F
Model	R	Square	Square	Estimate	Change	Change	df1	df2	Change
1	.452[a]	.204	.196	2.30926	.204	25.403	2	198	.000
2	.475[b]	.226	.214	2.28352	.022	5.489	1	197	.020

a. Predictors: (Constant), SelfInterest, DesiredState

b. Predictors: (Constant), SelfInterest, DesiredState, DSIPxIPSI

Hence, based on *Equation 3*, the β_0 = 3.0, β_1DSIP = .27, β_2IPSI = .89, β_3(DSIP)(IPP) = -.63, and *e* = .77. The implication is that when the coefficient β_3(DSIP)(IPSI) goes up by 1.0, the equipoise goes down by 0.634. The effects of the β_3(DSIP)(IPSI) are that it has a direct effect of -.634 on the equipoise and indirect effect of -.178 on the selective disclosure, which means that *the self-interest diminishes the positive relationship between the desired state of information privacy and the information privacy equipoise*—see Figure 11 (Dawson, 2016).

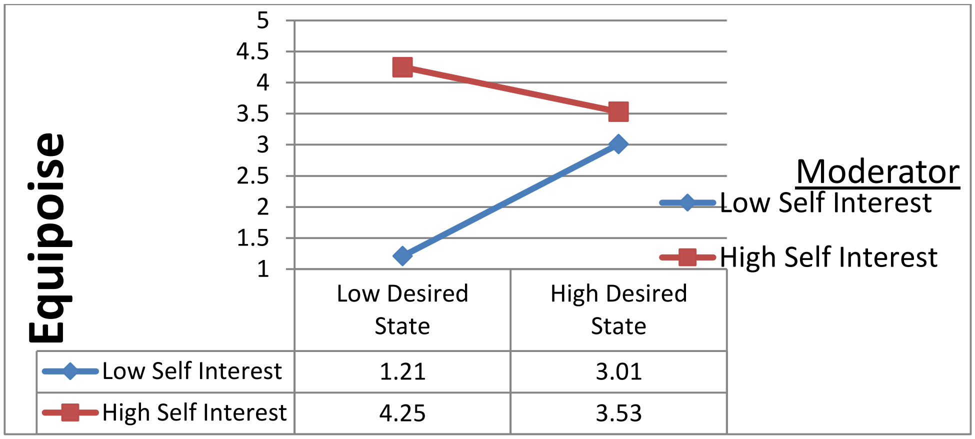


Figure 11. The Desired State and Self-Interest Interaction Effect on Equipoise

This result is consistent with the proposed phenomenon of the information privacy equipoise espoused in the theoretical model and in Table 5 because a high degree of self-interest will soften the information privacy equipoise of someone who is in the reserve or solitude desired state of information privacy.

For the information privacy permeability:

> *H_3: A consumer's information privacy permeability moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.*

The structural model in Figure 12 provides a depiction of the result of the test for the moderation effect of the information privacy permeability on the relationship between the desired state of information privacy and the information privacy equipoise. The structural model has an excellent fit as well because the relative chi-square was 0.315, SRMR = 0.009, GFI = 0.999, AGFI = 0.990, CFI = 1.000, TLI = 1.008, NFI = 0.999, RMSEA = 0.000, and the PNFI =0.200.

Although the model in Figure 12 has an excellent fit, H_3 is not supported because the regression weight for the coefficient β_3 (DSIP x IPP) in the prediction of the equipoise is not statistically significant from zero at the 0.05, two-tailed, with *p-value* = 0.718. However, the desired state of information privacy was statistically significant in the positive prediction of the selective disclosure at 0.01 level with *p-value* = .005. In addition, the regression weight of the equipoise is significant in the positive prediction of the selective personal information disclosure with *p-value* = 0.001.

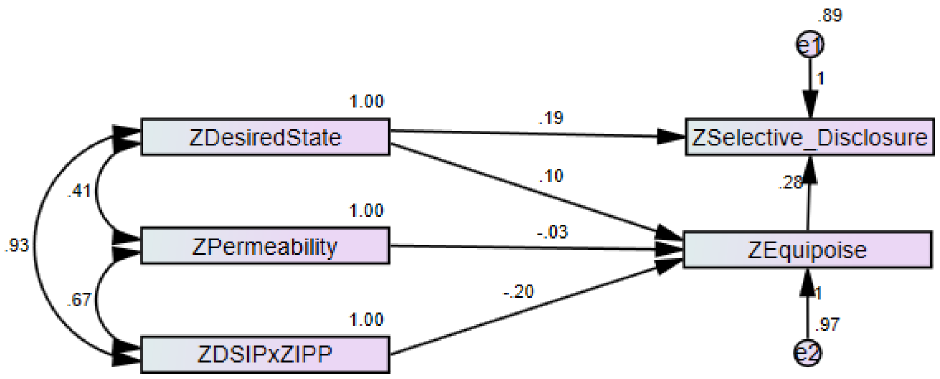


Figure 12. The Moderation Effect of Permeability

The implication of the effect, nonetheless, is that when the coefficient β_3(DSIP)(IPP) goes up by 1.0, the information privacy equipoise goes down by 0.201, and the selective disclosure goes down by 0.056. This means that the β_3(DSIP)(IPP) has a direct effect of -.201 on the information privacy equipoise and indirect effect of -.056 on the selective personal information disclosure, despite its statistical insignificance.

The test for the interaction manifested similar result. The interaction between the desired state, permeability, and the product of DSIP and IPP (Table 28) also did not account significantly more variance than the desired state and permeability by themselves, where R = .140 and .143; R^2 change = .020 and .001; and *p* = .140 and .721 in Model 1 and Model 2 respectively.

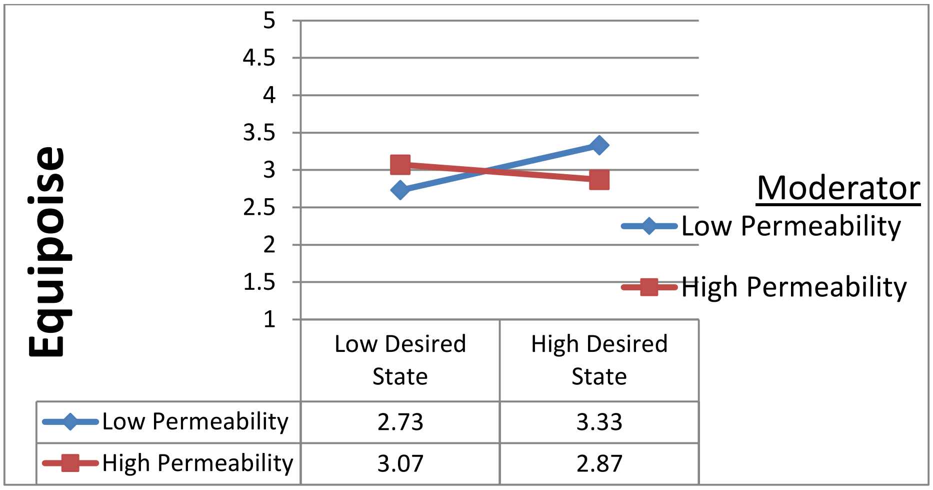
Table 28. Permeability Moderation Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.140[a]	.020	.010	2.56302	.020	1.989	2	198	.140
2	.143[b]	.020	.005	2.56869	.001	.128	1	197	.721

a. Predictors: (Constant), Permeability, DesiredState

b. Predictors: (Constant), Permeability, DesiredState, DSIPxIPP

Based on *Equation 3*, The β_0 = 3.0, β_1DSIP = 0.10, β_2IPP = -.03, β_3(DSIP)(IPP) = -.20, and e = .97. Therefore, although the coefficient β_3 is not statistically significant, *the result indicates that permeability, to some degree, dampens the positive relationship between the desired state of information privacy and the information privacy equipoise*—see Figure 13 (Dawson, 2016).



	Low Desired State	High Desired State
Low Permeability	2.73	3.33
High Permeability	3.07	2.87

Figure 13. The Desired State and Permeability Interaction Effect on Equipoise

4.2.3.4.2 Mediation.

H4: A consumer's information privacy equipoise is positively related to the consumer's selective personal information disclosure behaviors online.

The mediation test strategy for the study, including the step-by-step approach proposed for this study was specified in Table 9, Chapter 3. In the table, Step 1 is the test of the relationship between the independent (DSIP) variable and dependent variable (SPID). In addition, the proposal in Figure 5 path coefficient (β): *c*, was to conduct a simple regression analysis, in which DISP would predict SPID.

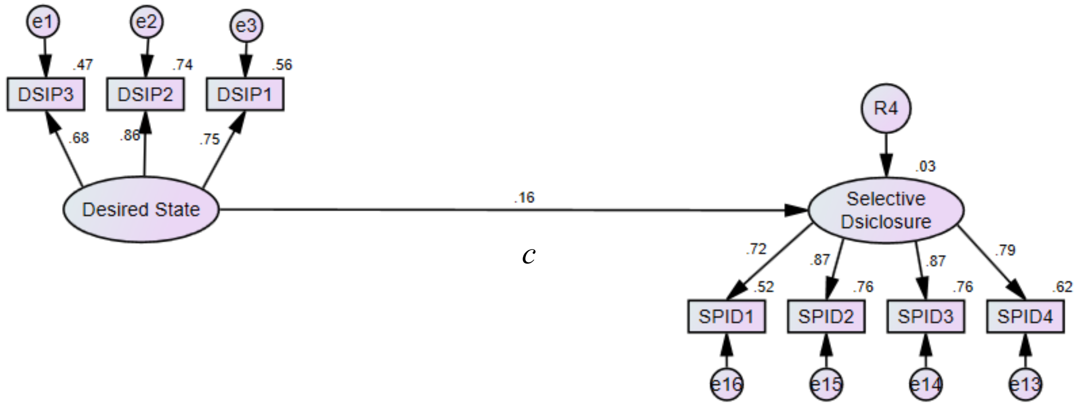


Figure 14. Standardized Mediation Model Path Coefficient (*β*): *c*

The result indicates that the regression weight for the desired state of information privacy in predicting the selective personal information disclosure, without any moderation or mediation, is not statistically significant but is relatively high, where *selective disclosure <--- desired state* standardized regression estimate is 0.16 and *p-value* = .056 in a two-tailed test in which the alpha was set at 0.05. However, the goodness of fit for the SEM model expressed in Figure 14 is acceptable because the relative chi-square (χ^2/df) is 3.022, GFI = 0.952, AGFI = 0.897, RMSEA = 0.101, SRMR = 0.117, TLI =0.937, CFI = 0.961, NFI = 0.944, PNFI = 0.584, and PCFI = 595. Although the relationship was not significant there is a high degree of correlation because the direct effect for the desired state on the selective disclosure is 0.16, which means that an increase to the desired state by 1.0 standard deviation will cause an increase to the selective disclosure by 0.16 standard deviation.

In addition, based on the test proposal in the Table 9, the following relationships for mediation were tested as presented in Figure 15. Reference to Figure 5:

Step 2. Path coefficient (*β*): *a*, a simple regression analysis was conducted in which the relationship between DSIP (desired state) and IPE (equipoise) was tested.

Step 3. Path coefficient (*β*): *b*, a simple regression analysis was conducted in which the relationship between IPE (equipoise) and SPID (selective disclosure) was tested.

Step 4. Path coefficient (*β*): *ć*, a multiple regression analysis was conducted to show that DISP and IPE would predict SPID.

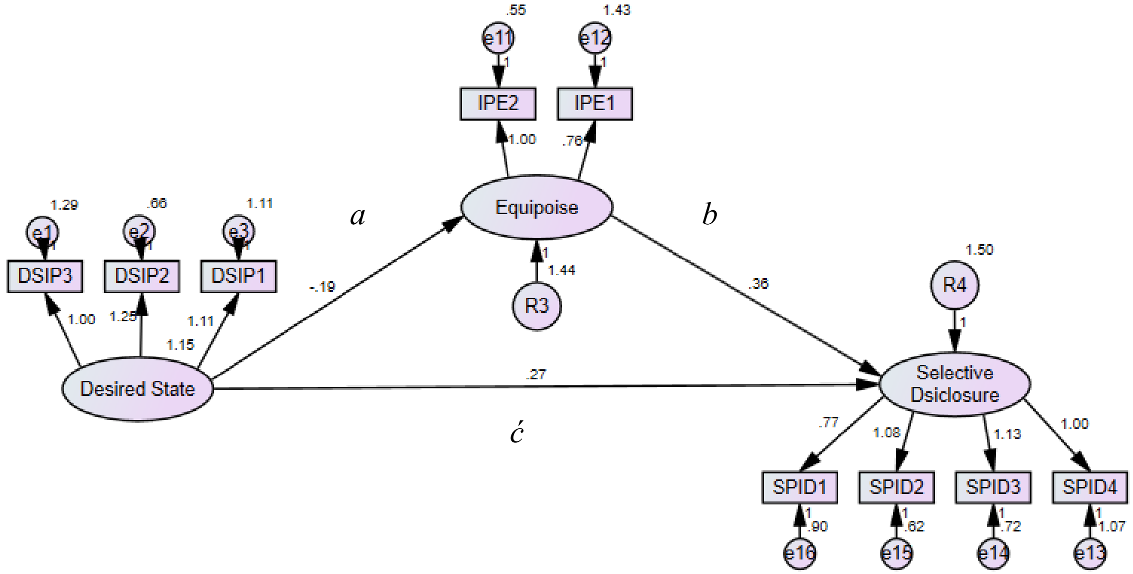


Figure 15. Mediation Model Path Coefficients (*β*): *a, b,* and *ć*

The goodness-of-fit for the mediation model was strong because the relative chi-square (χ^2/df) is 1.928, GFI = 0.955, AGFI = 0.916, RMSEA = 0.068, SRMR = 0.108, TLI =0.956, CFI = 0.970, NFI = 0.941, PCFI = 0.628, and the PNFI = 0.647. The result of the two-tailed regression test (see Table 29) indicated that the regression weight for the desired state in the prediction of equipoise (Equipoise <--- Desired State) is not statistically significant with *p* = 0.081 at 0.05 level. Note the difference between the *p*-values in Figure 14 and 15—and increase in *p-value* 0.056 to 0.081. Notwithstanding, the regression weight for the information privacy equipoise in predicting the selective personal information disclosure is significant with *p* = 0.007 at 0.01 level (see Selective

Disclosure <--- Equipoise in Table 29). In addition, the desired state is statistically significant at .01 level, with *p* = 0.010, in the prediction of the selective disclosure when mediation is in effect. The standardized mediation model path coefficients (*β*): a, b, and ć is in Appendix J.

Table 29. Regression Weights: (Group number 1 - Default model) Mediation

			Estimate	S.E.	C.R.	P	**Path (β)**
Equipoise	<---	Desired State	-.18767	.10750	-1.74586	.08083	*a*
Selective Disclosure	<---	Equipoise	.36491	.13530	2.69699	.00700*	*b*
Selective Disclosure	<---	Desired State	.26805	.10368	2.58524	.00973*	*ć*

For the path coefficient (*β*) *a*, the direct (unmediated) effect of the desired state on the equipoise is -.188 and the indirect (mediated) effect of the desired state on the equipoise is 0.00. Hence, the total (direct and indirect) effect of the desired state on the equipoise is -.188, which means that when the desired state goes up by 1.0, the equipoise goes down by 0.188 (Kline, 1998, p. 52).

For the path coefficient (*β*) *b*, the direct effect of the equipoise on the selective disclosure is 0.365 and the indirect effect is 0.00. Therefore, the total effect of the equipoise on the selective disclosure is 0.365, which means that when the equipoise goes up by 1.0, the selective disclosure will go up by 0.36491.

For the path coefficient (*β*) *ć*, the direct effect of the desired state on the selective disclosure is 0.268 and the indirect effect of the desired state on the selective disclosure is -.068. Hence, the total effect of the desired state to the selective disclosure is 0.20 (unmediated + mediated effect), which means that an increase by 1.0 in the desired state will cause an increase to the selective disclosure by 0.20 (see unstandardized mediation model in Appendix J).

This observation in the data is consistence with the expectations of the study because an increase in the desired state will increase a consumer’s concern, as such will cause an increase in the consumer’s selective disclosure of personal information. Based on this mediation analysis and the regression weight estimates in Table 29, the information privacy equipoise has partial mediation on the relationship between the desired state of information privacy and the selective personal information disclosure. Therefore, H_4 is supported.

4.3 Findings

The followings are the findings in this study. The remarks on whether the data supported the proposed hypotheses or not are presented in Table 30.

For H_1, a consumer’s desired state of information privacy was found to have a causal relationship with the consumer’s information privacy equipoise because the regression weight for the desired state in the prediction of the equipoise is statistically significant from zero at the 0.05 two-tailed level with *p-value* = 0.038. Based on the data and a look at the two extremes of the desired state of information privacy, the notion that a consumer who is in the desired state of intimacy will likely reach the information privacy equipoise state and disclose his or her personal information even when there is a high or low information privacy self-interest or permeability is supported. Conversely, a consumer who is in the desired state of solitude will, most likely, not reach the information privacy equipoise and will not disclose personal information unless his or her information privacy self-interest (need signal) is high and he or she has some sense of low information privacy permeability.

Table 30. The Research Hypotheses Result

	Hypothesis	Remark
H_1	A consumer's desired state of information privacy has a causal relationship with the consumer's information privacy equipoise.	Supported
H_2	A consumer's information privacy self-interest moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.	Supported
H_3	A consumer's information privacy permeability moderates the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise.	Not supported
H_4	A consumer's information privacy equipoise is positively related to the consumer's selective personal information disclosure behaviors online.	Supported

For H_2, a consumer's information privacy self-interest was found to have moderated the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise. Using a standardized data for the regression test, the regression weight for the product of the desired state of information privacy and the information privacy self-interest (DSIP x IPSI) indicated that the capacity of the coefficient β_3 in the prediction of the information privacy equipoise is statistically significant from zero at the 0.05 two-tailed level with *p-value* = 0.018. This result was validated with the linear regression test, using the SPSS software, in which the *R* changed from .452 to .475 and $R^{2\ change}$ changed from .204 to .022, with p = .000 and .020 respectively, when the predictors, desired state and self-interest, were tested by themselves and when they were tested in conjunction with the product of the desired state and the self-interest (DSIP x IPSI).

For H_3, a consumer's information privacy permeability was found not to be statistically significant in moderating the relationship between the consumer's desired state of information privacy and his or her information privacy equipoise. The regression weight for the coefficient β_3(DSIP x IPP) in the prediction of the equipoise is not statistically significant from zero at the 0.05 two-tailed level with *p-value* = 0.718. In addition, in the linear regression test, the change in *R* from .140 to .143 and $R^{2\ change}$ from .020 to .001 was not statistically significant with *p* = .140 and .721 respectively.

However, the study also found that the information privacy permeability has a direct (unmediated) effect of -.032 to the information privacy equipoise and an indirect (mediated) effect of -.009 on the selective disclosure of personal information. This means that an increase by 1.0 in the permeability will cause a decrease by 0.032 to the equipoise and a decrease by 0.009 to the selective disclosure. In addition, the regression weight for the desired state in the prediction of the permeability is significantly different from zero at 0.001 two-tailed level. Therefore, based on the aforementioned, the construct of the information privacy permeability was not supported in the prediction of equipoise (also see Table 25).

For H_4, a consumer's information privacy equipoise was found to positively related to the consumer's selective personal information disclosure behaviors online. In other words, there is a partial mediation (see Table 11) of the effects as previously discussed. The path coefficient (β) *ć* and path coefficient (β) *b* were statistically significant with *p* = .010 and *p* = .007 respectively at .01 two-tailed level and path coefficient (β) *a* was not significant at *p* = .081 at .05 two-tailed level (see Table 29).

Furthermore, the study found that the data is consistent with the information privacy equipoise scheme presented in Table 31.

Table 31. The Information Privacy Equipoise Scheme

Desired State of Privacy	Privacy Self-Interest	Privacy Permeability	Information Privacy Equipoise	
			Yes	No
Intimacy	High (open)	High	X	
	High (open)	Low	X	
	Low (close)	High	X	
	Low (close)	Low	X	
Anonymity	High (open)	High	X	
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low		X
Reserve	High (open)	High		X
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low	X	
Solitude	High (open)	High		X
	High (open)	Low	X	
	Low (close)	High		X
	Low (close)	Low		X

Although the moderation effect of information privacy permeability was not statistically significant, permeability has a direct (unmediated) effect of -.032 to the information privacy equipoise and an indirect (mediated) effect of -.009 on the selective disclosure of personal information. In addition, the regression weight for the desired state in the prediction of permeability is statistically significant with *p-value* = 0.001 (see Table 25).

Based on the data and the scheme, the followings are the inferences drawn from the study. Generally, a consumer in an intimacy state will most likely reach information privacy equipoise, transact online, and disclose his or her personal information regardless of whether he or she has a high or low privacy self-interest and/or a high or low information privacy permeability. Secondly, a consumer in the anonymity state will reach information privacy equipoise, transact, and disclose personal information online when the self-interest is high, irrespective of whether the privacy permeability is high or low because the consumer's sense of anonymity seems to lessen the consumer's permeability concerns. In a computer-mediated communication, Joinson (2001) found that in a dilemma discussion, dyads disclosed more information about themselves when they were visually anonymous than when they were not.

Furthermore, a consumer in the reserve state is pragmatic, as such will reach privacy information equipoise, transact, and disclose personal information online when the information privacy permeability is low, regardless of whether the information privacy self-interest is high or low. Finally, a consumer in the solitude state will reach information privacy equipoise, transact, and disclose personal information online when the privacy the information privacy self-interest is high and the information privacy permeability is low. Therefore, the fact that any consumer could be in any of the three states (intimacy, reserve, and solitude), and in the anonymity state at the same time could explain why the construct of the information privacy permeability is statistically insignificant because the permeability effect may have been baked in (see Table 32).

The SPSS software *compute variable* was used to sum up each case in the data in order to estimate and categorize the desired state. Upon the summation, the *frequencies* in the descriptive statistics was used to analyze the result. The dispersion or distribution was between minimum = 3.0 and maximum = 21 as presented in Table 32. The study used a 7-point Likert scale and the following items, DSIP1, DSIP2, and DSIP3 (see Appendix A), for the assessment of the desired state. The response from the item, DSIP4 (usually, I believe in concealing my personal information, to the maximum extent possible, when transacting online), was used to estimate the anonymity state.

Table 32. The Taxonomy of the Desired State of information Privacy

Desired State			Compute Value*	Frequency	Valid Percent	Cumulative Percent
**** Anonymity**	5%	**Intimacy** 10.5%	3.00	1	0.5	0.5
			5.00	4	2.0	2.5
			6.00	9	4.5	7.0
	36%		7.00	7	3.5	**10.45**
		Reserve 73.1%	8.00	6	3.0	13.4
			9.00	8	4.0	17.4
			10.00	15	7.5	24.9
			11.00	17	8.5	33.3
			12.00	26	12.9	46.3
			13.00	13	6.5	52.7
			14.00	18	9.0	61.7
			15.00	22	10.9	72.6
			16.00	6	3.0	75.6
			17.00	16	8.0	**83.58**
		Solitude 16.4%	18.00	16	8.0	91.5
	59%		19.00	6	3.0	94.5
			20.00	4	2.0	96.5
			21.00	7	3.5	**100.00**
100%			Total	201	100.0	

*Compute values for the desired state based on numeric transformations of three observed variables (DSIP1, DSIP2, and DSIP3) for the intimacy, reserve, and solitude (see Appendix L).
** Used DSIP4 to calculate the anonymity.

Based on the 201 valid responses for the study and the calculation in Appendix L, 10.5% of the data from the sample subjects were classified as the intimacy, 73.1% as the reserve, and 16.4% as the solitude, as presented in Table 32. The anonymity cut across all other states. The responses from the 7-point Likert scale were used to estimate the percentages of the anonymity state associated with each state proportionally (see detail in Appendix L). The indication was that although 16.4 percent of all the respondents were in the solitude state naturally, 59% of them would transact online anonymously. Likewise, although 73.1% were in the reserve state, only 36% of them would transact anonymously. In addition, only 5% of the 10.5% who were in the intimacy state would transact anonymously.

4.4 Summary

The chapter followed and presented the three-phase data collection and analysis approaches presented in Chapter 3. Therefore, this chapter was organized chronologically as follows: the expert panel data collection and analysis, the pilot study data collection and analysis, and the final data collection and analysis, including the data reliability and the construct validity assessments.

In the first phase, the substantive validity analysis and the content validity ratio were used in ensuring content validity. The survey instruments were sent to a 15-member expert judges on two occasions for the substantive validity analysis and the content validity ratio, which helped in the refinement of the instrument prior to its administration to the pilot test sample subjects. The goal of the substantive validity analysis was to ensure that proper definitions were obtained for the operationalized items. On the other hand, the goal of the content validity ratio was to ensure the adequacy of the items' reflection on their target latent variables or constructs.

The result of the substantive validity analysis led to the revision of some of the items for clarity, accuracy, and relevance. The revision involved the removal of four questions and the succinctness of the remaining items. The content validity ratio survey allowed the study to identify the items in which over 50% of the panelist deemed as essential to a construct. It also facilitated the changes to the newly developed and modified items. Finally, the result of the content validity ratio was instrumental in finalizing the instrument for the Pilot Test.

The second phase comprised of the administration of the survey instrument for the pilot study, the receipt of the data, and the analysis of the data. The EFA and PCA were conducted in this phase furtherance to the data refinement objective. The EFA was used in validating the observed variables by ensuring that the latent variables were well-reflected in their associated observed variables. The PCA was used in the grouping of the data to manageable units in order to avoiding the issue of multicollinearity and in detecting patterns in the data. The use of a pilot test as a primary test to try out a research approach or discover problems in a research study for corrections or adjustments is prevalent in the extant literature (John et al., 2011; Randolph, 2009; Vogt & Johnson, 2016). The overall result of the pilot test was good, acceptable, and indicative, as such, the study proceeded with the final data collection.

In the final data collection and analysis, the CFA, including the construct reliability and validity were estimated for the hypothesized model, and the SEM was used to assess the structural and the measurement model. The tests for moderation and mediation were also performed in this phase. Finally, the research findings for the study were delineated.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

5.1 Introduction

This chapter presents the conclusions of the study, the implications of the study for practitioners and researchers, the limitations, the recommendations for future studies, and the overarching summary of the study.

5.2 Conclusions

The theory of this study is that the consumers' willingness to transact online and disclose their personal information depend largely on the degree of their need signal (self-interest), and to some extent, their awareness and concern of the online merchant's capacity to collect their personal information, irrespective of their previously declared or undeclared intent to transact and disclose personal information, or despite their desired natural state of information privacy (see Table 28). A consumer's intention to disclose his or her personal information online depends on the person's natural or desired state of information privacy, whereas the customer's actual personal information disclosure behavior depends on his or her information privacy equipoise or the compromised state of information privacy.

The goal of this study in examining the information privacy paradox from cognitive predisposition perspective based on the theoretical framework of the privacy regulation theory, in order to add a novel perspective to the body of knowledge, was met. The extant literature on the phenomenon of the information privacy paradox had assumed that the consumers are always rational when dealing with the notion of personal information disclosure online. The thesis of this study is that the consumers are sometimes rational, but at other times irrational in their decision to disclose personal information online.

Grounded on the aforementioned thesis, the study developed the constructs of the desired state of information privacy, information privacy self-interest, information privacy permeability, and the information privacy equipoise based on the principles of the privacy regulation theory, including the taxonomy of the self, to examine the information privacy paradox from cognitive predisposition perspective. The principles in the privacy regulation theory are the access to the self, the dynamic dialectic process, the multimodal or multi-mechanism process, and the optimization process. The taxonomy of the self deals with the grouping of people based on their natural information privacy posture or their natural (desired) state of information privacy.

Empirical evidence in this study showed that a person's information privacy equipoise is predictable based on the person's natural information privacy posture. In addition, there is evidence that a person in the information privacy equipoise will be willing to disclose his or her personal information online. More importantly, the selective disclosure occurs because being in the desired or natural state of the information privacy posture is static in nature, while being in the information privacy equipoise posture or in a compromised state is dynamic in nature. The information privacy equipoise is dynamic because an individual would reach the compromised level of information privacy (equipoise) at a given time and in a given circumstance when the person has no need for more or less information privacy resulting from the moderating effects of the information privacy self-interest and permeability.

The information privacy self-interest and permeability are the two moderating variables in the study. There is evidence that the self-interest is critical to whether a person transacts and discloses his or her personal information online or not. On the other hand, although there is evidence that the permeability has some influence on whether individuals disclose their personal information online or not, it is not a determinant because it's influence was not statistically significant.

The study identified and defined the instance in time in which individuals transition from thinking about transacting online to the time the person actually transacts, or not transact, as a gain or loss of one unit of information privacy equipoise respectively. This means that a person who has gained a unit of information privacy equipoise, within the context, will proceed with the online transaction and will disclosure personal information, whereas a person who has not attained or archived a unit of information privacy equipoise will not transact online at that moment, and may seek an alternative means of satisfying the need in order not to disclose personal information. This supposition is consistent with the data and with the assumption of the optimization process inherent in the privacy regulation theory. Empirical evidence in this study showed that information privacy equipoise has a positive relationship with the consumers' selective personal information disclosure online.

Therefore, based on the result of this study, the argument that a consumer's discriminant or selective willingness to disclose personal information when transacting online is based on cognitive predispositions has been substantiated through a quantitative examination. The result demonstrated that a consumer's information privacy predisposition effects the consumer's information privacy paradox. The outcome of this study illustrated the dynamism among the constructs of the consumers' desired stated of information privacy, information privacy self-interest, and information privacy permeability in relation to the information privacy equipoise, and the relationship between the information privacy equipoise and the consumers' selective information privacy disclosure behaviors.

5.3 Implications

This study provides researchers and practitioners evidence that the disparity between the consumers' intended and actual personal information disclosure behaviors online or the information privacy paradox is based on the consumers' cognitive predispositions as well.

5.3.1 For researchers.

This study shows evidence that the information privacy paradox is not only economic- or value-based, but cognitive predisposition-based as well. In addition, this study substantiated the Privacy Regulation Theory. Therefore, the study has advanced knowledge by providing a different logical and empirical evidence to information privacy paradox, and by constructing a theory or model, which has the fist-level constructs. According to Lee (2004), a social science theory must be consistence with the four Popper's natural science conditions of internal consistency demonstration, empirical testability, survival of attempts at empirical testing, and explanatory or predictive, as well as "account for the world of subjective meaning [of the] first-level constructs" (p. 9). The result of the research, including the theory and the model presented in this study is in line with the aforementioned conditions of the social science theory.

5.3.2 For practitioners.

The understanding of this phenomenon from cognitive predisposition perspective will help practitioners in restoring consumers' confidence in e-commerce, e-government, e-healthcare, and will help in organizations' *maximization of wealth* objectives. Better consumer confidence in the online marketplace environment can be established by the assurance of information privacy by online merchants, which will help in maximizing consumers' willingness to disclose personal information online.

Hence, organizations will understand consumers' information privacy concerns and tendencies better, which could propel them to limit their personal information requirements to those critical and essential for OLTP, limit information permeability, and communicate their collection procedures better to consumers in order to remove permeability completely as a consideration for online transaction participation. In addition, it will provide practitioners with the basis for better marketing campaigns by identifying, classifying, and targeting only those customers who have the propensities for online transactions and personal information disclosure.

5.4 Limitations

This section identified some integral and salient limitations, which could have threatened the result or the internal validity of this study. It also provided the measures the study took to mitigate the limitations. Limitations are factors outside the control of a researcher, which "provide a method to acknowledge possible errors or difficulties in interpreting results of the study" Baron (2008, p. 4). One of the significance of reporting limitations is that it allows a researcher to be self-aware and to minimize the severity of the limitations in the design and in the conduct of a study (Baron, 2008). Therefore, issues associated with the sampling method, data collection methods (Sekaran & Bougie, 2009), low response rate, lack of non-response feedback loop, completion rate, and possible response bias or lack of candor (Baron, 2008) were some of the limitations identified in this study.

Sampling method. This study used the convenient sampling technique. The data for this study were collected from subjects from three organizations and two social media forums. Convenient sampling involves the collection of data from a convenient and available sample subjects in a given population (Sekaran & Bougie, 2009). In addition, the unit of analysis for this study was individual, as such the sample subjects were individuals with autonomous thinking capacities in many respects. However, it is possible that certain common professional idiosyncrasies, objectives, or organizational culture may have likened some of the subjects' attitudes; consequently, made the generalizability of this study relative. Therefore, the study adopted a mix-mode sampling method, comprising of the convenient and cluster sampling, in which the study pulled the participants from available and accessible groups in multiple organizations.

Data collection method. The data for this study was collected through a Website. The link for the web address or uniform resource locator (URL) was sent to the participants via emails and were posted on the Websites. The use of the email or mail survey is deemed advantageous if the sample subjects are geographically dispersed; if the cost of obtaining the research data is a consideration; and if the number of the expected sample size is large (Maxim, 1999; Sekaran & Bougie, 2009). Nonetheless, mail survey has its limitations as well because it is characterized with very low response rates. In addition, there is potential for response bias, which has the potential of threatening the internal consistency of a study (Maxim, 1999; Sekaran & Bougie, 2009). Furthermore, a researcher would have limited or no control over the sample subjects' response time. In order to mitigate the response rate issue, the study sent the survey link through the survey champions in the slated organizations. A survey champion is an influential and/or a respected advocate of a researcher's study in an organization, social media network or otherwise. In addition, the study addressed the issue of the low response rate by developing and applying an effective reminder strategy that encouraged respondents to complete the survey without having a sense of annoyance or inconvenience. Another mitigation measure was to send a cover page with the survey, which explained the intent and the objective of the study, including the need for an accurate and complete response. Finally, the study sent the pre-mail notices of incoming survey to the participants as necessary.

Nonresponse bias. The issue of nonresponse bias was given adequate consideration in this study. Meanwhile, there is not a well-defined feedback loop mechanism, the study was aware of, which explained why some participants failed to respond to the survey or why they provided incomplete responses. A nonresponse bias is a consequence of a participant not responding to a survey at all, or failing to complete a survey entirely because of his or her objection to certain questions (Maxim, 1999). To mitigate this limitation, the study followed the recommendations espoused in Moattar (2014), which were choose an appropriate sample frame, make the survey instrument concise and brief, design a good-looking survey, allow participants access to the survey from any Internet capable device, and resurvey the non-respondents if necessary. A sample frame is "the population that has a chance to be selected" (Girden & Kabacoff, 2011, pp. 67-68) or "your accessible population, which might be different from your target population" (Vogt & Johnson, p. 394), or "a physical representation of all the elements in the population from which the sample is drawn" (Sekaran & Bougie, 2009, p. 267).

5.5 Recommendations

This study is one of the few that have examined the information privacy paradox from the cognitive perspective based on the review of extant literature, and the first examination from the cognitive predisposition prism. Hence, future research should replicate the study or advance other theories because research work on the linkages or the reasons why the paradox exists has not been exhaustive.

In the extant literature, evidence shows that information privacy intention is a poorly prediction of the actual behavior (Keith et al., 2013), yet the conventional wisdom or anecdotal evidence is that the information privacy intention is predictive of the actual information privacy disclosure. Therefore, future studies should examine if there is an inverse relationship between the two, which means that future research should examine whether the actual information privacy disclosure would predict the information privacy intentions.

5.6 Summary

Organization are unable to project or assess consumers' actual willingness to disclosure personal information in e-commerce even though consumers' personal information is the cornerstone for an effective e-commerce, e-healthcare, or e-government activities today. One of the reasons for the inability to project personal information disclosure is the existence of information privacy paradox. Therefore, this study was an empirical examination of the antecedents to the paradoxical changes in the consumers' intended and actual personal information disclosure in online transactions or in an e-commerce environment from cognitive predisposition perspective, with emphasis on mindsets and perceptions rather than on reasoning and judgement. The focus of this study was on the cognitive mindset and perception because privacy calculus had focused on the cognitive reasoning and judgment.

An extensive review of the extant literature was undertaken. The concept of the value of information was used to assess the potency of conducting this study on the phenomenon of information privacy paradox. The review helped the study in estimating known facts and assumptions, and involved the evaluation of the research articles and books in various dimensions of the general privacy and information privacy. The study appraised the literature, which dealt with the information privacy paradox, privacy calculus, information privacy concerns, risks and trust, regulation, personal information collection, use, and storage, and the personal information as an obligatory passage point.

Furthermore, the theoretical conceptualization and modelling of the consumers' selective personnel information disclosure was articulate based on the privacy regulation theory. In addition, the study developed the information privacy constructs and the hypotheses. The study also advanced the hypothesized model, and discussed the research strategy or approach, which involved the research design (quantitative analysis), instrument development and validation, measurement of the constructs, data collection, and the data analysis. The empirical validations, reliability, content validity, and construct validity, including the limitations were also addressed.

The data collection and analysis was broken down into three stages. The first stage described the result of the data collected from the expert panelists who validated the survey instrument. The content validation in the first stage was completed through the application of the *substantive validity analysis* and the c*ontent validity ratio*. A pilot study was undertaken in the second stage. During the second stage, the EFA and PCA were conducted and further refinement of the instrument was attained. The third stage was a complete presentation of the final result of the data collection, analysis, validation, and interpretation.

The outcome of this study can be summarized as follows: consumers' willingness to transact online and disclose their personal information depend largely on the degree of their need signal (self-interest), and to some extent, their awareness and concern of the online merchant's capacity to collect their personal information, irrespective of their previously declared or undeclared intent to transact and disclose personal information, or despite their desired natural state of information privacy.

Appendices

Appendix

A. Final Data Collection Instrument

Survey Instrument	
Demographics	
1	Gender? 1) Male 2) Female
2	Age? 1) 17 years and under 2) 18—20 years 3) 21—30 years 4) 31—40 years 5) 41—50 years 6) 51—60 years 7) 61—and over
3	Highest level of education (degree) completed? 1) None 2) High school or its equivalent 3) Associate Degree 4) Bachelor Degree 5) Graduate-Professional Degree 6) Others _______________
4	Employment category? 1) Student 2) Self-employed 3) Private organization 4) Government agency 5) Public organization 6) Non-government organization (NGO)

Survey Instrument	
	7) Others _______________
5	Years worked in your current organization or position? 1) None 2) One year and under 3) Two—three years 4) Four—five years 5) Six—seven years 6) Eight—nine years 7) 10—20 years 8) 21 years and over
6	I have access to the Internet regularly as needed. 1) Not at all 2) Very little 3) Somewhat 4) To a moderate extent 5) To a large extent
7	I have access to the Internet at home and/or at work as needed. 1) Not at all 2) Very little 3) Somewhat 4) To a moderate extent 5) To a large extent
8	I have the freedom to logon to the Internet and transact online as needed using either my home computer or one of my personal mobile devices. 1) Not at all 2) Very little 3) Somewhat 4) To a moderate extent 5) To a large extent
9	I have the freedom to logon to the Internet and transact online as needed using my work computer or any of my employer provided mobile devices. 1) Not at all 2) Very little 3) Somewhat 4) To a moderate extent 5) To a large extent

<table>
<tr><th colspan="5">Survey Instrument</th></tr>
<tr><td><b>10</b></td><td colspan="4">Please enter any six alphanumeric characters of your choice (<i>this is necessary because there is a need to show that your response is unique since the survey itself is anonymous</i>), for example, KDJRO9.</td></tr>
<tr><td colspan="5"><b>H1:</b> Desired State of Information Privacy → Information Privacy Equipoise.
Background: there are four states of information privacy as described in Westin (1970): solitude, reserve, intimacy, and anonymity.
In this study, we described how a person will be in one of these states naturally (i.e., if one has a choice, how will the person behave toward online transaction in other not give his or personal information), and we called it the Desired State of Information Privacy. Your honest answers will help us identify what people really want. Therefore, the followings are the definition of the four states in this study:
1. Solitude: those who naturally do not want to purchase things online for fear of disclosing their personal information.
2. Anonymity: those who usually conceal their identities when they purchase things online for the same reason.
3. Reserve: those who are very cautious or selective when deciding to purchase things online for the same reason as well.
4. Intimacy: those who are always eager to purchase thing online and do not worry much about disclosing their personal information online.
<i>Rate from never (1) to always (7) the extent to which each statement is true of your own behavior concerning desired state of information privacy.</i>
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always</td></tr>
<tr><td colspan="2" rowspan="4"><b>Desired State of Information Privacy (DSIP)</b></td><td rowspan="4"><b>H1</b></td><td colspan="2"><b>DSIP → Information Privacy Equipoise</b>:</td></tr>
<tr><td>DSIP1</td><td>Usually, I feel that I have lost control over how my personal information is collected, stored, or used by organizations in online transactions.</td></tr>
<tr><td>DSIP2</td><td>Usually, I believe that most businesses do not handle my personal information, they collected during an online transaction, in a proper and confidential way.</td></tr>
<tr><td>DSIP3</td><td>Usually, I believe that existing laws and current organizational practices do not provide reasonable protections for my personal information in online transactions.</td></tr>
</table>

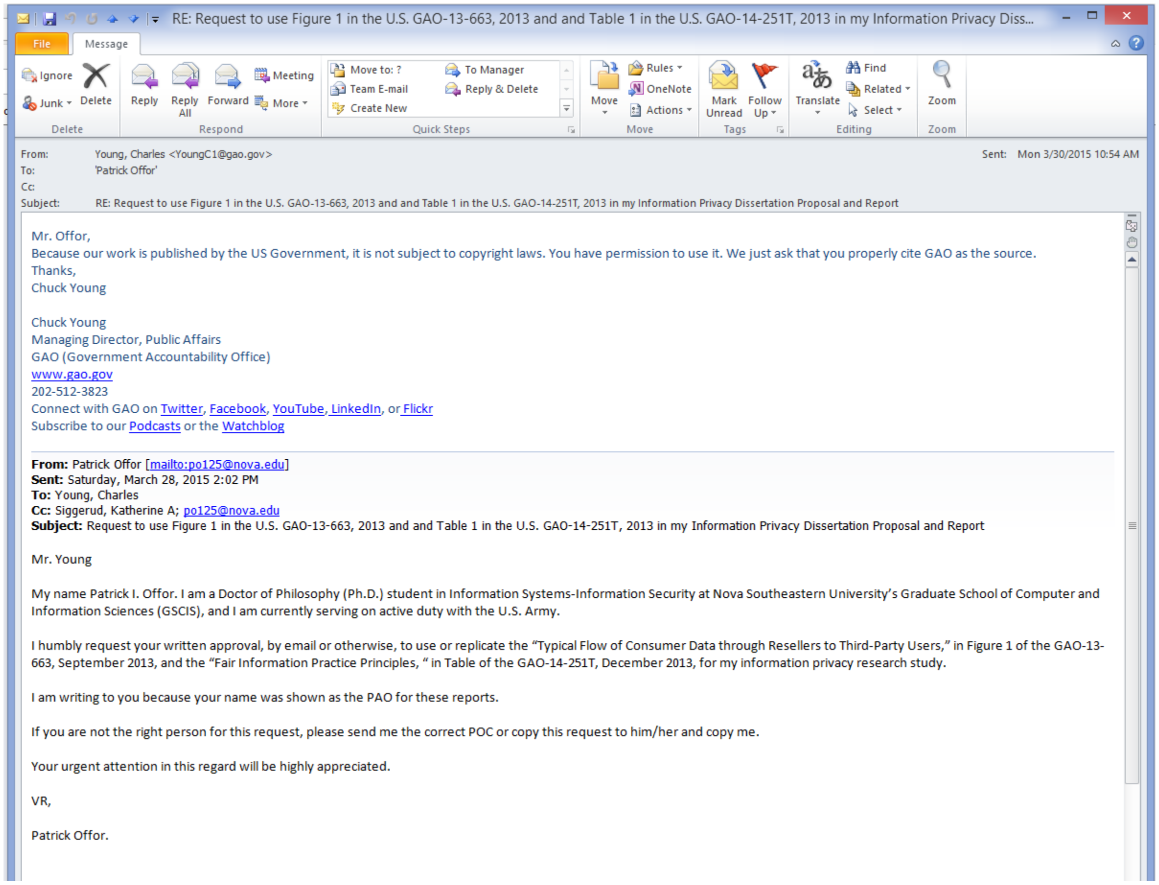
<table>
<tr><th colspan="4">Survey Instrument</th></tr>
<tr><td></td><td></td><td>DSIP4</td><td>Usually, I believe in concealing my personal information, to the maximum extent possible, when transacting online.</td></tr>
<tr><td colspan="4">**H2: Information Privacy Self-Interest → Information Privacy Equipoise**:
Scenario: suppose that I am in a solitude state of information privacy, which means that my natural state of information privacy. Hence, I am one of those people who hate to transact online in order not to disclose my personal information. However, I am in need of a book, like yesterday, and my local bookstore does not carry the book or would not be able provide the book to me in a timely manner if I were to order it from them. In addition, I learned that the nearest store that carries the book is about 75 miles away and I have no intention of driving that far for the book, since I can get the book from an online merchant for overnight delivery.
Options: The study argues that there three major courses of action in this case, (1) do not buy the book and bear the consequences, (2) travel 75 miles and buy the book, or (3) buy the book online. My natural information privacy posture, solitude, will remain intact if I were to travel 75 miles to get the book or if I decide not to buy the book at all. However, there will be a change to my information privacy posture if I decide to buy the book online.
Rate from never (1) to always (7) the extent to which each statement is true of your own behavior concerning information privacy self-interest.
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always</td></tr>
<tr><td>**Information Privacy Self-Interest (IPSI)**</td><td>**H2**</td><td>IPSI1</td><td>I find that my interest in the goods or services that I want to obtain overrides my concerns of possible risk or vulnerability that I may have regarding my personal information disclosure online.</td></tr>
<tr><td></td><td></td><td>IPSI2</td><td>The greater my interest to purchase a certain good or service, the more I tend to suppress the risk of disclosing my personal information online.</td></tr>
<tr><td></td><td></td><td>IPSI3</td><td>In general, my interest in the goods or services that I want to purchase online is greater than my concern about disclosing my personal information.</td></tr>
<tr><td colspan="4">**Information Privacy Permeability → Information Privacy Equipoise**:
Information Privacy Permeability is the collection of additional information from a customer by an online merchant during a transaction with or without his or her knowledge.
Background: a consumer may be forced to provide additional information online, which may not be necessary for the completion of a sales transaction, i.e., personalization, advertisement, and/or other information. In such situation, the consumer may provide the information being asked online, just to be able to complete the transaction. Secondly, an organization may use technology to collect personal information from a consumer during a transaction without the</td></tr>
</table>

<table>
<tr><th colspan="4">Survey Instrument</th></tr>
<tr><td colspan="4">person’s knowledge, i.e., network IP addresses, visited sites, consumer-purchasing patterns, and the like.
Rate from never (1) to always (7) the extent to which each statement is true of your own behavior concerning information privacy permeability.
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always</td></tr>
<tr><td>**Information Privacy Permeability (IPP)**</td><td>**H3**</td><td>IPP1</td><td>It bothers me when an organization insists on getting certain personal information from me, before allowing me to complete an online transaction or purchase; especially, when I believe the information to be unnecessary.</td></tr>
<tr><td></td><td></td><td>IPP2</td><td>It bothers me to know that an organization can collect my personal information, without my knowledge or approval, when I am transacting online.</td></tr>
<tr><td></td><td></td><td>IPP3</td><td>It concerns me when an organization is using technology to collect my personal information, without my knowledge, during an online transaction.</td></tr>
<tr><td></td><td></td><td>IPP4</td><td>I am concerned that organizations are collecting too much personal information from consumers online.</td></tr>
<tr><td colspan="4">**H4: Information Privacy Equipoise → Consumers’ Selective Personal Information Disclosure Behavior**:
Information privacy equipoise is a state of mind, in information privacy context, in which the people who normally will and those who normally will not transact or disclose their personal information online, will come to terms with idea, and occasionally feel at ease with disclosing their personal information online.
Scenario: Suppose I am naturally in a state of solitude, which means that I naturally do not want to purchase things online for fear of disclosing their personal information. However, I am willing to transact online sometimes.
Rate from never (1) to always (7) the extent to which each statement is true of your own behavior concerning information privacy equipoise.
Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always</td></tr>
<tr><td>**Information Privacy Equipoise (IPE)**</td><td>**H4**</td><td>IPE1</td><td>At times, my concern for personal information disclosure in an online transaction seems to fade away, despite my awareness of the possible risks and/or vulnerabilities of disclosing my personal information in an online transaction.</td></tr>
</table>

Survey Instrument			
		IPE2	At times, I feel at ease with disclosing my personal information in an online transaction, despite the potential risk and/or vulnerability it poses to my personal information.
		IPE3	At times, I feel like there is no need in worrying about disclosing my personal information in an online transaction setting because of my belief that if an organization needs my personal information, it will get it in any way possible.
		IPE4	At times, I feel like there is no sense in worrying about disclosing my personal information in an online transaction setting because an organization will get my personal information, in any case, whether I do the purchase from its online store, or from its brick-and-mortar store.
Consumers' Selective Personal Information Disclosure Behavior: Selective Information Privacy Disclosure is the idea that consumers disclose their personal information online sometimes and at other times, they do not. *Rate from never (1) to always (7) the extent to which each statement is true of your own behavior concerning consumers' selective personal information disclosure behavior*. Key: 1 = Never 2 = Hardly ever 3 = Seldom 4 = Occasionally 5 = Often 6 = Usually 7 = Always			
Selective Personal **Information Disclosure Behavior (SPID)**		SPID1	I have disclosed my personal information online, at times, during the purchase of a good or service, from a website that requires me to submit accurate and identifiable information, such as my name, address, credit card, and others.
		SPID2	I have disclosed my personal information online, at times, during the registration for an activity relating to banking, insurance coverage, loan application, mortgage payment, device or card activation, social media membership, or others, on a website that requires me to submit accurate and identifiable information.
		SPID3	I have disclosed my personal information online, at times, in order to view and/or retrieve my financial (bank, credit card, or stocks), medical, and other information, from a highly personal- and password-protected website.
		SPID4	I have disclosed my personal information online, at times, when registering, renewing, retrieving, or updating my highly personal- and password-protected information, such as voter's registration, driver's license, postal address, personal property, or others, on a government or public website.

Appendix

B. Government Accounting Office Approval



From: Young, Charles <YoungC1@gao.gov>
To: 'Patrick Offor'
Cc:
Subject: RE: Request to use Figure 1 in the U.S. GAO-13-663, 2013 and and Table 1 in the U.S. GAO-14-251T, 2013 in my Information Privacy Dissertation Proposal and Report
Sent: Mon 3/30/2015 10:54 AM

Mr. Offor,
Because our work is published by the US Government, it is not subject to copyright laws. You have permission to use it. We just ask that you properly cite GAO as the source.
Thanks,
Chuck Young

Chuck Young
Managing Director, Public Affairs
GAO (Government Accountability Office)
www.gao.gov
202-512-3823
Connect with GAO on Twitter, Facebook, YouTube, LinkedIn, or Flickr
Subscribe to our Podcasts or the Watchblog

From: Patrick Offor [mailto:po125@nova.edu]
Sent: Saturday, March 28, 2015 2:02 PM
To: Young, Charles
Cc: Siggerud, Katherine A; po125@nova.edu
Subject: Request to use Figure 1 in the U.S. GAO-13-663, 2013 and and Table 1 in the U.S. GAO-14-251T, 2013 in my Information Privacy Dissertation Proposal and Report

Mr. Young

My name Patrick I. Offor. I am a Doctor of Philosophy (Ph.D.) student in Information Systems-Information Security at Nova Southeastern University's Graduate School of Computer and Information Sciences (GSCIS), and I am currently serving on active duty with the U.S. Army.

I humbly request your written approval, by email or otherwise, to use or replicate the "Typical Flow of Consumer Data through Resellers to Third-Party Users," in Figure 1 of the GAO-13-663, September 2013, and the "Fair Information Practice Principles, " in Table of the GAO-14-251T, December 2013, for my information privacy research study.

I am writing to you because your name was shown as the PAO for these reports.

If you are not the right person for this request, please send me the correct POC or copy this request to him/her and copy me.

Your urgent attention in this regard will be highly appreciated.

VR,

Patrick Offor.

Appendix

C. Minimum Values of Content Validity Ratio

CVR_t One tailed Test with *p* = 0.05 (CVR = 1.00 was adjusted to .99 for ease of manipulation)

Number of Panelists	Minimum Value
5	.99
6	.99
7	.99
8	.75
9	.78
10	.62
11	.59
12	.56
13	.54
14	.51
15	.49
20	.42
25	.37
30	.33
35	.31
40	.29

CVR table adapted from Lawshe (1975)

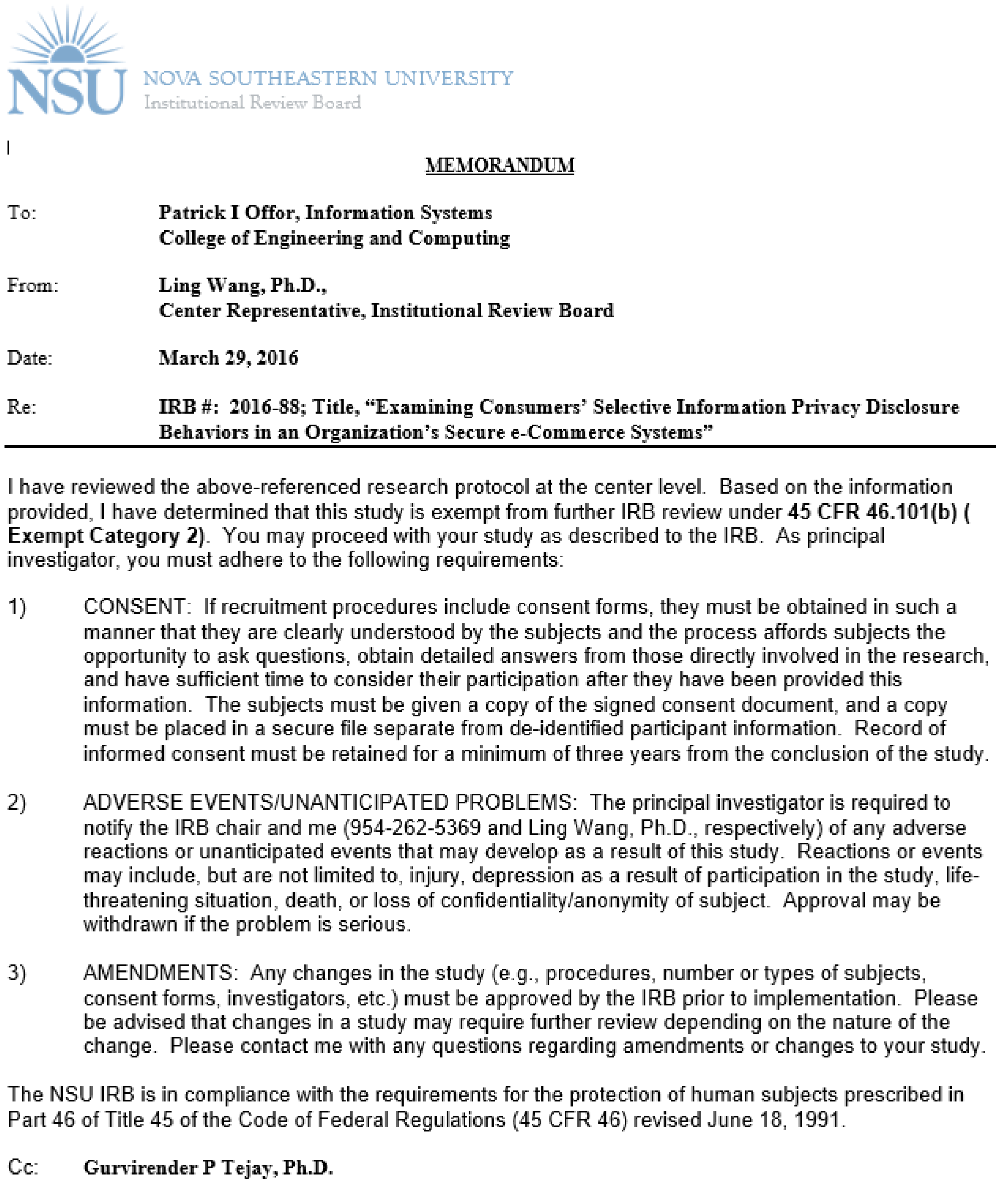
Corrected and Expanded Critical Values for Lawshe's (1975) Content Validity Ratio ($\text{CVR}_{\text{critical}}$) adapted from Wilson, Pan, and Schumsky (2012)

	Level of Significance for Two-Tailed Test					
	.1	.05	.025	.01	.005	.001
	Level of Significance for Two-Tailed Test					
N	.2	.1	.05	.02	.01	.002
5	.573	.736	.877	.99	.99	.99
6	.523	.672	.800	.950	.99	.99
7	.485	.622	.741	.879	.974	.99
8	.453	.582	.693	.822	.911	.99
9	.427	.548	.653	.775	.859	.99
10	.405	.520	.620	.736	.815	.977
11	.387	.496	.591	.701	.777	.932
12	.370	.475	.566	.671	.744	.892
13	.356	.456	.544	.645	.714	.857
14	.343	.440	.524	.622	.688	.826
15	.331	.425	.506	.601	.665	.798
16	.321	.411	.490	.582	.644	.773
17	.311	.399	.475	.564	.625	.750
18	.302	.388	.462	.548	.607	.729
19	.294	.377	.450	.534	.591	.709
20	.287	.368	.438	.520	.576	.691
21	.280	.359	.428	.508	.562	.675
22	.273	.351	.418	.496	.549	.659
23	.267	.343	.409	.485	.537	.645
24	.262	.336	.400	.475	.526	.631
25	.256	.329	.392	.465	.515	.618
26	.251	.323	.384	.456	.505	.606
27	.247	.317	.377	.448	.496	.595
28	.242	.311	.370	.440	.487	.584
29	.238	.305	.364	.432	.478	.574
30	.234	.300	.358	.425	.470	.564
31	.230	.295	.352	.418	.463	.555
32	.227	.291	.346	.411	.455	.546
33	.223	.286	.341	.405	.448	.538
34	.220	.282	.336	.399	.442	.530
35	.217	.278	.331	.393	.435	.522
36	.214	.274	.327	.388	.429	.515
37	.211	.270	.322	.382	.423	.508
38	.208	.267	.318	.377	.418	.501
39	.205	.263	.314	.372	.412	.495
40	.203	.260	.310	.368	.407	.489

Note: Values for $\text{CVR}_{\text{critical}}$ greater than or equal to the limit value of 1.00 were set to .99.

Appendix

D. IRB Approval Memo



NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Patrick I Offor, Information Systems**
College of Engineering and Computing

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **March 29, 2016**

Re: **IRB #: 2016-88; Title, "Examining Consumers' Selective Information Privacy Disclosure Behaviors in an Organization's Secure e-Commerce Systems"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: **Gurvirender P Tejay, Ph.D.**

Appendix

E. Introductory Letters to the Participants

Substantive Validity Analysis

Dear Panelist,

The essence of this survey is to validate the constructs. In other words, to check whether the items or the questions have adequate reflection on the constructs they represent. Validation of a construct is essential, especially with the introduction of new items or observes variables. In addition, validation is warranted when an existing item is modified. The survey has 24 items/questions for the five constructs.

The constructs are as follows:

1. Desired State of Information Privacy
2. Information Privacy Self-Interest
3. Information Privacy Permeability
4. Information Privacy Equipoise
5. Selective Personal Disclosure behaviors

Hence, please read the definition of the constructs and select the construct that is best represented in the questions. Please note that items are randomized to avoid any type response biases.

Also, use the comment box to provide me with any suggestion in this regard.

This is the Part I of the Expert Panel survey. I will send the second part once the items are properly aligned to their respective constructs.

Again, thank you!

Patrick Offor.

Content Validity Ratio

Dear Panelist,

As you may know, this is the second part of the survey for the expert panelists. The survey is for the content validity ratio. Hence, the essence is to check whether an item or an indicator variable has relevance to the latent variable it is design to observe reflectively or formatively. The *Desired State of Information Privacy* and the *Information Privacy Equipoise* constructs are formative in nature, whereas the rest of the other constructs are reflective. Validation of these variables or indicators are essential, especially with the introduction of new items. In addition, validation is warranted when an existing item is modified.

Most of your recommendations in Part I, concerning the Substantive Validity Analysis, were considered, and modifications to some of the items have taken place. However, please do not hesitate to identify any error and omission in this one as applicable.

The survey contains a total of 35 questions, 29 items and five demographic questions. Therefore, please assess the relevancy of each item to the construct by selecting any one of the followings:

1. Essential
2. Useful but not essential
3. Not essential

In some cases, I provided background information on the constructs for better understanding and perspective. I also simplified some of the descriptions and/or provided examples per your earlier recommendations.

The comment box in each page is not a mandatory field, but was provided so that you can provide me pinpointed suggestions, if necessary.

I am very appreciative of your earlier responses and feedbacks, and I am looking forward to a healthy feedback from you on this one as well. Therefore, accept my gratitude for your participation as an expert panelist in my study!

Thank you!

Sincerely,

Patrick Offor.

Pilot Test and the Study

Dear Participant,

As a Ph. D. student at Nova Southeastern University, Florida, I am conducting a research study, pursuant to a Dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems. The goal of the research is to understand consumers' selective information privacy disclosure behaviors in an organization's based on Privacy Regulation Theory.

I am very appreciative of the time you would spend in this research survey. The study will protect all information gathered in this research and will not distribute or use the information for any other reason or purpose.

Please note that there are seven sections in the survey, which will take you approximately 10-20 minutes to complete. In addition, please be aware that your survey will count only if you complete ALL the questions in each section. The survey contains a total of 31 questions, 21 items and 10 demographic questions.

The survey is anonymous. Please answer the questions as honestly as you can because the idea is understanding your true feelings and experiences—there are no correct answers.

By taking the survey, you indicated that your participation in the study is voluntary. Please contact me with your questions by phone at 931-206-2472 or by email at po125@nova.edu.

Sincerely,

Patrick I. Offor

Nova Southeastern University

THANK YOU!

Appendix

F. Substantive Validity Analysis Result

	Questions	N	DSIP	IPSI	IPP	IPE	SPID	*Substantive Validity Coefficient ${}^{6}C_{SV} = \frac{n_{c\text{-}n_o}}{N}$	The Study's Initial Construct Associated with the Each Item
Q1	I believe that consumers have lost control over how their personal information is collected and used by organizations.	9.0	**2.0**	0.0	**7.0**	0.0	0.0	**-0.56**	**DSIP**
Q9	I believe that most businesses handle the personal information they collect about consumers in a proper and confidential way.	9.0	**6.0**	0.0	0.0	**3.0**	0.0	**0.33**	**DSIP**
Q14	I believe that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	9.0	**3.0**	0.0	0.0	**6.0**	0.0	**-0.33**	**DSIP**
Q17	I usually conceal my personal information, to the maximum extent possible, when transacting online.	9.0	**2.0**	1.0	0.0	**5.00**	1.0	**-0.33**	**DSIP**
Q4	Whenever I am online to obtain a particular item or service, I disclose my personal information if the Website or the online merchant designates the personal information as required.	9.0	2.0	**3.0**	0.0	**1.0**	3.0	**-0.22**	**IPE**
Q7	I usually complete an online purchase even if I feel that the disclosure of additional personal information being asked for is not necessary for me to receive a personalized advertisement.	9.0	0.0	2.0	2.0	**1.0**	**4.0**	**-0.33**	**IPE**
Q8	Whenever I am online to obtain a particular item or service, I disclose my personal information with the belief that the Website or the online merchant will not collect additional information without telling me.	9.0	**4.0**	2.0	1.0	**1.0**	1.0	**-0.33**	**IPE**

[6] C_{SV} = the substantive validity coefficient.
n_c = the number of respondent's assignment of an observed variable to its intended construct in the set.
n_o = the highest number of assignment of an observed variable to an unintended construct in the set.
N = the total number of respondents.
(Anderson & Gerbing, 1991)

	Questions	N	DSIP	IPSI	IPP	IPE	SPID	*Substantive Validity Coefficient $^{6}\mathrm{Csv} = \frac{n_{c\text{-}n_o}}{N}$	The Study's Initial Construct Associated with the Each Item
Q10	I usually share my required personal information when purchasing goods or services online whenever I am at ease with an online merchant's information privacy posture.	9.0	**4.0**	2.0	0.0	**2.0**	1.0	**-0.22**	**IPE**
Q15	Whenever I am online to obtain a particular item or service, I disclose my personal information based on my needs or interests at the time.	9.0	0.0	**4.0**	0.0	**1.0**	4.0	**-0.33**	**IPE**
Q19	I use third party payment services or methods, such as Pay-Pal, whenever possible, to obtain goods or services online.	9.0	2.0	**5.0**	0.0	**2.0**	0.0	**-0.33**	**IPE**
Q21	I usually complete an online purchase even if I feel that the disclosure of my personal information is not necessary for me to obtain a particular item or service.	9.0	0.0	1.0	2.0	**1.0**	**5.0**	**-0.44**	**IPE**
Q24	I usually complete an online purchase even if I feel that the disclosure of additional personal information being asked for is not necessary for me to receive an immediate or future discount.	9.0	0.0	2.0	1.0	**0.0**	**6.0**	**-0.67**	**IPE**
Q3	It concerns me that organizations are using technology to collect my personal information, without my knowledge, whenever I am making an online transaction.	9.0	**1.0**	0.0	**8.0**	0.0	0.0	**0.78**	**IPP**
Q6	I am concerned that organizations are collecting too much personal information from consumers online.	9.0	2.0	0.0	**4.0**	**2.0**	1.0	**0.22**	**IPP**
Q12	It usually bothers me when an organization insists on getting certain personal information before allowing me to complete an online transaction or purchase.	9.0	1.0	2.0	**1.0**	2.0	**3.0**	**-0.22**	**IPP**
Q20	I usually think twice before providing my personal information online whenever an organization asks for it.	9.0	1.0	1.0	**1.0**	**4.0**	2.0	**-0.33**	**IPP**
Q2	In general, my interest in the goods or services that I want to purchase online is greater than	9.0	1.0	**5.0**	0.0	0.0	**3.0**	**0.22**	**IPSI**

	Questions	N	DSIP	IPSI	IPP	IPE	SPID	*Substantive Validity Coefficient $^{6}\mathrm{Csv} = \frac{n_{c}\text{-}n_{o}}{N}$	The Study's Initial Construct Associated with the Each Item
	my concern about disclosing my personal information.								
Q22	I find that my interest in the goods or services that I want to obtain overrides my concerns of possible risk or vulnerability that I may have regarding the disclosure of my personal information online.	9.0	1.0	**2.0**	**2.0**	2.0	2.0	**0.00**	**IPSI**
Q23	The greater my interest to purchase a certain good or service, the more I tend to suppress the risk of disclosing my personal information online.	9.0	0.0	**4.0**	**2.0**	1.0	2.0	**0.22**	**IPSI**
Q5	I have disclosed my personal information online when I either registering, renewing, or updating highly personal and password-protected e-government information (e.g., using websites that allow me to access my voter registration, driver's license renewal, updating postal address, or the like).	9.0	3.0	**4.0**	0.0	0.0	2.0	**-0.22**	**SPID**
Q11	I have disclosed my personal information online when I was conducting sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software).	9.0	1.0	**6.0**	0.0	1.0	**1.0**	**-0.56**	**SPID**
Q13	I have disclosed my personal information online during a retrieval of information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates).	9.0	1.0	**3.0**	2.0	0.0	**3.0**	**0.00**	**SPID**
Q16	I have disclosed my personal information online during a retrieval of highly personal and password-protected financial information (e.g., using websites that allow me to	9.0	2.0	**3.0**	1.0	1.0	**2.0**	**-0.11**	**SPID**

	Questions	N	DSIP	IPSI	IPP	IP E	SPID	*Substantive Validity Coefficient $^{6}\mathrm{Csv} = \frac{n_{c}-n_{o}}{N}$	The Study's Initial Construct Associated with the Each Item
	access my bank account or my credit card account).								
Q18	I have disclosed my personal information online during a purchase of goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information).	9.0	3.0	**3.0**	0.0	1.0	**2.0**	**-0.11**	**SPID**

*Substantive Validity Coefficient is equal to the subtraction of "the highest number of assignments of the item to any other construct in the set" (Anderson & Gerbing, 1991, p. 734) from the number of participants who correctly assign an item to its intended construct, and dividing the result by the total number of participants.

Appendix

G. Content Validity Ratio Result

Construct	Item ID	Items	N[7]	Essential[8]	Useful but not essential	Not essential
Desired State of Information Privacy (DSIP)	**DSIP1**	Usually, I believe that consumers have lost control over how their personal information is collected and used by organizations.	11	**0.73**	0.09	0.18
	DSIP2	Usually, I believe that most businesses handle the personal information they collect about consumers in a proper and confidential way.	11	**0.55**	0.18	0.27
	DSIP3	Usually, I believe that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	11	0.36	0.45	0.18
	DSIP4	Usually, I believe in concealing my personal information, to the maximum extent possible, when transacting online.	11	**0.73**	0.18	0.09
Information Privacy Self-Interest (IPSI)	**IPSI1**	I find that my interest in the goods or services that I want to obtain overrides my concerns for possible risks or vulnerabilities that I may have regarding the disclosure of my personal information online.	11	**0.73**	0.18	0.09
	IPSI2	The greater my interest to purchase a certain good or service, the more I tend to suppress the risks or vulnerabilities of disclosing my personal information online.	11	**0.91**	0.00	0.09
	IPSI3	In general, my interest in the goods or services that I want to purchase online is greater than my concern about disclosing my personal information.	11	**0.73**	0.09	0.18
Information Privacy Permeability (IPP)	**IPP1**	It bothers me when an organization insists on getting certain personal information, especially when I believe the information to be unnecessary, before allowing me to complete an online transaction or purchase.	11	**0.73**	0.09	0.18

[7] *N* is the number of participants

[8] An item with an *essential* selection of 0.50 or greater from *N* is positive and falls between 0.0 and 0.99—CVR 1.0 is adjusted to 0.99 for manipulation purpose (Lawshe (1975, p. 568).

Construct	Item ID	Items	N[7]	Essential[8]	Useful but not essential	Not essential
	IPP2	I usually think twice before providing certain personal information online, whenever an organization asks for it, because I do not know who else will have asses to it and for what purpose.	11	**0.55**	0.36	0.09
	IPP3	It bothers to know that organizations can collect my personal information, without my knowledge or approval, when I am transacting online.	11	**0.82**	0.00	0.18
	IPP4	It concerns me that organizations are using technology to collect my personal information, without my knowledge, whenever I am making an online transaction.	11	**0.73**	0.18	0.09
	IPP5	I am concerned that organizations are collecting too much personal information from consumers online whether they know it or not.	11	**0.82**	0.09	0.09
Information Privacy Equipoise (IPE)	**IPE1**	I believe in sharing my personal information when purchasing an item or service online.	11	0.45	0.36	0.18
	IPE2	I believe in making an assessment of the information being requested before providing my personal information in an online transaction whenever an organization asks for it.	11	0.36	0.09	0.55
	IPE3	I believe that the use of a third-party payment service or method, such as Pay-Pal and other, to obtain goods or services online allows me to disclose my personal information online.	11	0.45	0.36	0.18
	IPE4	Although I dislike the idea of disclosing my personal information when transacting online, at times, I believe in disclosing my personal information in an online transaction without regard for any potential risk or vulnerability involved.	11	**0.64**	0.09	0.27
	IPE5	I believe in sharing my personal information when transacting online to obtain a particular good or service based on my need or interest at the time.	11	**0.73**	0.18	0.09
	IPE6	I believe that the need to obtain a certain good or service online diminishes my concern for personal information disclosure risks and vulnerabilities at the time.	11	**0.82**	0.09	0.09

Construct	Item ID	Items	N[7]	Essential[8]	Useful but not essential	Not essential
	IPE7	I believe in disclosing my personal information online to obtain a good and service even when I think that an online merchant is using technology to collect additional formation from me at the time.	11	0.45	0.36	0.18
	IPE8	My concern of an organization collecting additional information from me when transaction online, knowing and unknowing, diminishes based on my belief that the organization's information privacy practices are in line with available laws and regulations at the time.	11	0.45	0.18	0.36
Selective Personal Information Disclosure (SPID)	**SPID1**	I have disclosed my personal information online during a purchase of goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information).	11	**0.73**	0.09	0.18
	SPID2	I have disclosed my personal information online during a retrieval of information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates).	11	**0.73**	0.09	0.18
	SPID3	I have disclosed my personal information online when I was conducting sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software).	11	**0.64**	0.09	0.27
	SPID4	I have disclosed my personal information online during a retrieval of highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account).	11	**0.91**	0.09	0.00

Construct	Item ID	Items	N[7]	Essential[8]	Useful but not essential	Not essential
	SPID5	I have disclosed my personal information online when I am either registering, renewing, or updating highly personal and password-protected e-government information (e.g., using websites that allow me to access my voter registration, driver's license renewal, updating postal address, or the like).	11	**0.73**	0.09	0.18

Appendix

H. Correlation Matrix for the Pilot Study

Correlation Matrix[a]

		DSIP1	DSPI2	DSIP3	DSIP4	IPSI1	IPSI2	IPSI3	IPP1	IPP2	IPP3	IPP4	IPE1	IPE2	IPE3	IPE4	SIPD1	SIPD2	SIPD3	SIPD4
Correlation	DSIP1	**1.000**																		
	DSPI2	**0.457**	**1.000**																	
	DSIP3	**0.566**	**0.549**	**1.000**																
	DSIP4	**0.377**	**0.432**	**0.399**	**1.000**															
	IPSI1	0.009	-0.245	-0.144	-0.074	**1.000**														
	IPSI2	0.268	-0.141	0.004	0.007	**0.637**	**1.000**													
	IPSI3	0.062	-0.164	-0.132	-0.108	**0.776**	**0.707**	**1.000**												
	IPP1	0.497	0.378	0.282	0.337	0.052	0.237	0.193	**1.000**											
	IPP2	0.323	0.417	0.268	0.498	0.057	0.204	0.176	**0.834**	**1.000**										
	IPP3	0.287	0.374	0.315	0.460	0.051	0.227	0.126	**0.755**	**0.905**	**1.000**									
	IPP4	0.380	0.457	0.365	0.494	-0.039	0.175	0.146	**0.755**	**0.880**	**0.866**	**1.000**								
	IPE1	-0.108	0.038	-0.088	0.000	0.370	0.396	0.495	0.224	0.309	0.288	0.324	**1.000**							
	IPE2	-0.044	-0.037	-0.134	-0.074	0.457	0.377	0.402	0.089	0.088	0.098	0.050	**0.664**	**1.000**						
	IPE3	-0.102	-0.088	-0.084	-0.143	0.135	0.073	0.090	-0.303	-0.125	-0.160	-0.215	**0.158**	**0.251**	**1.000**					
	IPE4	-0.016	-0.025	-0.036	-0.179	0.083	0.160	0.101	-0.201	-0.143	-0.144	-0.166	**0.146**	**0.248**	**0.760**	**1.000**				
	SIPD1	-0.013	-0.154	-0.143	-0.066	0.332	0.434	0.531	0.153	0.225	0.161	0.188	0.511	0.469	0.366	0.336	**1.000**			
	SIPD2	0.010	-0.222	-0.020	-0.136	0.284	0.243	0.338	0.131	0.023	-0.011	0.087	0.394	0.424	0.241	0.331	**0.687**	**1.000**		
	SIPD3	0.070	0.017	0.099	-0.024	0.237	0.356	0.448	0.253	0.289	0.223	0.281	0.494	0.366	0.218	0.234	**0.757**	**0.707**	**1.000**	
	SIPD4	-0.126	-0.154	0.047	-0.141	0.306	0.189	0.356	0.071	0.039	0.024	0.139	0.532	0.445	0.269	0.258	**0.639**	**0.697**	**0.670**	**1.000**

a. Determinant = 1.004E-7

Appendix

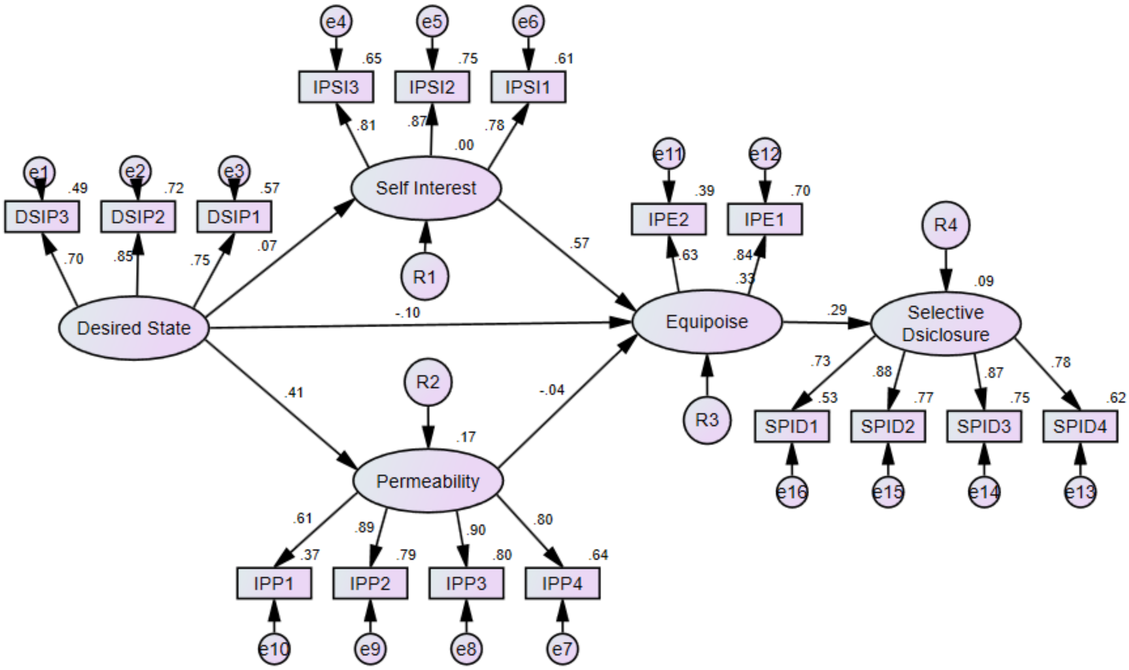
I. The EFA and the PCA Result for the Pilot Test

Descriptive Statistics

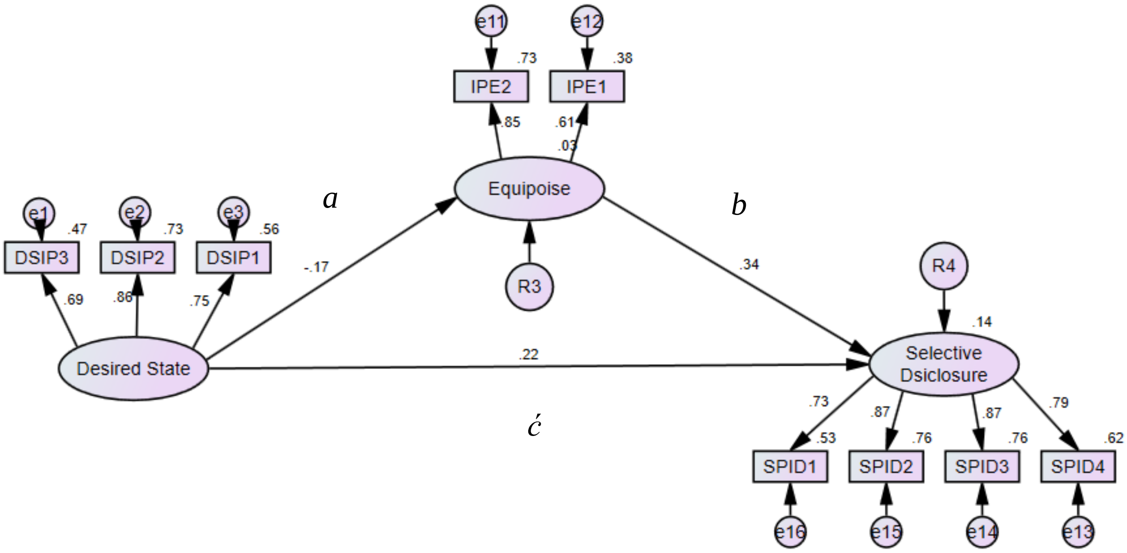
	Mean	**Std. Deviation**	**Analysis N**
DISP1	4.29	1.912	55
DISP2	3.98	1.616	55
DISP3	3.89	1.792	55
DISP4	4.93	1.804	55
IPSI1	4.15	1.726	55
IPSI2	4.27	1.683	55
IPSI3	3.96	1.815	55
IPP1	5.27	2.041	55
IPP2	5.51	1.855	55
IPP3	5.58	1.950	55
IPP4	5.42	1.739	55
IPE1	4.24	1.598	55
IPE2	3.89	1.595	55
IPE3	3.27	1.649	55
IPE4	3.36	1.693	55
SPID1	5.11	1.329	55
SPID2	4.84	1.561	55
SPID3	4.69	1.783	55
SPID4	4.13	1.925	55

Appendix

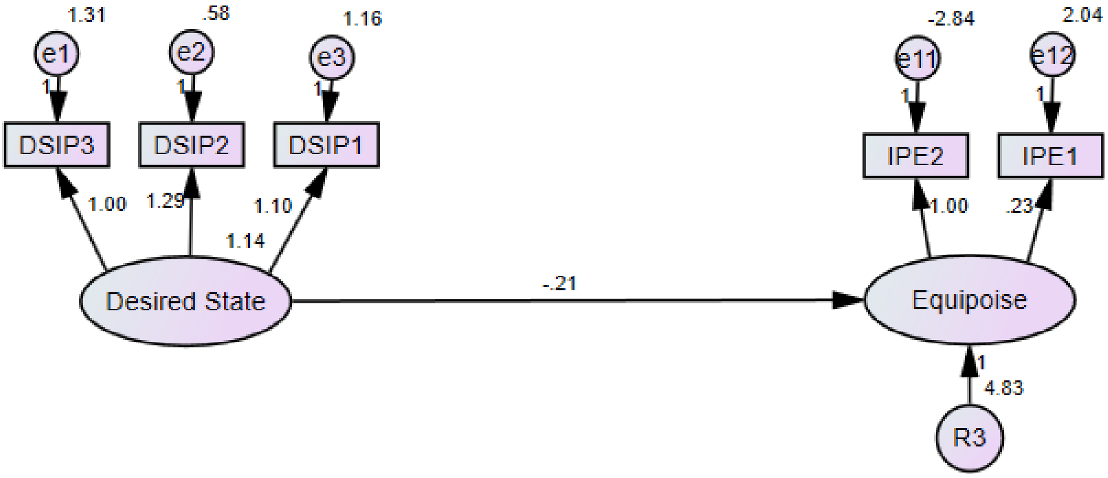
J. Standardized Models



The Standardized Hypnotized Structural Model



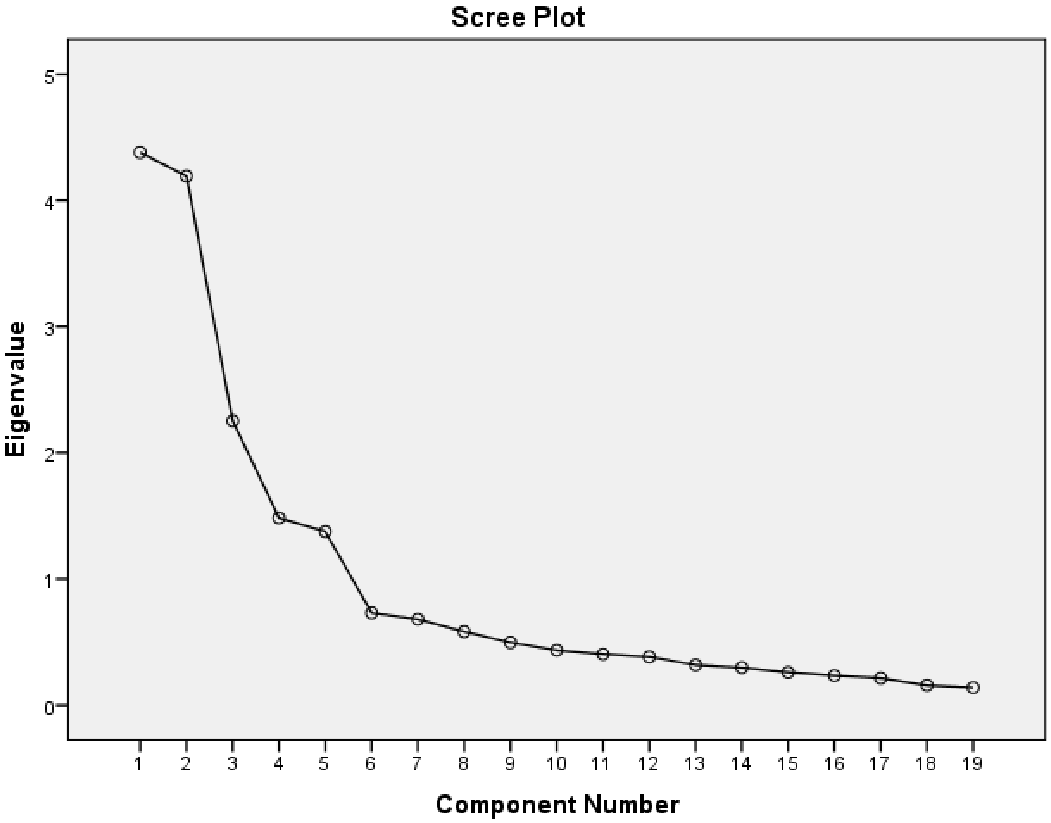
Standardized Mediation Model Path Coefficients (*β*): *a*, *b*, and *ć*



Unstandardized Effect of the Desired State on the Equipoise

Appendix

K. Principal Component Analysis Plot for the Pilot Test



Appendix

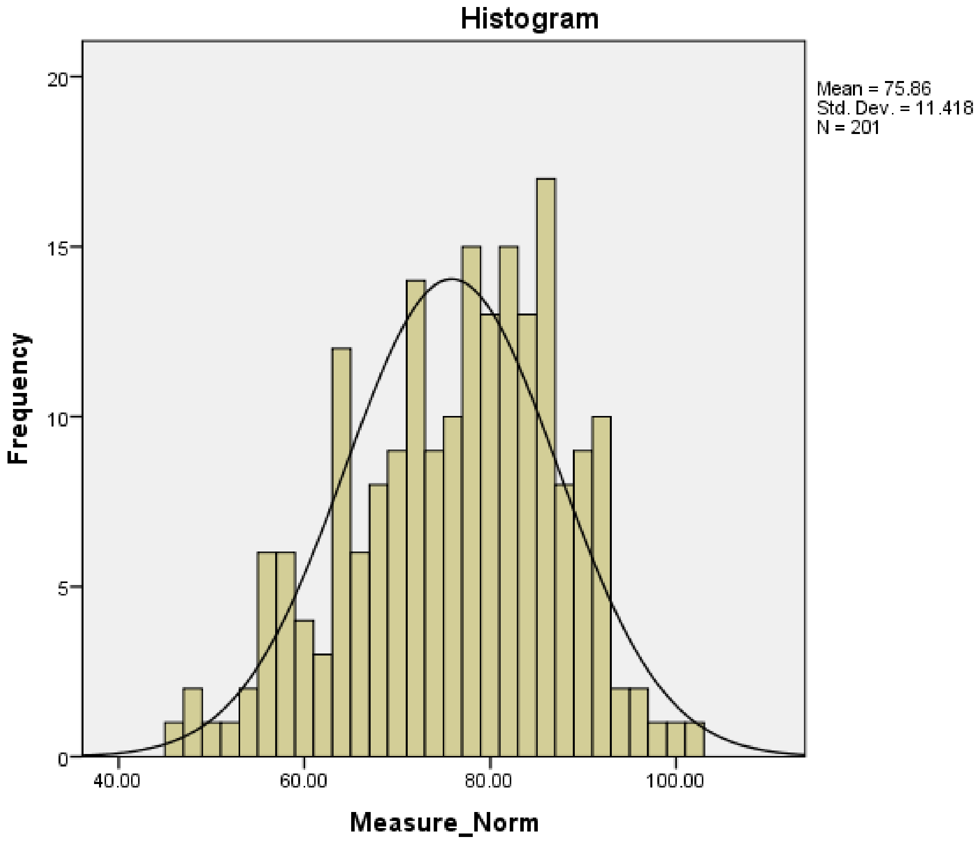
L. The Taxonomy of the Desired State of Information Privacy Calculation

	Intimacy				**Reserve**										**Solitude**			
Compute value	3	4	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Frequency Percentage	10.5%				73.1%										16.4%			

										Anonymity								
Compute value	3	4	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
7-point Likert scale	1		2			3			4				5			6		7
Frequency Percentage		5%								36%							59%	

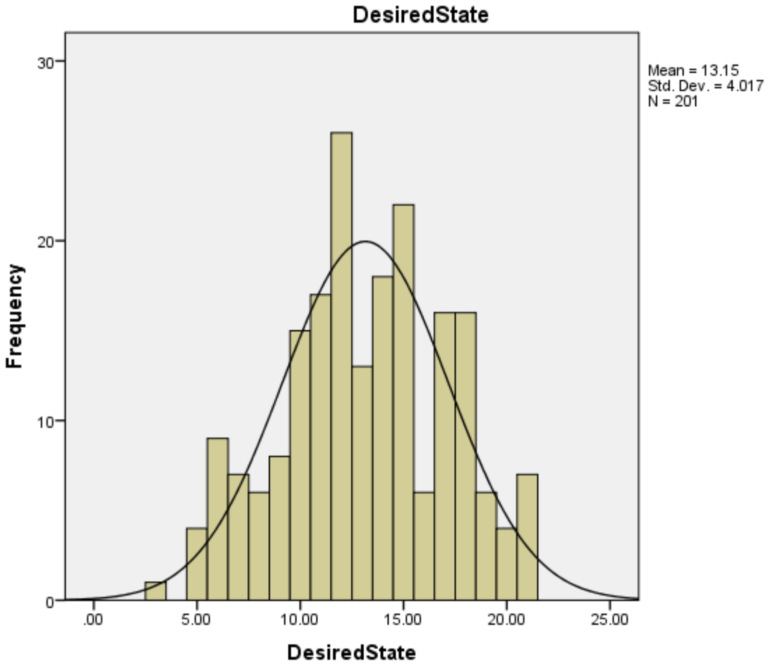
Appendix

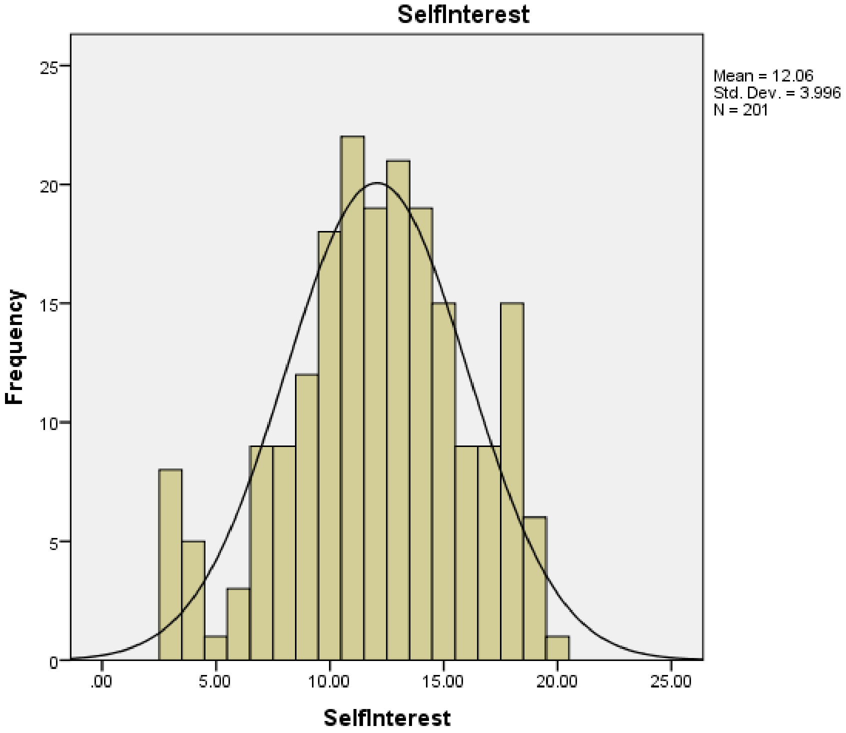
M. Normality Distribution

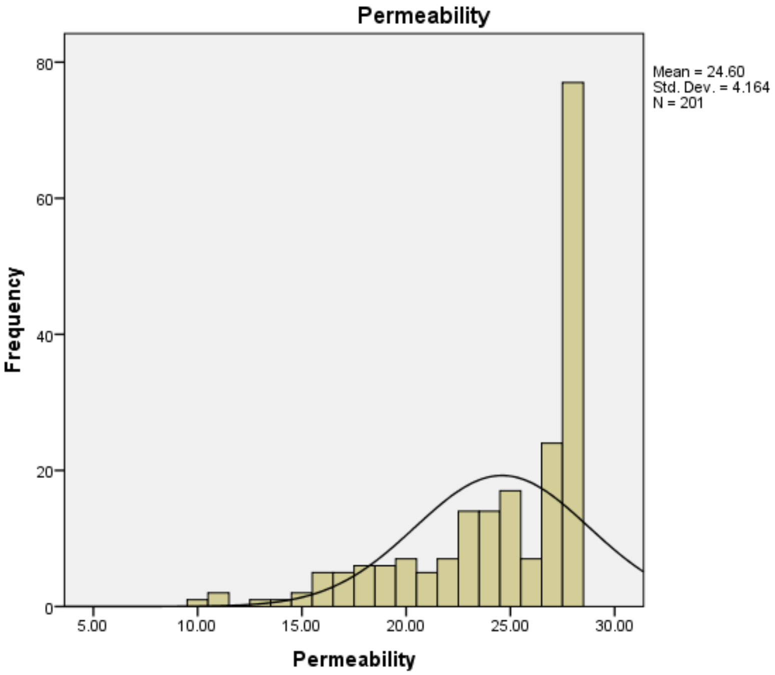


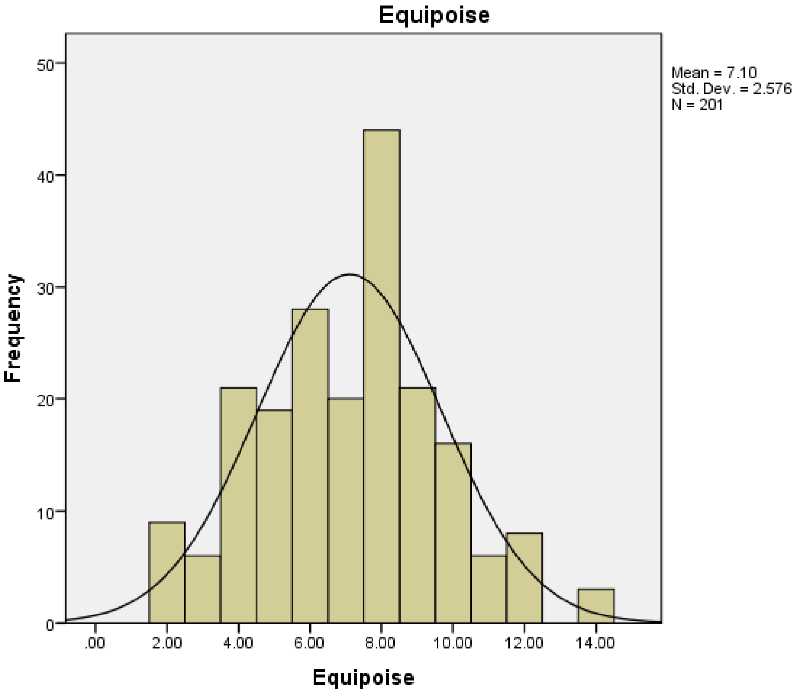
Statistics

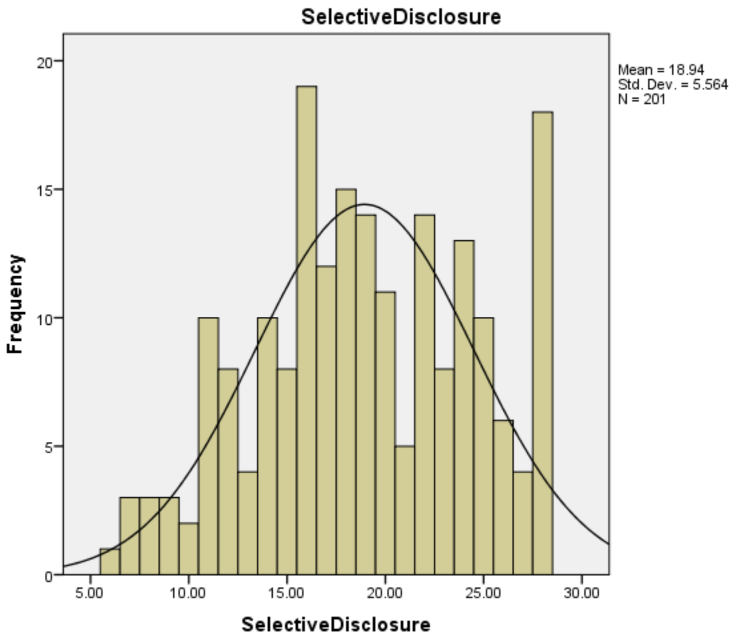
		Measure_Norm	DesiredState	SelfInterest	Permeability	Equipoise	SelectiveDisclosure
N	Valid	201	201	201	201	201	201
	Missing	0	0	0	0	0	0
Variance		130.374	16.138	15.971	17.342	6.634	30.956
Skewness		-.389	-.100	-.325	-1.294	.114	-.114
Std. Error of Skewness		.172	.172	.172	.172	.172	.172
Kurtosis		-.400	-.558	-.281	1.035	-.194	-.758
Std. Error of Kurtosis		.341	.341	.341	.341	.341	.341


DesiredState
Mean = 13.15
Std. Dev. = 4.017
N = 201
Frequency
0
10
20
30
.00
5.00
10.00
15.00
20.00
25.00
DesiredState


SelfInterest
Mean = 12.06
Std. Dev. = 3.996
N = 201
Frequency
0
5
10
15
20
25
.00
5.00
10.00
15.00
20.00
25.00
SelfInterest


Permeability
Mean = 24.60
Std. Dev. = 4.164
N = 201
Frequency
0
20
40
60
80
5.00
10.00
15.00
20.00
25.00
30.00
Permeability


Equipoise
Mean = 7.10
Std. Dev. = 2.576
N = 201
Frequency
0
10
20
30
40
50
.00
2.00
4.00
6.00
8.00
10.00
12.00
14.00
Equipoise



Assessment of normality (Group number 1)

Variable	min	max	skew	c.r.	kurtosis	c.r.
q0016	1.00000	7.00000	-.35327	-2.04472	-.24120	-.69803
q0017	1.00000	7.00000	-.42510	-2.46045	-.45488	-1.31639
q0018	1.00000	7.00000	-.45287	-2.62118	-.59295	-1.71596
q0019	1.00000	7.00000	-.22155	-1.28228	-.82582	-2.38989
q0012	1.00000	7.00000	.07376	.42692	-.61840	-1.78962
q0013	1.00000	7.00000	.27616	1.59841	-.43041	-1.24559
q0008	1.00000	7.00000	-1.47566	-8.54100	1.65576	4.79170
q0009	1.00000	7.00000	-1.51406	-8.76326	1.65020	4.77560
q0010	3.00000	7.00000	-1.59277	-9.21879	1.73906	5.03277
q0011	1.00000	7.00000	-1.41948	-8.21586	1.58422	4.58467
q0005	1.00000	7.00000	-.34655	-2.00583	-.48629	-1.40729
q0006	1.00000	7.00000	-.32986	-1.90918	-.29299	-.84790
q0007	1.00000	7.00000	-.05493	-.31794	-.88123	-2.55024
q0001	1.00000	7.00000	-.17038	-.98613	-.57940	-1.67676
q0002	1.00000	7.00000	.00593	.03434	-.85001	-2.45991
q0003	1.00000	7.00000	-.23484	-1.35921	-.66679	-1.92966
Multivariate					82.53032	24.37644

References

Ackerman, M. S. (2004). Privacy in pervasive environments: Next generation labeling protocols. *Personal and Ubiquitous Computing, 8*(6), 430-439.

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84*(5), 888-918.

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly, 25* (1)107-136.

Albright, J. J., & Park, H. M. (2009). Confirmatory factor analysis using Amos, LISREL, Mplus, and SAS/STAT CALIS. *The Trustees of Indiana University, 1*, 1-85.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational psychology*, *63*(1), 1-18.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing.

Altman, I. (1977). Privacy Regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66-84.

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation1. In B. Leonard (Ed.), *Advances in Experimental Social Psychology* (Vol. Volume 14, pp. 107-160): Academic Press.

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

Anderson, J. C., & Gerbing, D. W. (1991). Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. *Journal of Applied Psychology*, *76*(5), 732-740.

Anderson, S. (2015). *Technology device ownership: 2015*. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/

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

Asdal, K., Brenna, B., & Moser, I. (2007). *Technoscience: The politics of interventions*: Oslo Academic Press.

Awad, N. F., & Krishnan, M. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 13-28.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly, 30*, 413-438.

Baker, M. J. (2000). Writing a literature review. *Marketing Review, 1*(2), 219-247.

Bansal, G., Zahedi, F., & 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.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*(2), 248-287.

Baron, M. A. (2008). Guidelines for writing research proposals and dissertations. *Division of Educational Administration: University of South Dakota*, 1-52.

Barrett, P. (2007). Structural equation modelling: Adjudging model fit. *Personality and Individual Differences, 42*(5), 815-824.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69(*4), 133-152.

Beaumont, R. (2012). An introduction to Principal Component Analysis & Factor Analysis using SPSS 19 and R (psych package). *Factor Analysis and Principal Component Analysis (PCA), 24*(8-9).

Beavers, A. S., Lounsbury, J. W., Richards, J. K., Huck, S. W., Skolits, G. J., & Esquivel, S. L. (2013). Practical considerations for using exploratory factor analysis in educational research. *Practical Assessment, Research & Evaluation, 18*(6), 1-13.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-A1036.

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*(3), 245-270.

Bellia, P. L. (2009). Federalization in information privacy law. *The Yale Law Journal, 118*(5), 868-900.

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin, 107*(2), 238-246.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101-106.

Blaikie, N. (2007). *Approaches to social science enquiry*, (2nd ed.). Malden, MA: Polity Press.

Bollen, K. A., & Long, J. S. (1993). *Testing structural equation models*, 154. Newbury Park, CA: Sage.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Browne, M.W. & Cudeck, R. (1993). Alternative ways of assessing model fit. In Bollen, K.A. & Long, J.S. [Eds.] *Testing structural equation models*. Newbury Park, CA: Sage, 136–162.

Butters, G. R. (1977). Equilibrium distributions of sales and advertising prices. *Review of Economic Studies, 44*(3), 465.

Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). New York: Routledge.

Callon, M. (1986). Some elements of a sociology of translation: Domestication of the Scallops and the fishermen of St Brieuc Bay, in Law, J. (ed.) *Power, action and belief: A new sociology of knowledge,* 196–233. London: Routledge.

Callon, M. (2007). Actor-network theory: The market test, in Asdal, K., Brenna, B., & Moser, I. (Eds.). *Technoscience: The politics of interventions*, 273-286. Oslo Academic Press.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment,* (Vol. 17). Thousand Oaks, CA: Sage Publications.

Carvalho, C. M. (2015). Regression and model selection: Book chapters 3 and 6. Retrieved from University of Texas at Austin website: http://faculty.mccombs.utexas.edu/carlos.carvalho/teaching/Sec2_Regression.pdf

Chen, M., Gonzalez, S., Leung, V., Zhang, Q., & Li, M. (2010). A 2G-RFID-based e-healthcare system. *Wireless Communications, IEEE, 17*(1), 37-43.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Ed.), Modern methods for business research.

Clarke, E., Mansour, O., Foley, E., & Patel, R. (2013). P2. 152 Giving patients what they want: Disclosure advice for sexually transmitted infections and information on legal redress following infection. *Sexually Transmitted Infections*, *89*(1), A134-A134.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2), 60-67.

Corbett, S. (2013). The retention of personal information online: A call for international regulation of privacy law. Computer Law & Security Review, 29(3), 246-254.

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*(2), 73-91.

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.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *Management Information Systems Quarterly, 33*(4), 673-687.

Daniels, K., Gillett, W., & Grace, V. (2009). Parental information sharing with donor insemination conceived offspring: A follow-up study. *Human Reproduction, 24*(5), 1099-1105.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Dawes, J. (2008). Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales. *International Journal of Market Research, 50*(1), 61–77.

Dawson, J. (2016). Interpreting interaction effects. Retrieved from www.jeremydawson.co.uk/slopes.htm

Derlaga, V. J., & Berg, J. H. (1987). *Self-disclosure: Therapy, research, and therapy*. New York: Plenum Press.

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. (2012). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295-316.

Doohwang, L., & LaRose, R. (2011). The impact of personalized social cues of immediacy on consumers' information disclosure: A social cognitive approach. *CyberPsychology, Behavior & Social Networking, 14*(6), 337-343.

Dziuban, C. D., & Shirkey, E. C. (1974). When is a correlation matrix appropriate for factor analysis? Some decision rules. *Psychological Bulletin, 81*(6), 358-361.

Ellis, T. J., & Hafner, W. (2007). *Control structure in project-based asynchronous collaborative learning.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Elmore, P. B., & Beggs, D. L. (1975). Salience of concepts and commitment to extreme judgments in the response patterns of teachers. *Education, 95*(4), 325-330.

EMC Website. (2015). The EMC privacy index. http://www.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf

EPIC Website. (2013a). European Parliament Committee approves comprehensive privacy law. http://epic.org/privacy/intl/eu_data_protection_directive.html

EPIC Website. (2013b). *23 US NGOs support EU data protection regulation*. https://epic.org/2013/10/23-us-ngos-support-eu-data-pro.html

Ericsson Consumer Report. (2013). *Personal information economy: Consumers and the evolution commercial relationships*. Retrieved from http://www.ericsson.com/ res/docs/ 2013/consumerlab/personal-information-economy.pdf

European Union Website. (2013). *The increasing use of portable computing and communication devices and its impact on the health of EU workers*. Retrieved from https://osha.europa.eu/data/links/the-increasing-use-of-portable-computing-and-communication-devices-and-its-impact-on-the-health-of-eu-workers

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods, 4*(3), 272.

Fairchild, A. J., & MacKinnon, D. P. (2009). A general model for testing mediation and moderation effects. *Prevention Science, 10*(2), 87-99.

Feuer, M. J., Towne, L., & Shavelson, R. J. (2002). Scientific culture and educational research. *Educational researcher, 31*(8), 4-14.

Floyd, F. J., & Widaman, K. F. (1995). Factor analysis in the development and refinement of clinical assessment instruments. *Psychological assessment, 7*(3), 286.

Foddy, W. H. (1984). A critical evaluation of Altman's definition of privacy as a dialectical process. *Journal for the Theory of Social Behaviour, 14*(3), 297-307.

Gabisch, J. A., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *The Journal of Consumer Marketing, 31*(1), 13-26.

Gantmakher, F. R. (2000). *The theory of matrices*, 1, Providence, RI: American Mathematical Society.

Haans, A., Kaiser, F. G., & de Kort, Y. A. W. (2007). Privacy needs in office environments: Development of two behavior-based scales. *European Psychologist, 12*(2), 93-102.

Häyrinen, K., Saranto, K., & Nykänen, P. (2008) Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 77(5), 291-304.

Gertler, E. L. (1994). *Prying eyes: Protect your privacy from people who sell to you, snoop on you, and steal from you*. New York: Random House.

Girden, E. R., & Kabacoff, R. I. (2011). *Evaluating research articles: From start to finish,* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science, 57*(1), 57-71.

Govtrack Website (2013). SB. 24: Personal information: Privacy. https://www.govtrack.us/states/ca/bills/2011-2012r/sb24

Gregor, S. (2006). The nature of theory in information systems. MIS Quarterly, 611-642.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-152.

Halbesleben, J. R. B., Whitman, M. V., & Crawford, W. S. (2014). A dialectical theory of the decision to go to work: Bringing together absenteeism and presenteeism. *Human Resource Management Review, 24*(2), 177-192.

Harris, P. B., Werner, C. M., Brown, B. B., & Ingebritsen, D. (1995). Relocation and privacy regulation: A cross-cultural analysis. *Journal of Environmental Psychology, 15*(4), 311-320.

Harris Interactive, & Westin, A. (2002). Privacy on and off the Internet: What consumers want. *Privacy and American Business,* 1-127.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods, 1*(1), 104-121.

Hoaglin, D. C., & Iglewicz, B. (1987). Fine-tuning some resistant rules for outlier labeling. *Journal of the American Statistical Association, 82*(400), 1147-1149.

Hoerbst, A., & Ammenwerth, E. (2010). Electronic health records. *Methods of Information in Medicine, 49*(4), 320-336.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85.

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

Hooper, D., Coughlan, J. & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. *The Electronic Journal of Business Research Methods 6*(1), 53-60.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

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.

Hunt, S. D., Sparkman Jr, R. D., & Wilcox, J. B. (1982). The pretest in survey research: Issues and preliminary findings. *Journal of Marketing Research*, 269-273.

IGP Website. (2013). The core Internet institutions abandon the US government. Retrieved from http://www.internetgovernance.org/2013/10/11/the-core-internet-institutions-abandon-the-us-government

Ivanhoe, P.J., & Van Norden, B. W. (2005). Readings in classical Chinese philosophy (2nd ed.). Indianapolis, IN: Hackett Publishing.

Jamal, K., Maier, M., & Sunder, S. (2005). Enforced standards versus evolution by general acceptance: A comparative study of e-commerce privacy disclosure and practice in the United States and the United Kingdom. *Journal of Accounting Research*, *43*(1), 73-96.

Jamieson, L. F., & Bass, F. M. (1989). Adjusting stated intention measures to predict trial purchase of new products: A comparison of models and methods. *Journal of Marketing Research, 26*(3), 336-345.

Jianqing, C., & Stallaert, J. (2014). An economic analysis of online advertising using behavioral targeting. *MIS Quarterly, 38*(2), 429-A427.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858-873.

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*(2), 177-192.

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.

Jöreskog, K.G. & Sörbom, D. (1984). *LISREL-VI user's guide* (3rd ed.). Mooresville, IN: Scientific Software.

Judd, C. M., & Kenny, D. A. (1981). Process analysis estimating mediation in treatment evaluations. *Evaluation review, 5*(5), 602-619.

Kacmar, K. M., & Carlson, D. S. (1997). Further validation of the perceptions of politics scale (POPS): A multiple sample investigation. *Journal of management, 23*(5), 627-658.

Kauffman, R. J., Lee, Y. J., & Sougstad, R. (2009). *Cost-Effective Investments in Customer Information Privacy*. Paper presented at the System Sciences, HICSS '09. 42nd Hawaii International Conference on.

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies, 71*(12), 1144-1162.

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. (2005). Cognition-based versus affect-based trust determinants in e-commerce: Cross-cultural comparison study," in Proceedings of the 26th International Conference on Information Systems, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, 741-753.

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.

Kumaraguru, P., & Cranor L. F. (2005). Privacy indexes: A survey of Westin's studies. *Technical Report*, Carnegie Mellon University CMU-ISRI-5-138, 2015.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*: Harvard University press.

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.

Laurenceau, J.-P., Barrett, L. F., & Pietromonaco, P. R. (1998). Intimacy as an interpersonal process: The importance of self-disclosure, partner disclosure, and perceived partner responsiveness in interpersonal exchanges. *Journal of Personality and Social Psychology, 74*(5), 1238-1251.

Lawshe, C. H. (1975). A quantitative approach to content validity1. *Personnel psychology, 28*(4), 563-575.

Le Dinh, T., Rinfret, L., Raymond, L., & Thi, B.-T. D. (2013). Towards the reconciliation of knowledge management and e-collaboration systems. *Interactive Technology and Smart Education, 10*(2), 95-115.

Lee, A. S. (2004). Thinking about social theory and philosophy for information systems. *Social theory and philosophy for Information Systems*, 1-26.

Lee, D. J., Ahn, J. H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. *MIS Quarterly, 35*(2), 423-444.

Lenth, R. V. (2001). Some practical guidelines for effective sample size determination. *The American Statistician, 55*(3), 187-193.

Lenth, R. V. (2006-9). *Java applets for power and sample size* [Computer software]. Retrieved November 1, 2015, from http://www.stat.uiowa.edu/~rlenth/Power

Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2004). *The Sage encyclopedia of social science research methods*. Thousand Oaks, CA: Sage Publications.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62-90.

Losses, G., & Discounting, H. (2004). Privacy attitudes and privacy behavior. *Economics of Information Security, 12*, 165-178.

Lynham, S. A. (2002). The general method of theory-building research in applied disciplines. Advances in Developing Human Resources, 4(3), 221-241.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods,1*, 130–49.

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.

Marshall, N. J. (1974). Dimensions of privacy preferences. *Multivariate Behavioral Research, 9*(3), 255-271.

Marsh, H. W., & Hau, K.-T. (1996). Assessing goodness of fit: Is parsimony always desirable? *The Journal of Experimental Education, 64*(4), 364-390.

Martin, B. A. S. (2004). Using the imagination: Consumer evoking and thematizing of the fantastic imaginary. *Journal of Consumer Research, 31*(1), 136-149.

Maxim, P. S. (1999). *Quantitative research methods in the social science*. New York: Oxford University Press.

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

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35-57.

Miles, M. B., & Huberman, M. A. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Beverley Hills: Sage.

Miller, G. A. (1951). *Language and communication*. New York: McGraw-Hill.

Milne, G. R., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment- and technology-level analysis. *Journal of Public Policy & Marketing, 29*(1), 138-149.

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers’ perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Moattar, K. (2014). How to avoid non-response bias. Retrieved from https://www.surveylegend.com/avoid-non-response-bias/

Moseley, A. (2005). Egoism. *Internet Encyclopedia of Philosophy*. Retrieved from http://www.iep.utm.edu/egoism/#SH2a

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76-98.

Mulaik, S. A., James, L. R., Van Alstine, J., Bennett, N., Lind, S., & Stilwell, C. D. (1989). Evaluation of goodness-of-fit indices for structural equation models. *Psychological Bulletin*, *105*(3), 430.

Newcomb, T. M. (1953). An approach to the study of communicative acts. *Psychological Review*, *60*(6), 393-404.

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology, 15*(2), 87-104.

Newsom, J. T. (2014). Data analysis II: Testing mediation with regression analysis. Retrieved from Portland State University website: http://www.upa.pdx.edu/IOA/newsom/da2/ho_mediation.pdf

Newton, R. R., & Rudestam, K. E. (1999). *Your statistical consultant: Answers to your data analysis questions*. Thousand Oak, CA: SAGE Publications.

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

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

OECD Website. (2015). OECD guidelines on the protection of privacy and transborder flows of personal data. Retrieved from http://www.oecd.org/internet/ieconomy /oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Offor, P. I. (2013). *Managing Risk in Secure System: Antecedents to System Engineers' Trust Assumptions Decisions*. Paper presented at the Social Computing (SocialCom), 2013 International Conference on, 478-485.

Oliver, R. L. (1977). Effect of expectation and disconfirmation on postexposure product evaluations: An alternative interpretation. *Journal of Applied Psychology, 62*(4), 480-486.

Oliver, R. L. (1980). A Cognitive Model of the Antecedents and Consequences of Satisfaction Decisions. *Journal of Marketing Research, 17*(4), 460-469.

Oostenbrink, J. B., Al, M. J., Oppe, M., & Rutten-van Mölken, M. P. M. H. (2008). Expected value of perfect information: An empirical example of reducing decision uncertainty by conducting additional research. *Value in Health, 11*(7), 1070-1080.

Osman, A., Barrios, F. X., Kopper, B. A., Hauptmann, W., Jones, J., & O'Neill, E. (1997). Factor structure, reliability, and validity of the Pain Catastrophizing Scale. *Journal of behavioral medicine, 20*(6), 589-605.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.

Palen, L., & Dourish, P. (2003). *Unpacking privacy for a networked world*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Park, H. M. (2008). Hypothesis testing and statistical power of a test. *The University Information Technology Services (UITS) Center for Statistical and Mathematical Computing*, Indiana University, 1-40.

Paswan, A. (2009). *Confirmatory factor analysis and structural equations modeling. An introduction*. Department of Marketing and Logistics, COB, University of North Texas, USA.

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17*(2), 147-156.

Petronio, S. (2012). Boundaries of privacy: Dialectics of disclosure. New York: Suny Press.

Pink, D. H. (2009). *Drive: The surprising truth about what motivates us*. New York: Penguin.

Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems*, 75-105.

Randolph, J. J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research & Evaluation, 14*(13), 2-13.

Rogers, T. B. (1995). *The psychological testing enterprise*. Pacific Grove, CA: Brooks-Cole Publishing Company.

Salkind, N. J. (2012). *Exploring research* (8th ed.). Boston: Prentice Hall.

Sayre, S., & Horne, D. (2000). Trading secrets for savings: How concerned are consumers about club cards as a privacy threat? *Advances in Consumer Research, 27*(1), 151-155.

Schwartz, P. M. (2009). Preemption and privacy. *The Yale Law Journal, 118*(5), 902-947.

Schwartz, P. M., & Solove, D. J. (2013). Reconciling personal information in the United States and European Union. *California Law Review, 102*(4), 877-916.

Schwartz, P. M., & Solove, D. J. (2014). Defining 'Personal Data' in the European Union and US. *Bloomberg BNA Privacy and Security Law Report, 13*, (1581), 1-6.

Schickedanz, A., Huang, D., Lopez, A., Cheung, E., Lyles, C. R., Bodenheimer, T., & Sarkar, U. (2013). Access, interest, and attitudes toward electronic communication for health care among patients in the medical safety net. *Journal of General Internal Medicine, 28*(7), 914-920.

Sekeran, U., & Bougie, R. (2009). *Research methods for business: A skill building approach* (5th ed.). Great Britain: John Wiley.

Sharma, S., Durand, R. M., & Gur-Arie, O. (1981). Identification and analysis of moderator variables. *Journal of Marketing Research*, 291-300.

Sivo, S. A., Saunders, C., Chang, Q., & Jiang, J. J. (2006). How low should you go? Low response rates and the validity of inference in IS questionnaire research. *Journal of the Association for Information Systems*, *7*(6), 351-414.

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

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

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly, 34*(3), 463-486.

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.

Spreng, R. A., MacKenzie, S. B., & Olshavsky, R. W. (1996). A Reexamination of the Determinants of Consumer Satisfaction. *Journal of Marketing*, *60*(3), 15-32.

State of California Website. (2013). Bill information: Daily updates Assembly and Senate bills. http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual Differences*, *42*(5), 893-898.

Steiger, J. H., & Lind, J. C. (1980). *Statistically based tests for the number of common factors.* Paper presented at the annual meeting of the Psychometric Society, Iowa City, IA.

Steward, B. (2004). Writing a literature review. *The British Journal of Occupational Therapy*, *67*(11), 495-500.

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

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*(3), 349-411.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(24), 380-427.

Sun, J., Zhang, Y., Tang, D., Zhang, S., Zhao, Z., & Ci, S. (2015, 8-12 June 2015). *TCP-FNC: A novel TCP with network coding for wireless networks.* Paper presented at the 2015 IEEE International Conference on Communications (ICC).

Sutanto, J., Palme, E., Chuan-Hoo, T., & Chee Wei, P. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141-A1145.

Swanson, R. A., & Chermack, T. J. (2013). *Theory building in applied disciplines*. San Francisco, CA: Berrett-Koehler Publishers.

Symantec Report. (2010). Symantec global Internet Security report. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

Takahashi, T., Nakano, M., & Shinohara, S. (2010). Cognitive symmetry: Illogical but rational biases. *Symmetry: Culture and Science, 21*(1-3), 275-294.

Tan, F. B., & Hunter, M. G. (2002). The repertory grid technique: A method for the study of cognition in information systems. *MIS Quarterly, 26*(1), 39-57.

Tejay, G. (2008). *Shaping strategic information systems security initiatives in organizations* (Doctoral dissertation, Virginia Commonwealth University), Retrieved from https://dizzyg.library.vcu.edu/bitstream/handle/10156/2259/Tejay-ShapingStrategicSecurity.pdf?sequence=1

The U.S. Census Bureau, Department of Commerce, Washington DC. (2014). Quarterly retail ecommerce sale: Fourth quarter 2013. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review, 4*(3), 356-367.

Toulemon, L., & Testa, M. R. (2005). Fertility intentions and actual fertility: A complex relationship. *Population & Societies, 415*, 1-4.

Trochim, W. M. (2000). Research methods knowledge base. Retrieved from http://www.socialresearchmethods.net/kb/unitanal.php

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

Tucker, C. E. (2012). The economics of advertising and privacy. *International Journal of Industrial Organization, 30*(3), 326-329.

Ullman, J. B., & Bentler, P. M. (2012). *Structural equation modeling handbook of psychology*, (2nd ed.). New York: John Wiley & Sons

U.S. Government Accounting Office—GAO. (2013). *Information resellers: Consumer privacy framework needs to reflect changes in technology and the marketplace*. Retrieved from http://www.gao.gov/products/GAO-14-251T

U.S. Government Accounting Office—GAO-02-404. (2002). *International electronic commerce: Definitions and policy implications*. Retrieved from http://www.gao.gov/products/GAO-02-404

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

Vernon, D., Metta, G., & Sandini, G. (2007). A survey of artificial cognitive systems: Implications for the autonomous development of mental capabilities in computational agents. *Evolutionary Computation, IEEE Transactions on, 11*(2), 151-180.

Vezzali, L., Capozza, D., Giovannini, D., & Stathi, S. (2012). Improving implicit and explicit intergroup attitudes using imagined contact: An experimental intervention with elementary school children. *Group Processes & Intergroup Relations*, *15*(2), 203-212.

Vogt, W. P. (2005). *Dictionary of statistics and methodology: A nontechnical guide for the social sciences,* (3rd ed.). Thousand Oaks, CA: Sage

Vogt, W. P., & Johnson, R. B. (2016). *Dictionary of statistics and methodology: A nontechnical guide for the social sciences*, (5th ed.). Los Angeles, CA: Sage

Ward, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13-28.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Werner, C. M., Brown, B. B., & Altman, I. (2004). Privacy. In C. D. Spielberger (Ed.), *Encyclopedia of Applied Psychology* (pp. 109-119). New York: Elsevier.

Westin, A. (1970). *Privacy and freedom*. New York: Atheneum.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431-453.

Wilson, F. R., Pan, W., & Schumsky, D. A. (2012). Recalculation of the critical values for Lawshe’s content validity ratio. *Measurement and Evaluation in Counseling and Development, 45*(3), 197-210.

Wu, A. D., & Zumbo, B. D. (2008). Understanding and using mediators and moderators. *Social Indicators Research, 87*(3), 367-392.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. International Conference on Information Systems, 1-16.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push—pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-173.

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.

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.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems, 48*(2), 395-406.