

2015


Affect and Online Privacy Concerns

David Charles Castano

Nova Southeastern University, castada1@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Databases and Information Systems Commons](#), [Psychology Commons](#), and the [Quantitative, Qualitative, Comparative, and Historical Methodologies Commons](#)

Share Feedback About This Item

NSUWorks Citation

David Charles Castano. 2015. *Affect and Online Privacy Concerns*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (41)
https://nsuworks.nova.edu/gscis_etd/41.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Affect and Online Privacy Concerns

By:

David C. Castano

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

The Graduate School of Computer and Information Science
Nova Southeastern University

2015

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

Affect and Online Privacy Concerns

By
David C Castano

The purpose of this study was to investigate the influence of affect on privacy concerns and privacy behaviors. A considerable amount of research in the information systems field argues that privacy concerns, usually conceptualized as an evaluation of privacy risks, influence privacy behaviors. However, recent theoretical work shows that affect, a pre-cognitive evaluation, has a significant effect on preferences and choices in risky situations. Affect is contrasted with cognitive issues in privacy decision making and the role of affective versus cognitive-consequentialist factors is reviewed in privacy context.

A causal model was developed to address how affect influences privacy concerns and privacy behaviors. The model of privacy risk proposed in this model argues that affect (or “feelings”) influences privacy behaviors directly as well as thru privacy concerns.

To test the model, subjects were recruited using Mechanical Turk and paid for their participation. Affect, the key construct in this research, was measured using a word association technique as well as methods developed in the implicit attitudes research. Well-known scales were used to measure privacy concerns and behavioral intentions. Data was collected from subjects using a pretested privacy scenario.

Data analysis suggests that, in line with published IS research, privacy concerns affect privacy behaviors. Affect has no impact on privacy concerns nor on privacy behaviors at the traditional 5% level of significance, though it is significant at the 10% level of significance. Improving the instruments used to measure affect, use of a large sample size to detect small effect sizes and more control over the instrument administration instead of an online survey are suggested for future research.

Acknowledgements

Many years of hard work, none of which would have been possible without the support of colleagues, friends and family. First, I want to thank my dissertation chair, Dr. Easwar Nyshadham, who believed in me even when I was struggling and frustrated. His years of support, patience, insight, guidance and encouragement were some of the reasons I continued with this work. I would also like to thank my dissertation committee member, Dr. Souren Paul and Dr. Gerry van Loon for their insight and suggestions, which helped to strengthen the quality of this research.

I would also like to thank all of my NSU colleagues who supported my effort and were there when I needed them: John Bono, Abbe Foreman, Lisa Dabkowski Van Zanten, Sally Sue Richmond, Nanette Poulos, Kim Calabrese and many others. Especially, a big thanks to the late Kim Calabrese who encouraged me from the beginning to take on this work and she supported until the end. From studying together, bouncing ideas off each other and guidance along the way was invaluable.

I would like to thank my dear friends, especially Linda Beney who was always there when I was struggling and helped me to stay on track. Katherine Stanley-Cava, who understood the work and effort it requires to write, your support was golden. Keith and Melinda Mernovage, who always provided some insight and constant support even when I lost my way. Philip Jenkins and Lesley Holliday who always gave me a little boost when I needed it. I am also grateful to all my friends and family in Michigan and Texas for your support along the way.

I would also like to thank my mother, Gloria Castano, and brother, Michael Castano, for their constant cheerleading. Always sharing my steps along the way, you gave me the strength to keep moving forward.

Most importantly, I want to thank my partner, Rick De Francesco. His constant support, patience and love in supporting my dream gave me the strength to continue. Without your help with refining my ideas and getting beyond my roadblocks, I could not have done this work. You were there every moment of the way and you kept me going. I am so lucky to have you in my life to see my dream come true.

Table of Contents

Abstract iii
List of Tables vii
List of Figures viii

Chapters

1. Introduction 1
 Background
 Problem Statement 2
 Research Goals 4
 Research Questions, Hypotheses and Models 9
 Relevance and Significance 16
 Barriers and Issues 17
 Assumptions, Limitations and Delimitations 18
 Definition of Terms 19
 Summary 21

2. Review of Literature 22
 Overview 22
 Affect 22
 Implicit Attitudes 25
 Privacy Concerns 29
 Privacy Calculus 33
 Privacy Paradox 33

3. Methodology 35
 Overview 35
 Research Method 35
 Data Collection Procedures 37
 Participants 47
 Results Analysis 48
 Anticipated Difficulties 51
 Resource Requirements 51

4. Results 53
 Overview 53
 Pre-Analysis Data Screening 53
 Descriptive Analysis 54
 Measurement Model Analysis of Affect 55
 Measurement Model Analysis of Privacy Concerns and Behavioral Intentions 57
 Structural Model Analysis of Affect, Privacy Concerns and Behavioral Intentions 60
 Summary of Results 63

5. Conclusions, Implications, Recommendations, and Summary 66

- Overview 66
- Conclusion 66
- Implications 70
- Recommendations for Future Research 70
- Summary 71

Appendices 74

- A. Introduction 74
- B. Word Association Test 75
- C. Single Category Implicit Attitude Test 76
- D. Attitude Object Words used in the SC-IAT 77
- E. Target Object Words used in the SC-IAT 78
- F. Privacy Concerns Survey 79
- G. Behavior Intentions Survey 82
- H. Demographics Survey 83
- I. IRB Approval Letter from Nova Southeastern University 84
- J. Mturk Advertisement 85
- K. Overview and Loadings of Second Order PC and First Order BI Constructs 86
- L. Cross Loadings of Second Order PC, First Order PC and First Order BI Constructs 88
- M. Fornell-Larcker Discriminant Validity for PC 89
- N. Overview, Loadings and Weights of First Order AFF on Second Order PC and First Order BI Constructs 90
- O. Path Coefficient of First Order AFF on Second Order PC and First Order BI Constructs 93
- P. Cross Loadings of First Order AFF on Second Order PC and First Order Bi Constructs 94
- Q. Outer Loadings and Weights Mean, SD & T Stats of First Order AFF on Second Order PC and First Order BI Constructs 95
- R. Latent Variable Correlations of First Order AFF on Second Order PC and First Order BI Constructs 98
- S. Frequency Histograms for the z score of Aff1 and Aff2 99
- T. Outlier Boxplot of Aff1 and Aff2 101

References 102

List of Tables

Tables

1. Comparison of the Implicit Association Test (IAT) and Single Category IAT (SC-IAT) 29
2. Construct, Indicators and Measures of Affect 42
3. Survey Items for Privacy Concerns 43
4. Survey Items for Behavioral Intentions 46
5. Frequencies and Percentages of Demographic Data ($N = 80$) 55
6. Descriptive Statistics of Raw Scores of Aff1_WAT and Aff2_IAT 56
7. Pearson Correlation Results 57
8. Reflective Measurement Model Results of First Order Constructs 59
9. Collinearity Statistics of AFF and BI Constructs 61
10. Path Coefficient and Significance of AFF, PC and BI Constructs 61
11. Coefficient of Determination and Relevance of AFF and PC Constructs on BI Construct 63
12. Effect size f^2 of BI 63
13. Summary of Findings for Research Hypotheses 64

List of Figures

Figures

1. Cognitive versus Affective Approaches to a Privacy Decision 8
2. Current Cognitive Consequentialist Model of Privacy Concerns 9
3. Conceptual Model 1 – The Influence of Privacy Concerns and Affect on Behavioral Intentions 10
4. Illustration of Affective Processing 13
5. Conceptual Model 2 – The Influence of Affect on Privacy Concerns 15
6. Conceptual Model 3 - Privacy Concerns Mediating the Influence of Affect on Behavioral Intentions 16
7. Four Models of IS Risk 25
8. Conceptual Model of the Antecedents and Outcomes of Privacy Concerns 32
9. Structural and Measurement Model of the Influence of Affect on Privacy Concerns and Behavioral Intentions 36
10. Data Collection Procedure Website Flow Chart 38
11. Scenario 39
12. Measurement Model of PC and BI 59
13. Structural Model of Affect, Privacy Concerns and Behavioral Intentions 62

Chapter 1

Introduction

Background

The threat of losing control of private information online raises consumers' privacy concerns. When the news media announces a security breach of significant magnitude such as the recent "credit card skimming" incident at a major grocery store in November 2011 (Liebowitz, 2011), the consumer has to think about how to protect their personal information (Dinev & Hart, 2006b). This study examined the consumer's affective reaction to privacy threats instead of solely relying on traditional cognitive methods.

Consumers minimize their risk of losing control of personal information by taking advantage of online methods and tools. For example, consumers can help mitigate potential threats by reading website privacy policies and software license agreements. As well as managing cookie settings on Internet browser applications and by updating and running software that provides computer virus protection (Rifon, LaRose, & Lewis, 2007). Consumers can also subscribe to an online service that performs regular backups of a user's data and store those backups in an encrypted environment. Understanding privacy protection methods can help consumers make informed decisions about the best way to ensure sufficient protection of personal information on the Internet (John, Acquisti, & Lowenstein, 2011; Rifon et al., 2007).

Protecting privacy requires a trade off or the tolerance for the delay of a positive outcome to avoid any negative outcomes (Culnan & Armstrong, 1999; Rifon et al, 2007;

Smith et al., 2011). For example, if a person does not engage in sharing personal information, such as an email address on a social network website, then that person will minimize privacy risks. Because most social network websites require email addresses, the consumer will not have the benefit of participating. If the consumer is willing to disclose information, the consumer could use a privacy calculus to arrive at an appropriate tradeoff (Culnan & Armstrong, 1999, Smith et al., 2011).

A privacy calculus requires an assessment of informational factors (e.g., economic, social, environmental, etc.) that a consumer would weigh to ensure a benefit and avoid negative consequences (Culnan & Armstrong, 1999; Smith et al., 2011). While users are assumed to utilize a privacy calculus that will result in the most favorable outcome (John et al., 2011; Rifon et al., 2007; Smith et al., 2011), research suggests that this is not always the case. Empirical observations of the privacy paradox have shown that users behave in ways that do not match stated intentions (Belanger & Crossler, 2011; Rifon et al., 2007; Smith et al., 2011).

Problem Statement

The cognitive consequentialist models assumption is that people deliberately evaluate the cost and benefits prior to a risky activity (Nyshadham & Minton, 2013). This research pointed out that these current models of a consumer's privacy concerns and intentions do not adequately predict privacy behaviors and then addressed the need to add the role of affect in privacy decision-making. John et al. (2012) stated "individual measures of privacy preference have generally failed to predict privacy-related behaviors" and they examined the contextual factors as a possible explanation for this divergence. These findings, along with the privacy paradox, suggest that current privacy

concern measurements are inadequate since the privacy calculus is cognitively measured and does not account for the role of emotion in the decision.

Privacy concerns, as a measurable proxy for privacy, are a central construct in privacy measurements (Belanger & Crossler, 2011). Most studies use one of two scales:

- Concerns for Information Privacy (CFIP) developed by Smith et al. (1996). CFIP includes four related dimensions of privacy concerns: collection, errors, secondary use, and unauthorized access to information.
- Internet User Information Privacy Concerns (IUIPC) developed by Malhotra et al. (2004). IUIPC includes three dimensions of privacy concerns: control, awareness, and collection.

Subsequent research has consistently relied on CFIP as the preferred measure for information privacy concerns (Belanger & Crossler, 2011; Dinev & Hart, 2004; Hoadley, Xu, Lee & Rosson, 2010; Korzan and Boswell, 2008). Organizing existing research on information privacy Smith et al. (2011) created a macro model, Antecedent->Privacy Concern->Outcomes (APCO). Within the APCO model, antecedents of the privacy decision (e.g. privacy experiences, privacy awareness, etc.) affect privacy concern (i.e., central construct) resulting in outcomes such as behavioral reactions, privacy risk and benefits and regulations.

Recent research by Hong and Thong (2012) identified inconsistencies in privacy concern research and utilized Multidimensional Development Theory (MDT) to develop the Internet Privacy Concerns (IPC) with six dimensions: collection, secondary usage, errors, improper access, control, and awareness. Li (2011) constructed a framework, based on a review of 15 established theories (i.e. Theory Reasoned Action, Theory of

Planned Behavior, etc.) that outline the relationship between privacy antecedents, privacy beliefs, privacy-driven behavioral intentions and privacy behaviors.

Current privacy concern scales have addressed privacy risk (i.e. personal information loss) and shown that people use a privacy calculus, a cognitive-consequentialist trade-off of costs and benefits, to arrive at a net benefit. Inconsistencies in privacy concern research such as the privacy paradox and contextual factors suggest existing privacy concern measurements are inadequate because they do not account for emotion and feeling. Recent research on human decision making shows that emotion and reason do interact strongly in decision making and the specific role of affect as “a faint whisper of emotion” (Slovic, Finucane, Peters & MacGregor, 2004) has an important effect on risk perception and evaluation (Nyshadham & Castano, 2012).

Research Goals

Currently, instruments that evaluate risk perception have used the psychometric paradigm to judge the riskiness of hazardous activities, technologies, and substances to arrive at a balance between risk and benefits (Slovic, 1986; Slovic, 2010). The emphasis of emotion on reason has changed the view that people judge risk deliberately and consciously (Nyshadham & Castano, 2012). Hence, new concepts exist in the area of risk perception and evaluations.

Slovic et al. (2005) and Lowenstein, Weber, Hsee and Welch (2001) provided a characterization of risk perception in terms of affect and feeling. Slovic et al. (2005) suggested that affect guides perception of risk and benefit. For example, if a person has a positive affect toward an activity, they will conclude that the risk is low and benefit is high. If a person has a negative affect toward an activity, they will judge the risk as high

and benefit as low. Affective evaluations tend to take place automatically without much thought and are usually the first evaluable reaction to stimuli.

This research focused on an integral affect that is associated with an individual's response to a stimulus based on an object or a word. This approach is distinct to the work of Slovic's (2010), which uses the term "affect" to refer to an evaluative feeling caused by a stimulus and does not refer to affect as a strong emotion or mood.

Based on thoughtful deliberation of risks and benefits, privacy concern scales have been developed in a cognitive-consequentialist approach. This paper focused on how "affect" plays a fundamental role in online privacy risk decision making and in some situations may supersede deliberate evaluations. The primary goals of this research were:

1. Conceptualize privacy risk in terms of affect.
2. Compare and contrast affective and cognitive view of privacy decision-making.
3. Understand the role of affective vs. cognitive-consequentialist factors on privacy concerns and privacy behaviors.

The following scenario illustrates the argument that affect does indeed help drive decision-making on issues of risk and privacy. This hypothetical scenario assumed a well-known online hazard of the aggregation of private information from multiple sources (Nyshadham & Gabriel, 2011). A recent privacy policy change allows Google to integrate its data on all Google services. This can benefit Google because it will correlate a user's search patterns across services and offer more customized advertisements, while the user has the benefit of a single log-on and consistent experience. Google communicated the policy change extensively through various media and gave users the

choice to opt-in by agreeing to the new policy or opt-out and stop using Google services.

Two hypothetical narratives discuss how consumers decided which option to choose:

The Cognitive-consequentialist Account

The “cognitive-consequentialist approach” assumes that people are rational, have privacy concerns and use a privacy calculus to evaluate the pros and cons of accepting Google’s new policy.

John is a long time Google user and his response to Google’s privacy policy reflects the cognitive-consequentialist account. John has the choice to accept the new policy or terminate using Google services (see Figure 1). John would deliberate long and hard about this decision. He would examine Google’s current privacy policy and then carefully evaluate the changes that the new policy would provide. For example, he would rate the changes using six dimensions of privacy concern (Hong & Thong, 2012). He might consider using more detailed evaluations of sub-scales, score the instrument and arrive at an overall privacy score. One way for John to arrive at a privacy score is to develop a multi-attribute table with various items and score for the difference (e.g., does the new policy rate better or worse than the old policy?). John might have a well-developed set of weights to attach to each attribute (i.e., he has well-defined preferences). He then computes an overall score for the new versus old policies. If the score is positive, so that the new policy is better, he could simply sign up for the new services. If his score is negative and the multi-attribute table score indicates that the old policy is better, he could evaluate the pros and cons of giving up some privacy versus stopping using Google services altogether. This description of John’s decision-making process is consistent with most theories developed by work in privacy concerns, in that the process

follows a privacy calculus and follows a general online risk perception context (Glover & Benbasat, 2011).

The Affect Account

The affect approach assumes that people will respond emotionally to the announcement that Google plans to change its policy.

Mark is also a long-time Google user and he follows an affect mode of evaluation. He would evaluate the announcement that “Google changes its privacy policy” using a heuristic described in Figure 1. Mark feels that he knows Google and considers that Google “does no harm.” Mark knows that change in general requires an adjustment and he considers the proposed Google privacy change “bad.” He knows what a “Privacy Policy” consists of but has never really read one completely. He neither fully understands the current Google privacy policy nor the proposed change in the Google privacy policy. He would thus use a heuristic in which:

- Google is perceived to be a “good” thing (+1)
- Change is a “bad” thing (-1)
- Privacy policy is a “neutral” thing (0)

He scores the three terms in the list as +1, -1 and 0 and computes the overall effect of changes as zero. Thus, he does not have any concern with accepting the changes to the privacy policy and signs up with the new policy. It is possible that he might have different scores so that the “net” score might be positive or negative. In general, he might seek further information if the net score is negative and if the net score is neutral or positive; do nothing.

Mark then is using an affective evaluation of the change to guide his decision. A good-bad evaluation of the stimulus happens automatically and probably unconsciously. His perception is affect-laden and does not exist independently of affect (e.g., people do not just see a house; people see a “beautiful” or “ugly” house). This affect-laden perception influences further information acquisition and processing.

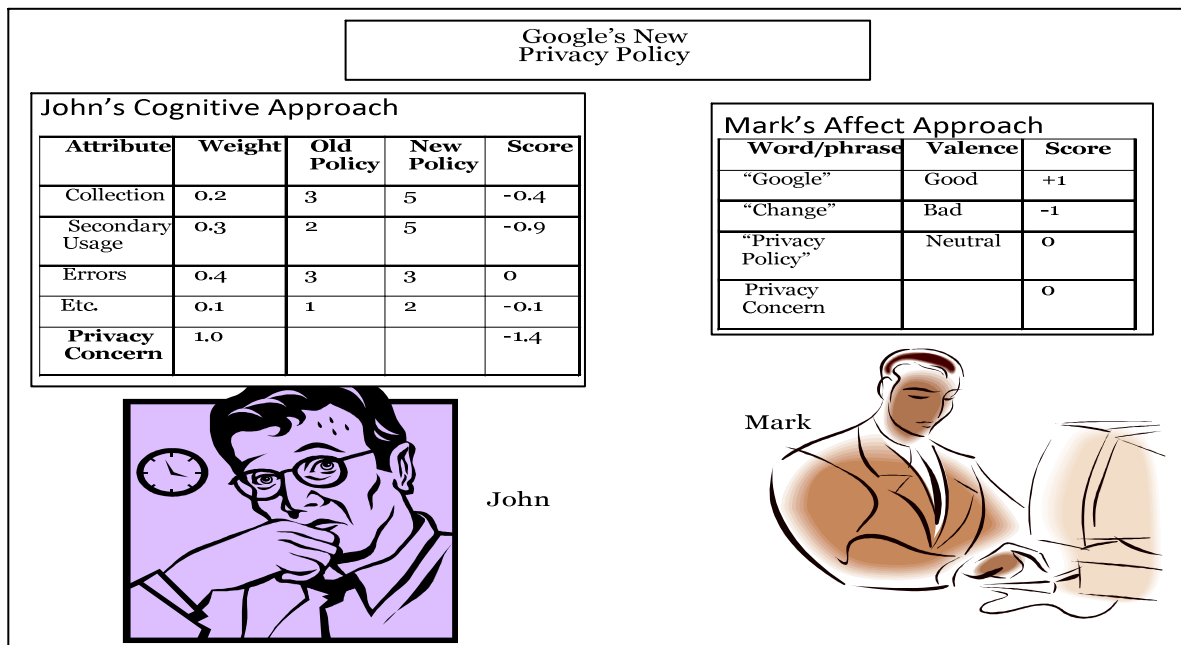


Figure 1. Cognitive versus Affective Approaches to a Privacy Decisions

Research Questions, Hypotheses and Models

Current cognitive consequentialist models (i.e. CFIP, IUIPC and IPC) suggest that privacy concerns influence privacy behaviors. Because of the complexity of and inconsistencies in defining and measuring privacy, the models have measured privacy using privacy concerns as a proxy (Smith et al., 2011; Xu, Dinev, Smith & Hart, 2011). Furthermore, because privacy behaviors are difficult to measure, behavioral intentions were measured (Malhotra et al., 2004, Smith et al., 2011) in this research. As shown in Figure 2, the relationship between privacy hazards, privacy concerns (PC) and behavioral intentions (BI) has been the accepted approach in online privacy concern research.

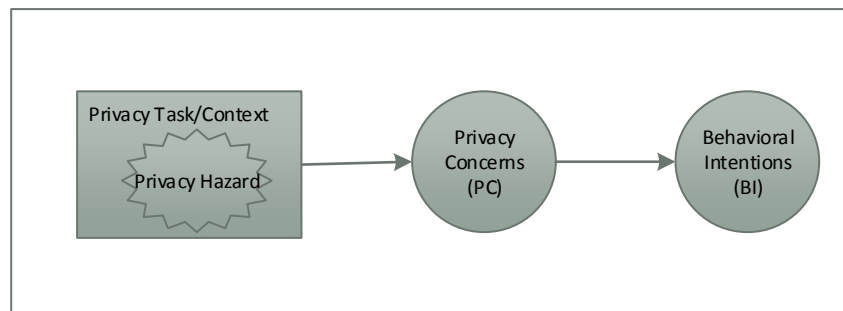


Figure 2. Current Cognitive Consequentialist Model of Privacy Concerns

Smith et al.'s (2012) APCO model demonstrates how previous research and developed models address antecedents and outcomes of privacy concerns. Based on this information the hypotheses are as follows:

H1a: Higher privacy concerns lead to less disclosure of private information online (a privacy behavioral intention)

H1b: Lower privacy concerns lead to more disclosure of private information online (a privacy behavioral intention)

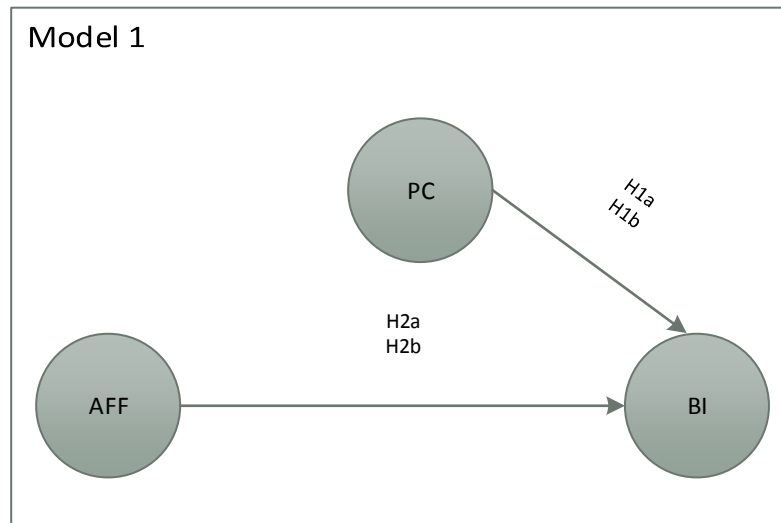


Figure 3. Conceptual Model 1 - The Influence of Privacy Concerns and Affect on Behavioral Intentions

Privacy concerns are not the only antecedents to influence behavioral intentions (i.e., privacy behavioral intentions). An approach to utilize a simple procedure, called a heuristic technique, helps people find an adequate answer to a difficult question (Kahneman, 2011). Slovic's (2010) affect heuristic proposal suggests that people look for an easier approach to answering difficult questions. Using a readily available affective decision can be easier and more efficient than weighing the pros and cons of various reasons. Kahneman refers to the heuristic technique as a mental shortcut of consulting their affect pool and substituting a difficult question with a much easier one. For example, "How do I feel about it?" serves as an answer to a much harder question, "What do I think about it?" (Kahneman, 2011, p.139). Slovic (2007) suggest that people allow their likes and dislikes to determine their beliefs and perceptions of risk and benefits. A study by Finucane, Alhakami, Slovic and Johnson (2000) found that the inverse relationship between the perceived risk and perceived benefits of an activity was linked to the strength of positive or negative affect associated with an activity. This implied that

people base their judgments not only on what they think about it but also on how they feel about it (Slovic, 2007). If they like the activity, they will judge it more favorably. If they do not like the activity, they will judge it less favorably. For example, if a person has a political party preference that does not support universal healthcare, he or she would judge a universal health bill unfavorably. If the person likes the political party and the party supports it, the bill might be judged as having huge benefits and negligible risk. Based on Slovic's work, the affect heuristic would have influence on privacy behavior suggesting the following hypotheses: (see Figure 3)

H2a: Negative affect leads to lower disclosure (a privacy behavioral intention)

H2b: Positive affect leads to a higher disclosure (a privacy behavior intention)

Affect plays a key role in risk perception and decision processing. Under the psychometric paradigm, a person's perception is distinguished by its amount of affect (Nyshadham & Gabriel, 2011). According to Zajonc (1980), all perceptions contain some affect and affective reactions are inescapable and uncontrollable. Zajonc argues that affective reactions to stimuli are often the very first reactions, "we don't just see a house, but a 'beautiful' house or an 'ugly' house" (p.154). After a stimulus event occurs, the first observations are typically involuntarily controlled. According to Zajonc, "we may fail to notice a person's hair color, but we can seldom escape the reaction that the person impressed upon us as unpleasant or pleasant, agreeable or disagreeable" (p.156).

In Epstein's (1994) dual-process theory, the experiential system that is characterized as intuitive, automatic, natural and non-verbal is assumed to be closely associated with the experience of affect. After a person responds to a stimulus, the person automatically searches emotionally-laden memories that might influence decision-making. Relying

more heavily on affect is quicker and easier than relying on cognitive analysis (Slovic, 2010).

Based on the work in neuroscience literature, Damasio (1994) suggested that thoughts are constructed of images that consist of sounds, smell, real and imagined visual impressions, ideas, and words. These images marked with positive and negative feelings and linked directly or indirectly to bodily states are referred to as somatic markers (Damasio, 1994). The collection of these images contains all the positive and negative tags associated with the representations consciously or unconsciously that are accessed in the process of making decisions from the “affect pool.” In the “Affect Account” scenario, the concept of core affect is introduced (Barret & Bliss-Moreau, 2009) in which Mark might instantly and without awareness respond to the images based on three key words (Google, change and privacy policy). He consults with his “affect pool” on whether each word raises a concern (arousal) and the strength of his accompanying feeling (valence).

The research conducted by Barret and Bliss-Moreau (2009), based on the studies by Wundt (1897), suggest that affective states have specific qualities: pleasantness/unpleasantness (valence), arousing/subduing (arousal) and strain/relaxation (intensity). Current research on core affect considers the state of pleasure or displeasure with some degree of arousal (Barret & Bliss-Moreau), concluding essentially that people cannot feel pleasant or unpleasant without feeling some level of arousal. As depicted in Figure 1, in Mark’s case, “Google” might raise a positive affect (+1) and “change” might raise a negative affect (-1). Because Mark has not paid any attention to a privacy policy, “privacy policy” might not raise any privacy concern at all. An affect measure using (+1)

for “Google”, (-1) for “change” and (0 or neutral) for “privacy policy” results in an overall total affect and feeling that is neither good/positive/pleasant nor negative/bad/unpleasant. The approach of this scenario suggests that a decision based on a privacy hazard (e.g., dotted line from privacy hazard to affect pool) that has a positive affect (e.g., dotted line from affect pool to final affect) would influence the user to assert a positive benefit and low risk based on the feelings of the imagery from the affect pool (see Figure 4). How the affect pool is processed would be addressed in the neuroscience domain, but in this case, an overall positive net affect (valence) on a specific stimulus would be the influencing factor for the outcome.

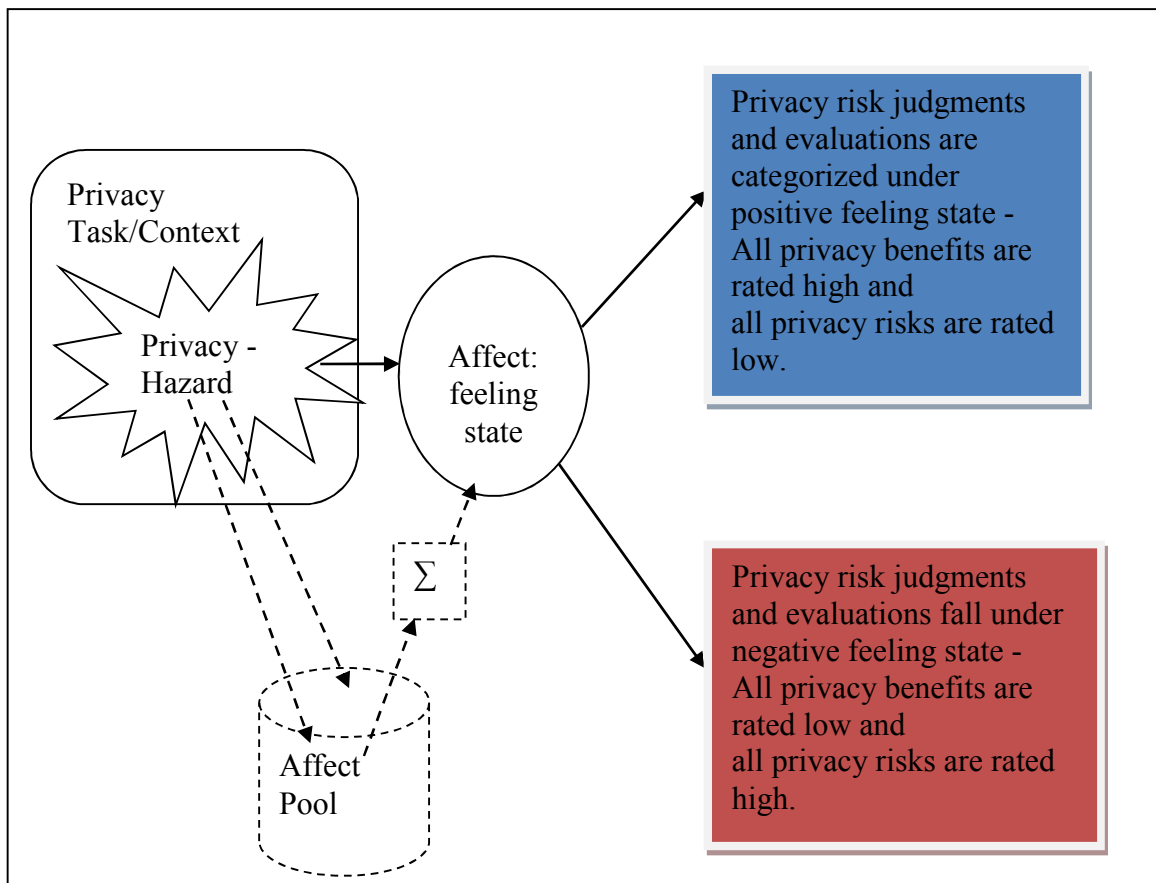


Figure 4. Illustration of Affective Processing

The majority of the privacy concern scales account for cognitive measures of anxiety and worry due to risk perceptions, lack of control and lack of information. People utilize a privacy calculus to weigh the risk and benefits of their decision but in some cases behaviors do not match stated intentions (e.g., privacy paradox). The research into the psychometric paradigm stresses that affect plays a clear role in judgment, decision-making and risk perception (Slovic, 2000). Based on the influence of affect on decision-making with the context of the experiential system and addressing privacy risk as risk hazards, there is evidence that would suggest affect would influence privacy concerns.

The evaluation of a stimulus can result in a positive, negative or neutral affect (Nyshadham & Castano, 2012). This research discussed that if affect results in a "negative feeling" then privacy concerns will be higher. If affect results in a "positive feeling", then privacy concerns will be lower. If there is no affect, there is no change in privacy concerns. Based on these concepts on negative and positive affect, the following hypotheses were presented (see Figure 5):

H3a: Negative affect causes higher privacy concerns.

H3b: Positive affect causes lower privacy concerns.

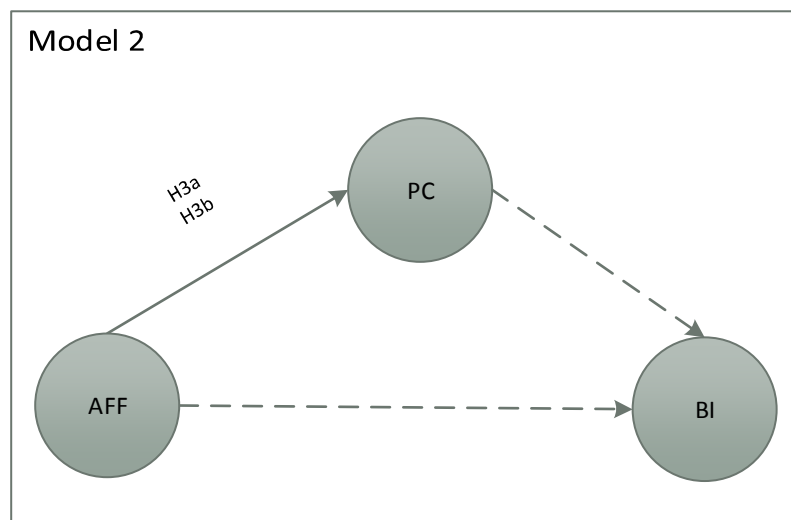


Figure 5. Conceptual Model 2 - The Influence of Affect on Privacy Concerns

Conceptual Model 1 suggests that privacy concerns influence behavioral intentions and Slovic's affect heuristic influences behavioral intentions (see Figure 3). Conceptual Model 2 suggests that affect influences privacy concerns (see Figure 5). Due to several factors that influence behavioral outcomes, the following research questions (RQs) were suggested:

RQ1. Do privacy concerns mediate privacy behavioral intentions?

RQ2. How does affect, "a faint whisper of emotion," affect privacy concerns?

RQ3. Does affect have an independent effect on privacy behavioral intentions?

For example, some people absolutely refuse to join a social networking website such as Facebook for fear of privacy exposure. Those who hold so strongly to their privacy concerns usually will not waver regardless of any affect. This example suggests that regardless of the type and valence of the affect, privacy concerns will determine the privacy behavioral action. However, the "affect" of an immediate payoff such as an exciting one-time subscription offer (stimulus) to receive free storage on Mozy, can cause the most cautious people to dismiss their privacy concerns. The example of free storage on Mozy suggests that "affect" is the main driver (antecedent) for a privacy behavioral action.

"The Facebook News Feed" outcry in 2006, demonstrates the behavioral outcomes of a perceived privacy violation (Hoadley et al., 2009). Even though Facebook's privacy settings were not changed, Facebook's introduction of a news feed influenced privacy behaviors. People perceived Facebook modified privacy settings but this was not the case. Only the informational format presented was modified. People assumed their

privacy was violated but it was not. This incident suggests that a stimulus created an “affect” which influenced privacy behaviors. Hoadley et al. did not specify the extent privacy concerns had in the final outcome. Further study of this phenomenon suggested the following hypothesis (see Figure 6):

H4: The relationship between affect and behavioral intentions (privacy behavior) is mediated by privacy concerns.

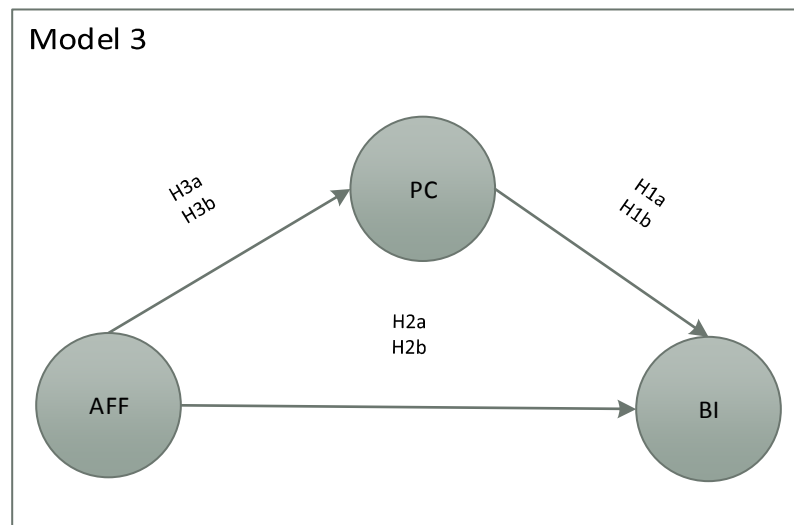


Figure 6. Conceptual Model 3 - Privacy Concerns Mediating the Influence of Affect on Behavioral Intentions

Relevance and Significance

The research in the privacy concern domain has focused on the outcomes and consequences of research with limited empirical research in the antecedents of privacy concerns. This research adds to the body of knowledge about the privacy concern domain by providing additional empirical information for antecedents of privacy concerns (Smith et al., 2011). Furthermore, the affect domain has thus far been limited to fields such as sociology, psychology, healthcare and financial investing. This research extends the affect domain into the information systems field and helps contribute to the understanding of why people indicate they will not perform a given behavior but, when

given the chance, act in a manner that is contrary to their stated intentions (Belanger & Crossler, 2011). Using a set of existing affect measurements (e.g., Single Category Implicit Attitude Test (SC-IAT)) and applying the measurements to existing privacy concern scales in the area of IT might provide a new measurement for privacy.

In addition, Belanger and Crossler (2011) suggest more studies should investigate the “why” related to privacy as opposed to the “how” (p. 1035).

Barriers and Issues

Some barriers and issues to fully understanding the influence of affect in the IS domain have made this problem difficult to solve. One such barrier is a lack of any implicit and explicit measurement in the IS field. Although, instruments such as SCI-AT and Word Association Test might have been utilized in other streams of non-IS research, the challenge was validating the current instrument against the current privacy constructs. To overcome this obstacle, these instruments were modified to closely match the existing research conducted by Dohle et al. (2010), Rubaltelli et al. (2010) and Slovic (2010) and were executed using the same online interface.

Another barrier that was encountered was conducting the SC-IAT and Word Association Test over the Internet. Previous research in affect had been conducted in classroom laboratory settings but this study was novel in its approach as it only used the Internet.

Assumption, Limitations and Delimitations

Assumptions

The main assumption in this study was that participants had a basic understanding of online transaction (i.e., e-commerce transaction such as online banking, online purchasing, social network usage, etc.).

Limitations

Limitations refer to the limiting conditions or weaknesses that cannot be controlled by the researcher that may influence the results of a study (Locke, Spirduso & Silverman, 2000). The limitations are as follows:

1. The lack of prior research where affect as an antecedent has never been considered.
2. Causal modeling using PLS-SEM does not require large samples but there is potential for error for not having a large sample.
3. The scenario used in this research may have not be salient enough to incite a privacy concern or privacy worry.

Delimitations

Delimitations are those characteristics that limit the scope of the study (Leedy & Ormrod, 2005; Locke et al., 2000). In order to conduct the study and avoid any external influences, the following were established:

- a. The study was delimited to participants who are over 18 years of age and located in the United States.
- b. The study was delimited to Internet users with online experience who have conducted online transaction such as online banking and retail purchasing

within the last six (6) months using IE 6.0 + and other browsers including Firefox and Chrome on computer systems which have Windows XP, Windows 7 and Windows 8 operating systems or MacOS.

- c. The study was delimited to Mturk Master workers.

Definition of Terms

Affect – the specific quality of “goodness” or “badness” (i) experienced as a feeling state (with or without consciousness) and (ii) demarcating a positive or negative quality of a stimulus (Slovic, 2004; Slovic et al., 2005, Slovic et al., 2007)

Affect pool – contains all the positive and negative tags associated with the representations consciously or unconsciously that are accessed in the process of making decisions (Slovic et al., 2005)

Attitude – An association between a concept and an evaluation – an assessment of whether something is good or bad, positive or negative, pleasant or unpleasant (Nosek & Banaji, 2009)

Blindfolding – A sample reuse technique that omits part of the data matrix and uses the model estimates to predict the omitted part (Hair et al., 2014)

Emotion – “refer to complex states of the organism characterized by changes in autonomic nervous system arousal accompanied by distinct physiological expressions, specific action tendencies and subjective feeling experiences of a certain valence” (Pham, 2007)

Endogenous latent variable – “serve only as dependent variables or as both independent and dependent variables in structural model” (Hair et al., 2014, p.29)

Exogenous latent variables – “latent variables that serve only as independent variables in a structural model” (Hair et al., 2014, p.29)

Hazards – “threats to humans and what they value” (Slovic, 2000, p.169).

Implicit attitude – “attitudes which are manifest as actions or judgments that are under the control of automatically activated evaluation, without the performer’s awareness of the causation” (Greenwald et al., 1998, p.1464)

Information privacy – “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent about them is communicated to other” (Westin, 1967, p. 9)

Intention – motivational factors that influence behavior and the amount of effort an individual will exert to perform the behavior (Ajzen, 1991)

Privacy benefit – an individual’s belief based on privacy decision that the most favorable net level outcome such as a financial reward (Smith et al., 2011)

Privacy calculus – a decision process of determining the consequentialist tradeoff of costs and benefits (Smith et al., 2011)

Privacy concern – a basic worry of the consequence of a loss of personal information (Rifon et al., 2007)

Privacy paradox – a state in which individuals state privacy concerns but behave in ways that seem to contradict their statements (Belanger & Crossler, 2011; Rifon et al., 2007; Smith et al., 2011)

Privacy risk – degree to which an individual might experience a potential loss after releasing personal information (Malhotra et al., 2004; Smith et al., 2011)

Psychometric paradigm – “psychophysical scaling methods and multivariate analysis to produce meaningful representations of risk attitudes and perceptions” (Slovic, 2000, p.189)

Risks – “quantitative measures of hazard consequence that can be expressed as conditional probabilities of experience harm” (Slovic, 2000, p. 169)

Somatic markers – thoughts made of images including sound, ideas and words that are states (Damasio, 1994)

Summary

Current measure of privacy concerns have only addressed measurements from a cognitive consequentialist approach. Most of the research has not addressed nor considered the influence of emotion on the privacy behavioral intentions. Recent research has suggested that human decision-making relies on interaction between emotion and reason more specifically the influence of “affect.” This research suggest that affect influences privacy behavioral intentions with privacy concerns acting as the mediator.

The primary goal of the research was to provide a better understanding of affect on privacy behavioral intentions. Secondary goal is to determine to what extent that privacy concerns influence the relationship between affect and privacy behavioral intentions.

Chapter 2

Review of Literature

Overview

This chapter first consists of the relevant literature involving affect on decision-making and how implicit attitudes can be used as proxy for measuring affect. Subsequent topics include the exhaustive review of privacy concerns including the cognitive consequentialist measurement approach, the privacy paradox and privacy calculus.

Affect

Early work on people's judgments and decision-making did not consider that feelings played any role in that process until 1970 when strategies around heuristics started to emerge especially around the ease of recalling previous events and occurrences (Slovic, 2010). Slovic's research begins to address the relationship of the collection of heuristic strategies and was used to question the addressing of positive and negative feelings. Although cognitive deliberations and decision processes were the focus of the research at the time, it was not until a perception study revealed that perceived risk and acceptable risk were closely associated with the feelings of dread risk evoked by a hazard (Fischhoff, Slovic, Read & Lichtenstein, 1978).

Zajonc (1980) claimed that all perceptions contain some "affect." Zajonc states that affect responses are universal among animal species. For example, a rabbit reacting to an approaching snake does not have a lot of time to process the situation and has to make a quick reaction to escape. Unlike judgments of objective stimulus properties, affective reactions that accompany these judgments cannot always be voluntarily controlled.

Affect often persist after a complete invalidation of its original cognitive basis, for example, judgments “feel” valid, which is why it is so hard to dismiss. Affective reactions are the first response to a stimuli, occurring automatically and thus driving information processing and judgments (Finucane et al., 2000; Zajonc, 1980).

Several streams of research refer to affect as an attitude (e.g. an evaluation with a positive or negative valance), a strong emotion (e.g., fear, dread), a mild emotion (e.g., anxiety), or a mood state (e.g. bored) (Nyshadham & Minton, 2013). Affect is different from emotion and is called a “faint whisper of emotion” and is distinct from primary emotions (e.g. fear, anger) or secondary emotions (e.g. anxiety) (Nyshadham & Minton, 2013; Slovic, 2004; Slovic et al., 2005).

Because affect is usually the first evaluation that occurs in response to risk and guides further decision processes, it is an important factor in studies of risk. First, affective reactions tend to be fast and efficient (Zajonc, 1980, Slovic et. al, 2007). Second, behaviors based on affective reactions tend to be extreme and polarized. This could be due to: a) affect being more extreme to begin with, b) affect leading to search for confirmatory evidence which in turn increases coherence of decisions, c) relative insensitive to probability and value and d) possessing strong drive properties, unlike reason (Nyshadham & Castano, 2012). Affect provides several interesting ways to rephrase the questions used in privacy risk research.

Several distinguishing characteristics of affect can have considerable application in understanding judgments and behaviors regarding online risks (Pham, 2007). Affect is a proxy for value if a risk is hard to evaluate (e.g., likelihood or consequence are unavailable, attributes of risk are novel), affective rating substitutes for constructs such as

the decision weight (subjective probability), magnitude of consequence and expected value/utility. Affect can serve as a common currency, thus enabling people to compare side-by-side widely different risks or attributes of risk so as to arrive at a global measure of risk on an affective scale. As a corollary, a signal from a stimulus (e.g., an attribute of privacy risk such as access) might have no effect on privacy concern, if it is not evaluable and thus has no affective valence.

Recent research by Nyshadham and Minton (2013) suggest models that help illustrate the difference between the cognitive-consequentialist and feeling-based notions of risk. They present four models of IS Risk as shown in Figure 7. The first model is based on well-understood cognitive-consequentialist model that assumes a person judges a hazard in context of terms of a subjective probability of an unfavorable event and potential loss if it were to happen. The person computes the net benefits using a privacy calculus. The second model is called the IS-Emotion model, which assumes that emotion may influence the antecedents or outcomes of the model and act as a moderator to benefit/costs or impact the behavior directly. The third model, Lowenstein-RAF model, based on Lowenstein et al.'s (2001) risk-as-feelings hypothesis, suggests: a) anticipated outcomes and subjective probabilities determine cognitive evaluations as well as feelings, b) other factors such as vividness, immediacy and background mood impact and, c) cognition and feelings interact to product judgment/decision. The Slovic-affect model introduces an automatic affect, the ability of properties/attributes of stimulus/context to create a “feeling state” (affective evaluability) and congruence between costs and benefits of decision and affect as novel concepts (Nyshadham & Minton, 2013).

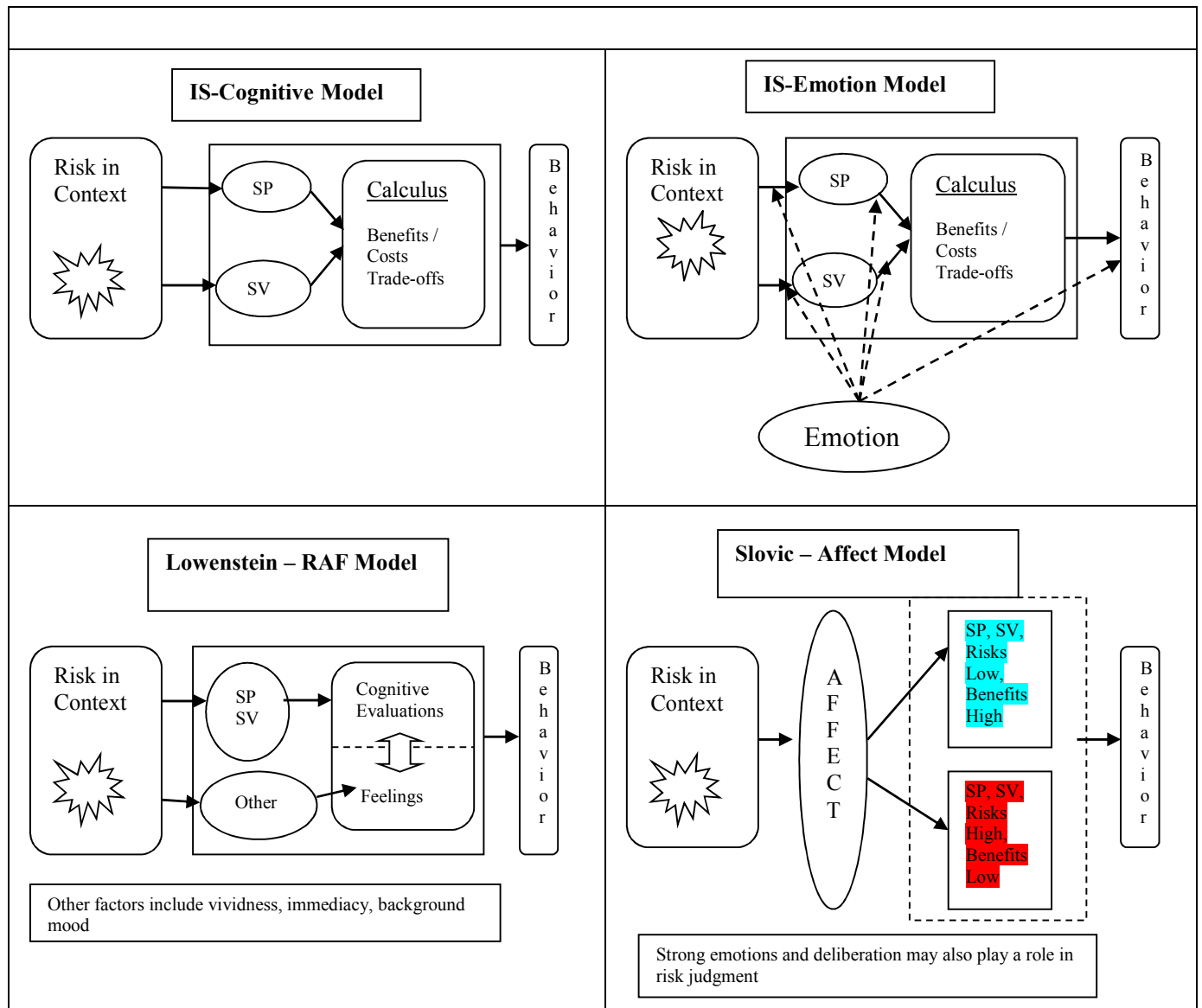


Figure 7. Four Models of IS Risk (SP= subjective probability, SV= subjective value)

Implicit Attitudes

An attitude is an association between a concept and the assessment of whether that concept is good or bad, pleasant or unpleasant, positive or negative (Nosek & Banaji, 2009). Positive or negative evaluations require introspection about one's feeling about a

concept. Nosek and Banaji (p. 2) cite that a familiar way to assess an attitude is to ask – “do I like this?”

In IS research, explicit attitudes serve as the basis for most risk measurement models in IS (e.g. privacy scales, perceived risk scale by Glover and Benbasat (2011)) and can be best thought of as evaluations (Nyshadham & Castano, 2012). Explicit attitudes are deliberate, intentional and readily available to the conscious awareness (Dohle et al., 2010; Karpinski & Hilton, 2001; Nosek & Banaji, 2009). When people have the opportunity and motivation to recollect their explicit attitude, then these consciously held attitudes will guide behaviors. The ability to automatically comprehend and evaluate a situation and take action without much thought is a natural process referred to as an implicit attitude (Nosek, Greenwald & Banaji, 2007; Karpinski & Hilton, 2001). It is easier to measure an explicit attitude by asking respondents how they feel about a situation than implicit attitude.

Implicit attitudes exist outside of conscious awareness and are not accessed introspectively and therefore more difficult to evaluate. They reflect positive and negative associations through experience and are not measured by self-reports. For example, a person might have an explicit attitude (e.g. pleasant) about Google’s cloud computing services, but possess a negative implicit attitude (e.g. bad) about the Google organization. A person can hold both types of attitudes but depending on the context and circumstance of the situation can result in different approaches. Holding positive and negative associations can result in multiple ways of how people express their likes or dislikes.

Implicit Association Test (IAT) measures how closely associated any given attitude object (e.g. flower or snake) is with an evaluative attribute (e.g. pleasant or

unpleasant) and assumes that the more closely related the objects and attributes are, the stronger the implicit attitude is (Karpinski & Hilton, 2001; Greenwald et al., 1998). Dohle et al. (2010) determined that the IAT correlates even further with explicit measures when affect has been an influencer. Karpinski, Steinman and Hilton (2005) developed the Single Category-Implicit Association Test (SC-IAT) as a single category measure to compliment the IAT. Measuring implicit attitudes using SC-IAT might be considered a proxy for affect. Because some instances (e.g. words regarding race or sexuality) can be socially embarrassing, when people are explicitly asked, the IAT overcomes these shortcomings by assessing associations indirectly (Dohle et al., 2010). The idea behind implicit measures is that they capture associations that are stored in memory and can be retrieved without requiring introspection (e.g. privacy policy+good).

Slovic et al. (2004) and Slovic et al. (2005) emphasize a person's ability to evaluate risk based on an intuitive and affective mode. In that mode, a person would associate a feeling with a specific word, which a person would think of immediately and without giving much thought to the feeling and the word. Slovic et al.'s (2004, 2005) approach provides insights into an instantaneous reaction.

Implicit social cognition may be inaccessible to conscious introspection, and thus it is necessary to develop measures that do not rely on introspection or self-report in order to understand and measure processes (Karpinski & Steinman, 2006). The Implicit Association Test has become the most commonly used among the implicit measurement techniques because it is reliable, easy to administer, robust and produces large effect sizes (Karpinski & Steinman, 2006). An example of an IAT (see Table 1) would be used to determine how wine drinkers compare to beer drinkers in their preferences. Imagine

sorting a deck of cards with four categories: Items with pleasant meaning (e.g. joyful), items with unpleasant meaning (e.g. terrible), items representing wine (e.g. wine glass) and items representing beer (e.g. beer mug). Test subjects sort the cards, each time with different sorting rules. For the first sorting, all the pleasant words with wine images go into one pile, and unpleasant words and beer images go into another. For the second sorting, all of the pleasant words and beer images go into one pile, and unpleasant words and wine images go into another. The speed of sorting is an indication of the association strengths between concepts and evaluation. In this example, it is likely that a wine connoisseur would sort the cards faster in the first sorting and the beer connoisseur would sort faster in the second sorting because each would have a positive association with their area of expertise. Because IAT uses complementary pairs of concepts and attributes, the IAT is limited to measuring relative strengths of pairs of associations (e.g. Coke/Pepsi, Flower/Insect, male/female) rather than absolute strengths of single associations (Karpinski & Steinman, 2006). In this research, a privacy hazard is a single category or attitude object which can be measured using the Single Category IAT.

The SC-IAT was designed as a two-stage modification of IAT procedure with a single category object that is simple to use and evaluate. Similar to IAT, in each state, target words are associated with attitude object and an evaluative dimension is presented in random order. In the first stage, good words and attitude object are categorized by respondents who click one response key, and bad words are categorized on a different key. In the second stage, bad words and attitude objects are categorized on one response key, and good words are categorized by pressing on a different key. The following table is an example of applying the IAT-Wine & Beer vs. SC-IAT Wine.

Table 1. Comparison of the Implicit Association Test (IAT) and Single Category IAT (SC-IAT)

IAT					SC-IAT				
Block	Trials	Function	Left-key response	Right-key response	Block	Trials	Function	Left-key response	Right-Key response
1	30	Practice	Pleasant Words	Unpleasant Words					
2	30	Practice	Wine words	Beer words					
3	30	Practice	Pleasant words + wine words	Unpleasant words + beer words	1	24	Practice	Good words + Wine words	Bad Words
4	30	Test	Pleasant words + wine words	Unpleasant words + beer words	2	72	Test	Good words + Wine words	Bad Words
5	30	Practices	Beer words	Wine words					
6	30	Practice	Pleasant words + beer words	Unpleasant words + wine words	3	24	Practice	Good Words	Bad words + Wine words
7	30	Test	Pleasant words + beer words	Unpleasant words + wine words	4	72	Test	Good words	Bad words + wine words

Privacy Concerns

Research in privacy concerns is important to IS researchers in order to understand privacy outcomes and behaviors such as willingness to transact online (Belanger & Crossler, 2011; Dinev & Hart, 2004). Numerous definitions conceptualize and explain privacy concerns on intention and behaviors to protect privacy (Culnan & Armstrong, 1999; Hong & Thong, 2012). Privacy concerns are associated with perceptions of risk, lack of control, information misuse or a feeling of anxiety (Rifon et al., 2007). Subjective fairness, collection, and secondary use have characterized privacy concerns (Belanger & Crossler, 2011; Culnan & Armstrong, 1999; Malhotra et al., 2004). Li (2012) suggests

that privacy concerns originated from social contract theory and agency theory, such that consumers are hesitant to provide information to opportunistic online merchants because of the lack of contractual enforcement. Various privacy definitions have been used in IS research but it is assumed that privacy concerns are associated with a privacy loss that drives decision-making and behaviors.

One of the earliest privacy concern models that conceptualized the relationship between antecedents and outcomes of privacy concerns was the Concerns for Information Privacy (CFIP) model developed by Smith et al. (1996). The CFIP model has four dimensions:

1. Collection - the concern about the amount of personal data collected and stored
2. Secondary use - the use of information by another party without the owner's authorization
3. Errors - the concern that protection against deliberate and accidental errors collected are inadequate
4. Improper access - the concern that data about individuals are available to people not properly authorized to view or work with the data

These dimensions defined the core constructs leading to the following subsequent research.

The IUIPC model defined three dimensions: collection, control, and awareness (Malhotra et al., 2004) and Dinev and Hart (2004) theorized two antecedents: perceived vulnerability and perceived ability to control and four dimensions: abuse, findings, control, and vulnerability. Another study by Dinev and Hart (2006b) identified two dimensions in the context of an online service: concerns related to finding personal

information on the Internet and concerns related to the possible abuse of personal information submitted online (Dinev & Hart, 2006b). The Internet Privacy Concern (IPC) model uses six dimensions: collection, secondary usage, errors, improper access, control and awareness (Hong & Thong, 2012). These models do not incorporate notions such as affect, feeling state or even emotions but rely on the cognitive-consequentialist approach (Nyshadham & Minton, 2013).

The APCO model provides a framework for conceptualizing the relationship between antecedents and outcomes of privacy concerns. Smith et al. (2011) developed the macro model that refers to the “antecedents -> privacy concerns -> outcomes. The model treats privacy concern as either a dependent variable or independent variable. As seen in Figure 3 of Smith et al. (2011, p. 998), the left portion of the diagram depicts the privacy concern as the “dependent variable” with the antecedents as the independent variables categorized as privacy awareness, personality differences, demographic difference, privacy experiences and culture/climate. Researchers focused a majority of the research on antecedents at the individual level of analysis with a few studies at the organizational level (Smith et al.). Also seen in Figure 3, the right side of the macro model considers privacy concerns as the “independent variable” with the outcomes such as behavioral reactions, trust, regulations, privacy calculus and risks/benefits (Smith et al.). The APCO captures an extensive number of antecedents and outcomes based models to help with understanding the relationship between the various models, Figure 8 provides a brief list.

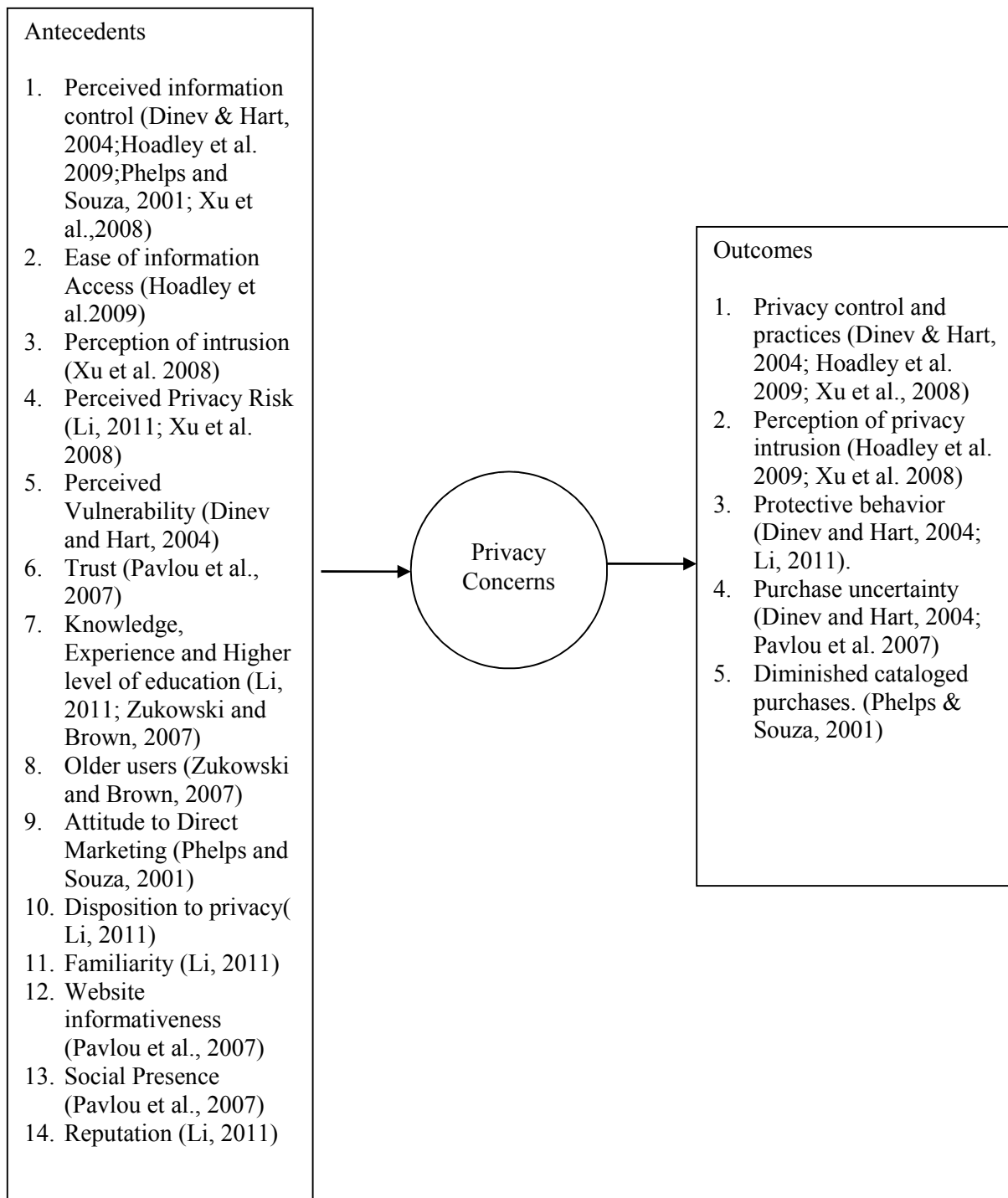


Figure 8. Conceptual Model of the Antecedents and Outcomes of Privacy Concerns

Privacy Calculus

Many studies address privacy calculus as assessments of privacy risk and privacy benefits (Xu et al., 2009; Smith et al., 2011; Dinev & Hart, 2004). The privacy calculus is a cognitive-consequentialist risk-benefit analysis used to determine privacy benefits (Xu et al., 2009; Smith et al., 2011). Privacy benefits are an individual's belief that the most favorable net outcome relies on the factors such as financial reward, personalization and social adjustment benefit (Smith et al., 2011). This opportunistic approach is not without engaging in some mitigation of risk (Dinev & Hart, 2006b). Privacy risks/costs is the probable experience of potential loss after releasing personal information (Malhotra et al., 2004; Smith et al., 2011). These losses can result from misuse of personal information, such as insider disclosure or theft (Dinev & Hart, 2004; Smith et al., 2011). Divulging more information or considering new technologies increases the complexity of conducting a privacy calculus.

Scholars, in recent research, have incorporated other theories (e.g. utility maximization, expectancy theory of motivation and expectancy-value theory) to develop tradeoff functions, as a different way to interpret how privacy calculus operates (Li, 2012).

Privacy Paradox

Being fully aware of the privacy threats, people express their privacy concerns but their actions do not seem to align with their desired intent (Smith et al., 2011; Rifon et al., 2007). Refraining from risky online behaviors would be beneficial at preventing loss but user's behavior is often contrary to user's stated intentions and concerns (Belanger & Crossler, 2011; Rifon et al., 2007; Smith et al. 2011). People divulge personal

information for a small benefit, even though people expressed the desire to keep their information private. The privacy paradox questions the validity of current privacy concerns since the research measures intentions and not behaviors (Smith et al., 2011).

Chapter 3

Methodology

Overview

This chapter presents the research methodology to understand the relationship between affect, privacy concerns and behavioral intentions. The first section presents a broad overview of the general research method employed. The next section describes the data collection procedures and respective measurements in more detail. The final section addresses the validity and reliability of the instrument along with data analysis.

Research Method

This study used a quantitative survey research method. This method was adequate because there was no variable that was systematically manipulated. It is difficult to observe physically the relationship between affect and behavioral intentions. It is only through a survey that such an internal relationship can be assessed. Because affect is an instantaneous response, using the survey research method will immediately ascertain attitudes and thoughts (Leedy & Ormrod, 2005).

The study was designed to assess the relationships between the constructs shown in the structural and measurement model (see Figure 9). As shown in Figure 9, the key constructs in the model are: affect, privacy concerns, and behavioral intentions. The key hypothesis of this research was that privacy concerns result from affect; thus, privacy concerns mediated the relationship between affect and behavioral intentions.

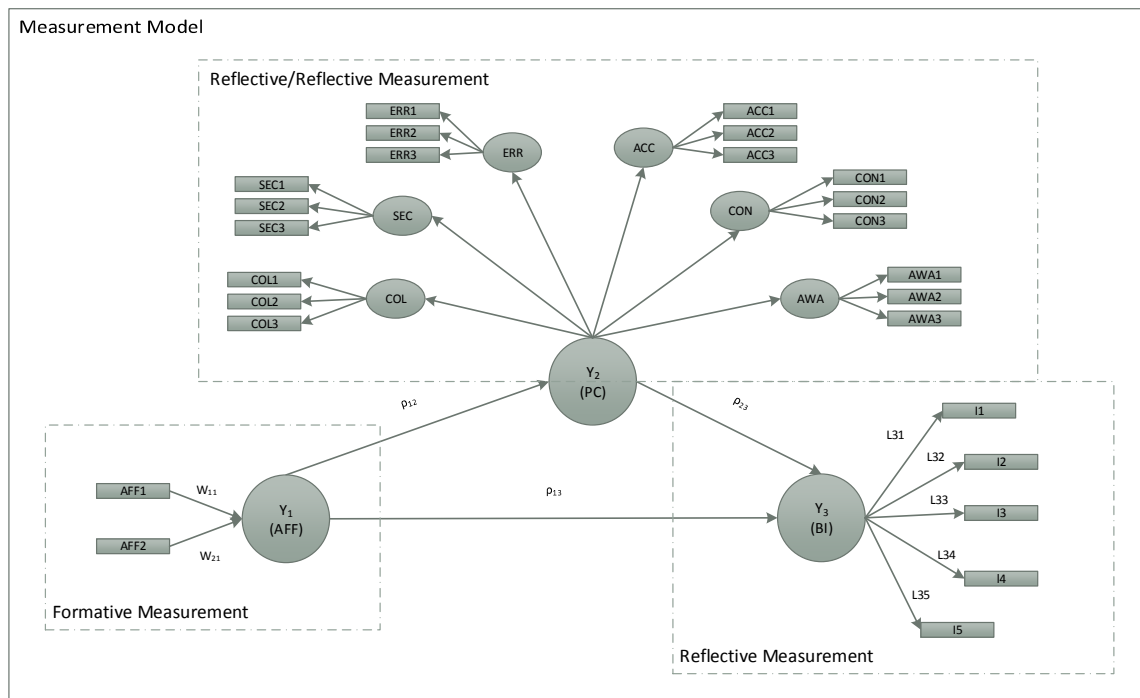


Figure 9. Structural and Measurement Model of the Influence of Affect on Privacy Concerns and Behavioral Intentions

Participants were first presented with a privacy hazard scenario based on typical privacy tasks in IS research. After reading the privacy scenario, participants were asked to express their feelings about the scenario. Their feelings (i.e., affect) were captured using two measurements. In the first measurement (Aff1), the Word Association Test, participants were asked to write the first the first thought that came to mind and then rated that thought on a like/dislike scale. The total score across all the words and concepts was used as an explicit measure. In the second measure of affect (Aff2), the Single Category Implicit Attitude Test, participants were asked to associate a stimulus with a set of specified words (i.e., words indicating positive or negative feelings). The experienced affect measure was the mean reaction time of the assignment of the target word to like/dislike words.

Once affect was measured, privacy concerns, behavioral intentions and demographics were captured by traditional well-established surveys. Both measurements are discussed in further detail later in this chapter.

Data Collection Procedures

First, participants accessed a website containing the tests and surveys that introduced the study, including the required disclaimers, and the IRB notice. The data collection was administered to the participants in three phases (see Figure 10).

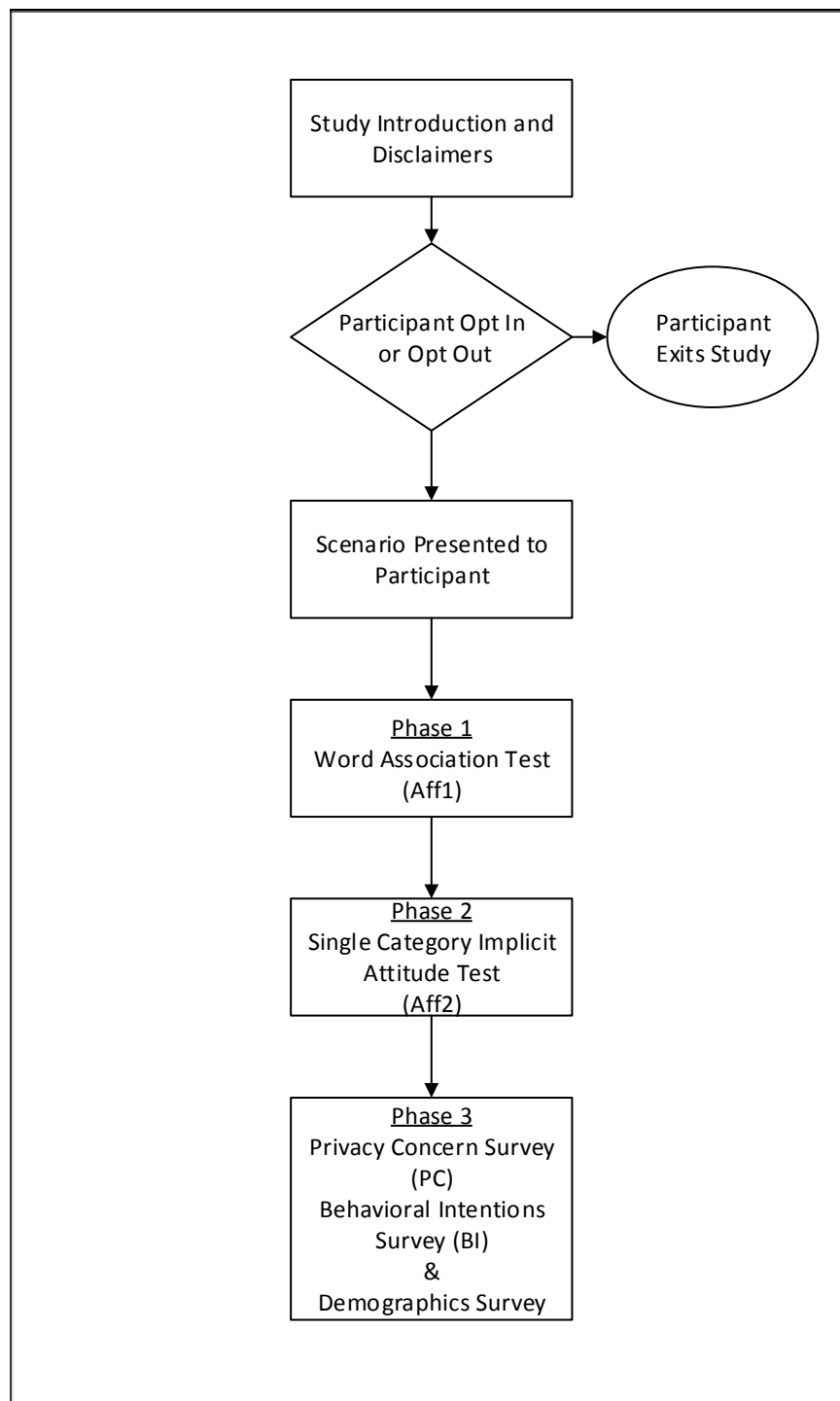


Figure 10. Data Collection Procedure Website Flow Chart

Before starting Phase 1, the participants were presented with an introduction to the study as shown in Figure 10. (see Appendix A containing the text for study introduction)

Next, the participants were given the option to participate or decline. Then, the scenario was presented to the participant as shown in Figure 10 for approximately three minutes. Test participants were not required to memorize the scenario. See Figure 11 for the full scenario text.

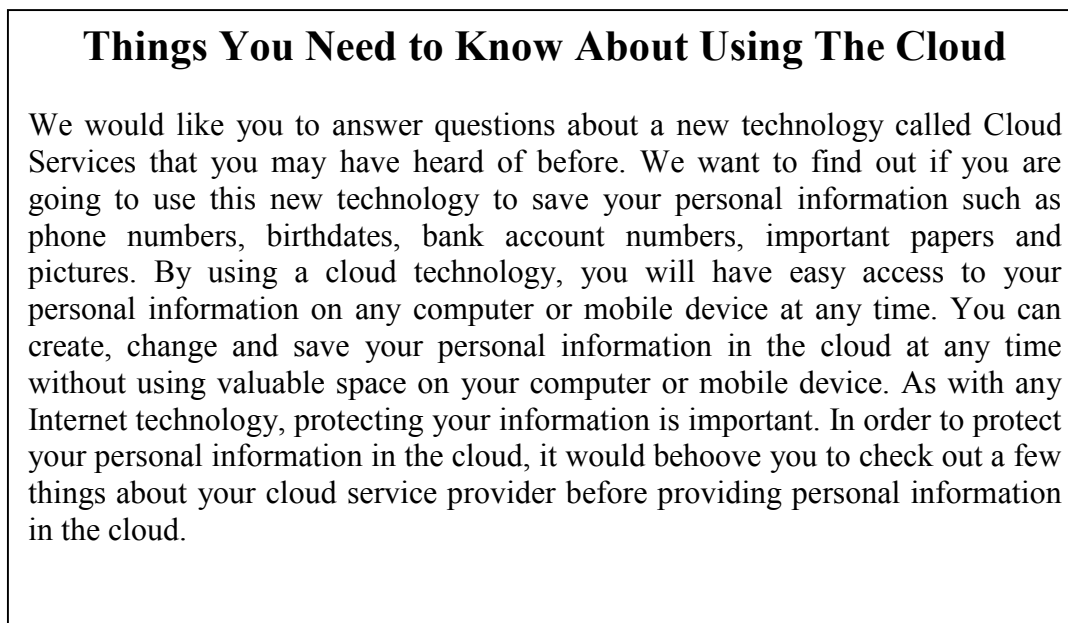


Figure 11. Scenario

This scenario was based on an article published on April 16, 2014 in CIO.com, “9 Things You Need to Know Before You Store Data in the Cloud” (Schiff, 2014). This article prompts readers to review the risks associated with managing and storing data in the cloud. The proposed scenario suggested a risk of unauthorized use or loss of personal information such as birthdates, bank account numbers, social security numbers (Phelps, Nowak & Ferrell, 2000; Office of Management & Budget, 2007) while using cloud technology. An important element in this scenario was creating affect-ladenness by the use of words or concepts (see the title as shown in Figure 11). Slovic (2010) states that

warnings are more effective when presented in the form of a vivid, affect-laden scenario or anecdotes. The scenario suggested the idea of storing personal information in a cloud environment can be beneficial. In addition, the scenario raised the possibility of risks that can generate negative feelings.

Phase 1: Word Association Test

After the participant read the scenario, the participant was directed to begin Phase 1. The purpose of using the Word Association Test (WAT) was to provide a direct measurement of Aff1. The WAT relies on the method of concept or word association to a corresponding privacy task hazard (Rubaltelli et al., 2010; Slovic et al., 2004; Slovic, 2010). Word association techniques are strongly rooted in the history of psychology and are capable of revealing the cognitive and affective elements of concepts people hold about complex stimuli (MacGregor, Slovic, Dreman & Berry, 2000). The WAT method involved presenting participants with a target stimulus (the scenario) and asking them to provide the first thought or concept that comes to mind. The participant submitted five associations. Subjects were then asked to rate each concept or word on a scale from positive (e.g., +2) to a negative (e.g., -2). Scoring was calculated by summing the rating to obtain the overall word index (MacGregor et al., 20002; Slovic et al., 1991).

The participant was presented with a web page consisting of five blank entries. The participant wrote the “first” thought that came to mind, and then, the process was repeated four more times (see Appendix B). After the person completed the entries, the participant clicked “next” to launch the web page where they rated their words. The participant rated each of their words using a five-point scale, where -2 is considered very bad, -1 is bad, 0 is neutral, +1 is good and +2 very good.

After the participant completed Phase 1, the participant clicked “next” to launch Phase 2, the SC-IAT.

Phase 2: Single Category – Implicit Association Test (SC-IAT)

The purpose of using SC-IAT was to measure affect through an indirect method (Dohle et al., 2010; Karpinski & Steinman, 2006). The SC-IAT measured how closely a person associated a specific word or image (action word) with an evaluative object (i.e. pleasant/unpleasant). The response time of the assignment of the evaluative object to the specific word or image provided the affect measure (Aff2). In Phase 2, the action words were based on the scenario and how people implicitly feel using a *cloud technology*: safe or unsafe when disclosing personal information.

The participant was presented with a set of action words including “disclose, divulge, reveal and upload.” The amount of time it took a subject to relate an action word with a good versus a bad word was a measure of automatic association. The bad words used were “unsafe, dangerous, terrible, shaky and vulnerable.” The good words were “safe, wonderful, stable, secure and protected” (see Appendices D and E).

The SC-IAT consisted of two stages that all participants completed in the same order. Each stage consisted of 24 practice trials immediately followed by 72 test trials (three blocks of 24 trials each). In the first stage (disclose + bad), “disclose” words and “bad” words were categorized on the “I” key of the keyboard and good words were categorized on the “E” key of the keyboard. In the second stage, (disclose + good), “disclose” attitude words and “good” words were categorized on the “E” key of the keyboard and “bad” words categorized on the “I” key of the keyboard. In order to prevent a response bias from developing, “disclose” words, “good” words and “bad words” were

not presented at an equal frequency (Karpinski et al. 2006). The data collected was a summary of the response times with the assumption that people generally responded quickly when positive words were associated with liked concepts, and respond more slowly when negative words were associated with the disliked concepts (Karpinski, 2006).

Formative measurements in this study were based on the assumption that indicators caused the construct (Rossiter, 2002) as each formative indicator captured a specific aspect of the construct's domain (Hair et al., 2014). The indicators Aff1 and Aff2 both captured affect from two different methods (i.e., explicit and implicit) and were not interchangeable and caused the construct. The construct and measures are shown in Table 2.

Table 2. Construct, Indicators and Measures of Affect

1st Order Construct	Indicators	Measures	Source
Affect	Aff1	Word Association Test	Slovic, 2004; Rubatelli et al., 2010
	Aff2	Single Category Implicit Attitude Test	Dohle et al., 2010; Karpinski & Steinman, 2006.

Upon completion of Phase 2, the participants clicked “next” to complete three surveys that measured privacy concerns, behavioral intentions and demographics. See Appendices F, G, and H for the web page format presented to the participant.

Phase 3: Surveys

Privacy Concern Survey: The most recent instrument developed by Hong and Thong (2011) was the basis for measuring this study's privacy concerns. Their

measurements stem from an extensive review of the conceptualization and operationalization of previous work in IS on privacy concerns. Using a sequence of surveys, Hong and Thong (2011) tested for the factorial structure of the measurement items and proposed a second-order privacy concerns construct composed of six distinct first-order constructs. The reflective measure is the standard confirmed by Hong and Thong's Model 3. Hong and Thong's (2012) privacy concern instrument was adapted for this study and used a seven point Likert scale containing valid and reliable (Hong and Thong, 2012, p. 15) items adapted for this research. A summary of the measures is shown in Table 3.

Table 3. Survey Items for Privacy Concerns

2nd Order Construct	1st Order Construct	Indicators	Measures	Source
Privacy Concerns (PC)	Collection	COL 1	It usually bothers me when cloud websites ask me for personal information.	Hong & Thong, 2012; Smith et al., 1996
		COL 2	When cloud websites ask me for personal information, I sometimes think twice before providing it.	Hong & Thong, 2012; Smith et al., 1996
		COL 3	I am concerned that cloud websites are collecting too much personal information about me.	Hong & Thong, 2012; Smith et al., 1996
	Secondary Usage	SEC 1	I am concerned that when I give personal information to a cloud website for some reason, the website would use the information for other reasons.	Hong & Thong, 2012; Smith et al., 1996
		SEC 2	I am concerned that cloud websites would	Hong & Thong, 2012; Smith et

			sell my personal information in their computer databases to other companies.	al., 1996
		SEC 3	I am concerned that cloud websites would share my personal information with other companies without my authorization	Hong & Thong, 2012; Smith et al., 1996
Errors		ERR 1	I am concerned that cloud websites do not take enough steps to make sure that my personal information in their files is accurate.	Hong & Thong, 2012; Smith et al., 1996
		ERR 2	I am concerned that cloud websites do not have adequate procedures to correct errors in my personal information.	Hong & Thong, 2012; Smith et al., 1996
		ERR 3	I am concerned that cloud websites do not devote enough time and effort to verifying the accuracy of my personal information in their databases.	Hong & Thong, 2012; Smith et al., 1996
Improper Access		ACC 1	I am concerned that cloud website databases that contain my personal information are not protected from unauthorized access.	Hong & Thong, 2012; Smith et al., 1996
		ACC 2	I am concerned that cloud websites do not devote enough time and effort to preventing unauthorized access to my personal information.	Hong & Thong, 2012; Smith et al., 1996
		ACC 3	I am concerned that	Hong & Thong,

			cloud websites do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers.	2012; Smith et al., 1996
Control	CON 1		It usually bothers me when I do not have control of personal information that I provide to cloud websites.	Hong & Thong, 2012; Malhotra et al., 2004
	CON 2		It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by cloud websites.	Hong & Thong, 2012; Malhotra et al., 2004
	CON 3		I am concerned when control is lost or unwillingly reduced as a result of marketing transactions with cloud websites.	Hong & Thong, 2012; Malhotra et al., 2004
Awareness	AWA 1		I am concerned when a clear and conspicuous disclosure is not included in online privacy policies of cloud websites.	Hong & Thong, 2012; Malhotra et al., 2004
	AWA 2		It usually bothers me when I am not aware of knowledge about how my personal information will be used by cloud websites.	Hong & Thong, 2012; Malhotra et al., 2004
	AWA 3		Is usually bothers me when cloud websites seeking my information online do not disclose the way	Hong & Thong, 2012; Malhotra et al., 2004

			the data are collected, processed, and used.	
--	--	--	--	--

Behavioral Intentions Survey: Current IS research does not adequately address privacy behavior due to measurement challenges. Therefore, this research employed a behavioral intention instrument used as a reflective measure by Malhotra et al. (2004) adopted from Smith et al.'s, (1996) study on privacy. Using behavioral intention measures, Smith et al. confirmed a high level of inter-item reliability with a Cronbach's alpha of .87. Malhotra et al. used the same measures and found behavioral intentions and UIIPC correlated strongly among three of the five indicators. A summary of the measures adapted for this research is shown in Table 4. The survey instrument used a seven point Likert scale.

Table 4. Survey Items for Behavioral Intentions

1st Order Construct	Indicators	Measures	Source
Behavioral Intention (BI)	I1	How likely are you to refuse to give information to a cloud website company because you think it is too personal?	Smith et al., 1996; Malhotra et al., 2004
	I2	How likely are you to take action to have your name removed from e-mail lists from a cloud website company?	Smith et al., 1996; Malhotra et al., 2004
	I3	How likely are you to write or call a cloud website company to complain about the way it uses personal information?	Smith et al., 1996; Malhotra et al., 2004
	I4	How likely are you to write or call an elected official or consumer organization	Smith et al., 1996; Malhotra et al., 2004

		about the way a cloud website companies use personal information?	
	I5	How likely are you to refuse to purchase a product because you disagree with the way a cloud website company uses personal information?	Smith et al., 1996; Malhotra et al., 2004

Demographics Survey: The survey collected demographic information including gender, age, education level and Internet experience. These demographic factors may have influenced participant's reactions to information privacy threats (Malhotra et al., 2004). The survey measures are indicated in Appendix H.

Participants

The target population for this study was adult (+18 year old) Internet users within the United States. Due to the novelty of this research, a sample size was selected based on a rule of thumb suggested by Hair et al. (2013). Based on Hair's recommendations, this study used an 80% statistical power, 1% probability of error for detecting R^2 (i.e., effect) value of .25 and a maximum of two independent variables in the structural model for a proposed sample size of 75 but 80 subjects were actually used. The participants were recruited from Amazon Mechanical Turk with a monetary incentive of \$5.00 to participate with payment through Amazon Mechanical Turk upon completion of the study. If the participant chose to opt out of the study, the participant was not offered compensation. The participation process was anonymous and any personal identifiable information was not provided to the researcher. All users were assigned an Inquisit unique ID not linked to any personal information thus insuring anonymity.

Results Analysis

A second-generation causal modeling statistical technique, partial least squares structural equation modeling (PLS-SEM), was used for data analysis research. PLS-SEM is widely accepted as a method for testing theory in early stages, while LISREL is usually used for theory confirmation (Fornell & Bookstein, 1982). PLS-SEM, as the statistical technique, was particularly suitable because of the exploratory nature of this study. Additionally, PLS-SEM is well suited for highly complex predictive models. Prior studies that applied PLS-SEM (e.g. Kim & Bebasat, 2006) have found that PLS-SEM is best suited for testing complex relationships by avoiding inadmissible solutions and factor interdeterminacy. This makes PLS-SEM suitable for accommodating the presence of a large number of constructs and relationships in current research. PLS-SEM also has the ability to assess the measurement model within the context of the structural model, which allows for a more complete analysis of inter-relationships in the model (Xu et al. 2011).

Before analyzing the results, data cleaning was conducted. Data cleansing was necessary to evaluate and minimize the effect of missing and/or misleading data that may have the potential of introducing bias into data analysis (Hair et al., 2014). When empirical data are collected using questionnaires, data collection issues such as missing data, suspicious responses, outliers, and data distribution must be addressed (Hair et al., 2014). Missing data occurs when a respondent either purposely or accidentally fails to answer one or more questions. When the amount of missing data exceeds 15%, the observation is usually removed from the data file. Suspicious response patterns such as straight lining, when a respondent marks the same response for a high proportion of the

questions, invalidates the study. Outlier, an extreme response to a particular question or extreme response to all questions, also skews the study. PLS-SEM is a nonparametric statistical method and does not require the data to be normally distributed. It was important to verify that the data is not too far from the norm, as extremely non-normal data prove problematic. Once the data was cleansed of potential issues, the data were ready for analysis.

The analysis consisted of measuring AFF, PC and BI. Two constructs, BI and PC are reflective models and AFF is a formative model. PC is a second order factor that is measured by six reflective first order factors that correspond to the survey item as shown in Table 3. BI is a reflective item measured as a first order factor shown in Table 4. Affect was measured by two formative measures (Aff1 and Aff2) captured from two previously discussed instruments. All of the data was collected in the data matrix used for analysis in the SmartPLS software. When a formative measurement model is assumed for a construct (e.g. latent variables, AFF as shown in Figure 9), the “*w*” coefficients (i.e., outer weights) are estimated by a partial regression where the latent Y construct (e.g., Y1) represents a dependent variable and its associated indicator variables Aff1 and Aff2 were the independent variables. According to Hair et al., “there is a partial regression model for every endogenous latent variable to estimate all the path coefficients in the structural model” (p.77).

In contrast, when a reflective measurement model was assumed for a construct (e.g., latent variable BI as shown on Figure 9), the “*l*” coefficients (i.e., outer loadings) were estimated through single regressions (one for each indicator variable) of each indicator variable on its corresponding construct.

Structural model calculations were as follows:

- a) Partial regressions for the structural model specify a construct as the dependent variable (e.g., BI in Figure 9).
- b) Dependent latent variable's direct predecessor (i.e., latent variables with direct relationship leading to target construct; PC and AFF) were the independent constructs in a regression used to estimate the path coefficients.

PLS-SEM algorithms iterative procedures estimated all partial regressions in two stages. The construct scores were estimated in the first stage. The final estimates of the outer weights and loadings were calculated in the second stage, including the structural models path coefficient and results R^2 values of the endogenous latent variable (Hair et al., 2014).

The evaluation of the measurement models were as follows:

- a) Reflective models were assessed on the indicator reliability, convergent validity and internal consistency.
- b) Formative models were assessed on the convergent reliability and collinearity among indicators and significance and relevance of outer weights.

Once the measures' quality had been established, the primary evaluation criteria should be ascertained for the structural model which were the coefficients of determination (R^2), predictive relevance (Q^2), and effect size and significance of path coefficients.

Anticipated Difficulties

There were two weaknesses to the proposed design. The first was the measure of affect which can be induced by factors aside from the proposed “Scenario” stimulus. Pham (2007) distinguishes between integral affect attributed to a stimulus and incidental affect attributed to context, mood and other conditions apart from a stimulus. Affect is a product of both the stimulus and context. For example, a virus in a medical context may raise a different set of concerns than a virus in a computer context. In this design, data was collected from subjects under identical conditions to insure equal impact of affect across all subjects. Data on control variables such as gender, age, etc. was collected and used in the estimation models to explain their effect.

The second weakness was the novelty of the task. Since there was no prior IS or privacy research measuring affect, there were unanticipated factors that might have influenced the measurements. To mollify this weakness, a small sample size of subjects (10+) from Nova Southeastern University was used to judge the comprehension of the task and measurement procedures.

Resources Requirements

The following resources were required to complete the study

- **Literature Research:** Literature was retrieved from the Internet catalog of the Nova Southeastern University library. For literature that was not available online, a document retrieval service was requested at Nova Southeastern University library.
- **Survey Instrument Approval:** The Institutional Review Board (IRB) at Nova Southeastern University provided approval of the survey instrument in this study.

- **Survey Instrument Administration:** The Word Association Test, SC-IAT and surveys were accessed from the Internet using a secure hosted website provided by Millisecond using the Inquisit 4.0 software.
- **Data Analysis Software:** SmartPLS software (www.smartpls.de) was used to analyze data gathered from the survey.

Chapter 4

Results

Overview

The objectives of this quantitative study were to examine the extent to which affect influences privacy behavioral intentions and how the mediation of privacy concerns plays a role in this decision process. To fulfill the objectives, SPSS and PLS-SEM were employed to determine the relationship between affect (AFF), privacy concerns (PC) and behavioral intentions (BI).

This chapter is organized as follows: First, pre-analysis data screening was conducted and descriptive statistics of the final data used for analysis is presented. Second, the novelty of using two different methods to measure AFF is presented along with an analysis. Next, a measurement model analysis of PC and BI was conducted and presented. Finally, the proposed structural model that includes AFF, PC and BI is analyzed and results summarized.

Pre-Analysis Data Screening

Data was collected using Amazon Mechanical Turk (Mturk) crowd sourcing Internet marketplace. Using MTurk, the researcher solicited only Mturk Masters to participate because they have demonstrated 95% accuracy on previously completed work (Amazon Mechanical Turk, n.d.). Selecting an Mturk Master was preferred to insure that the participant would complete the study.

After a participant selected to take part in the survey, the participant was directed to the survey link at (<http://research.millisecond.com/castada1/BatchTest.web>) as instructed

in the advertisement (see Appendix J). The online survey was hosted in Millisecond's secure server environment. The participants were given an ample 25 minutes to complete the assignment based on a pilot test that took 11 to 12 minutes to complete along with a \$5.00 payment upon completing the assignment with a completion code. The completion code was uploaded to the researcher before payment was issued to verify results and grant payment. Ninety-four participants completed the survey and were paid.

Millisecond provided a participant ID that was used to ensure data alignment for the analysis. The researcher matched the completed survey data with each participant ID. Data were reviewed for the following: missing data, suspicious responses, outliers, and data distribution (Hair et al., 2013). Since each section of the online survey was required and did not allow for any section of the survey to be skipped, there was no missing data. Suspicious responses were detected in the Word Association Test (WAT). Fourteen participants were removed from the analysis because the responses did not reflect any words or concepts in the scenario just read. The researcher detected an anomaly in the data distribution. Three separate respondents provided identical responses for the PC and BI surveys (e.g., 7, 7, 7...7) including one outlier confirmed in a boxplot (see Appendix T). The measure of the WAT confirmed that the participants were engaged, because their answers reflected "words" or "images" from the scenario. After removing all unusable data, 80 out of 94 response samples were used for the data analysis.

Descriptive Analysis

Each survey response included gender, age, and educational demographic data. Slightly more males (52.1%) than females (47.9%) participated. They ranged from 18 years old to 65 with most participants in the age ranges of 24-34 (53.8%) and 35-44

(20.0%). The education level stated for the majority of the participants was some college and/or an associate's degree (46.2%) and Bachelor's degree (38.8%). All participants had Internet usage experience in excess of six years. The full distribution of demographic data is shown in Table 5 below.

Table 5. Frequencies and Percentages of Demographic Data ($N = 80$)

<i>Item</i>	<i>Frequency</i>	<i>Percentage</i>
<i>Gender</i>		
Female	37	46.2%
Male	43	53.8%
<i>Age Range</i>		
18-24	11	13.8%
24-34	43	53.8%
35-44	16	20.00%
45-54	7	8.8%
55+	3	3.7%
<i>Education Level</i>		
High School	7	8.8%
Some College & Associates Degree	37	46.2%
Bachelor's Degree	31	38.8%
Graduate Level +	5	6.2%

Measurement Model Analysis of Affect

Affect is measured using two indicators - Aff1 (an explicit measure of positive/negative feeling using a Word Association Test) and Aff2 (an implicit measure of positive/negative feeling using a Single Category–Implicit Association Test). Aff1 is referred to as “Aff1_WAT” and Aff2 is referred to as “Aff2_IAT”.

The result of Aff1_WAT is computed by summing the participant's score on the five words (Rubaltelli et al., 2010 Slovic et al., 2004) with a minimum score of -10 and maximum score of +10.

Aff2-IAT scores are “D-scores” based on an algorithm used by Karpinski and Steinman (2006) and Greenwald, Nosek and Banaji (2003). The D-scores are calculated based on the mean response time divided by standard deviation. The mean response time is arrived by subtracting the compatible block category from the incompatible block category, which may result in a negative value. Each difference score was divided by the standard deviation of the correct responses within both of the blocks. Thus, a positive score indicated that an attitude word is more related to a positive concept and a negative score is more related to a negative concept (Dohle et al., 2010). The Aff1_IAT raw scores range from a minimum score of -.914 to a maximum score of +.578.

The following is a descriptive breakdown of the raw scores for Aff1_WAT and Aff2_IAT. (see Table 6, below).

Table 6. Descriptive Statistics of Raw Scores of Aff1_WAT and Aff2_IAT Indicators

	Mean	Std. Deviation	Variance
Aff1_WAT	2.500	4.1062	16.861
Aff2_IAT	-.10357	.310227	.096

Correlation between Indicators

In order to compare and identify the correlation between the two measures, a z-score transform was performed on Aff1_WAT resulting in Z-score (Aff1_WAT). The Pearson Correlation of Z-score (Aff1_WAT) and Aff2_IAT was computed between these two variables, resulting in an $r = -.001$ ($n=80$) which was not significantly different from zero at the .05 level with a t-value of .994 as shown in Table 7. The conclusion is that Aff1_WAT and Aff2_IAT are uncorrelated.

Table 7. Pearson Correlation Results

		Zscore(Aff1_ WAT)	Aff2_IAT
Zscore(Aff1_ _WAT)	Pearson Correlation	1	-.001
	Sig. (2-tailed)		.994
	N	80	80
Aff2_IAT	Pearson Correlation	-.001	1
	Sig. (2-tailed)	.994	
	N	80	80

Measurement Model Analysis of Privacy Concerns and Behavioral Intentions

This study measures PC and BI as reflective constructs based on previous research (Smith et al., 1996; Malhotra et al., 2004; and Hong & Thong, 2012). Establishing that this instrument measures what it should be measuring (validity) and that it yields consistent results (reliability) is essential before testing the theoretical model (Lowry & Gaskin, 2014; Leedy & Ormrod, 2005). Evaluation of the reflective measurement model of PC and BI (see Figure 12) relies on evaluation criteria including internal consistency reliability, convergent validity and discriminant validity (Hair et al., 2014).

The first criterion evaluated is internal consistency reliability. Reliability refers to a scale's ability to measure constructs consistently over time and applies to reflective indicators (Lowry and Gaskin, 2014; Hair et al., 2014; Sekaran, 2003). Due to Cronbach alpha's limitation in PLS-SEM, it is more appropriate to apply composite reliability (Hair et al.). Composite reliability is interpreted similarly as Cronbach's alpha with values greater than .70 (Hair et al.). All first order constructs demonstrated a level of composite

reliability well above the recommended threshold of .70 (Hair et al.; Lowry & Gaskin, 2014) as shown in Table 8.

To establish convergent validity, outer loadings of the indicators as well as average variance extracted (AVE) needs to be established (Hair et al. 2014). Convergent validity is established when highly correlated scores obtained from two different instruments measure the same concept (Lowry & Gaskin, 2014; Sekaran, 2003). SmartPLS was employed to identify values above .708 to determine if the factor outer loadings were significant (Hair et al., 2014). All PC and BI first order constructs had indicators that load above .708, suggesting sufficient indicator reliability except for indicator I-4 (.683) below the accepted value. The value of .683 was removed from the measurement model. The result of removing the indicator only decreased the AVE. The AVE decrease was not beneficial and thus the item was restored. Restoring the indicator maintains an acceptable AVE value of .466 approaching the standard acceptable value of .50 (Hair et al. 2014, p. 107). Finally, convergent validity on the construct level is determined by AVE. An AVE value of .50 or higher indicates that the construct explains more than half the variance of its indicators. In the case of this study, all of the first order constructs of PC and BI are greater than .50 suggesting that the measures correlate positively.

Discriminant validity implies that a construct is unique and uncorrelated with other constructs in the model (Hair et al., 2014; Sekaran, 2003). One method of determining discriminant validity was identifying the cross loadings. “Discriminant validity is adequate if the cross loadings are more than the absolute value of .100 distant from the loading of the primary latent variable (Lowry & Gaskin, 2014, p. 2).” The second method of determining discriminant validity is accomplished using Fornell-Larcker

criterion, which is a more conservative approach. This method was used for those cross loadings that have loadings of .100 or less from primary construct loading (see Appendix L). The cross loadings between first order privacy concern constructs such as SEC & COL and COL and CON had a .100 difference. The SQRT of each construct AVE exceeded the highest correlation between the two constructs thus confirming the discriminant validity. Discriminant validity was established for all constructs (see Table 8 below).

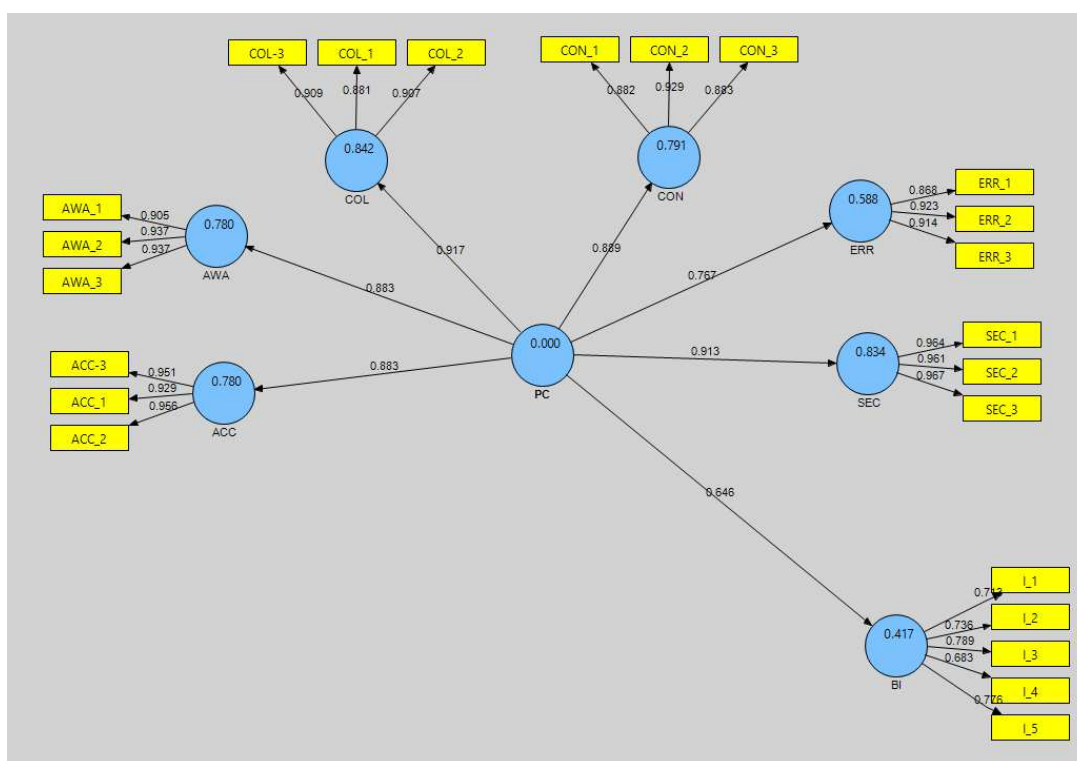


Figure 12. Measurement Model of PC and BI

Table 8. Reflective Measurement Model Results of First Order Constructs

1st Order Variables	Indicators	Loadings	Indicator Reliability	Composite Reliability	Ave	Discriminant Validity
AWA	AWA_1	0.905	0.820	0.948	0.858	Yes

	AWA_2	0.937	0.877			
	AWA_3	0.937	0.878			
ACC	ACC_1	0.929	0.862	0.962	0.894	Yes
	ACC_2	0.956	0.914			
	ACC_3	0.951	0.905			
CON	CON_1	0.882	0.777	0.926	0.807	Yes
	CON_2	0.929	0.863			
	CON_3	0.883	0.780			
COL	COL_1	0.881	0.775	0.926	0.808	Yes
	COL_2	0.907	0.822			
	COL_3	0.909	0.826			
ERR	ERR_1	0.868	0.754	0.929	0.814	Yes
	ERR_2	0.923	0.852			
	ERR_3	0.914	0.836			
SEC	SEC_1	0.964	0.929	0.975	0.929	Yes
	SEC_2	0.961	0.924			
	SEC_3	0.967	0.936			
BI	I-1	0.713	0.508	0.858	0.548	Yes
	I-2	0.736	0.541			
	I-3	0.789	0.622			
	I-4	0.683	0.466			
	I-5	0.776	0.602			

Structural Model Analysis of Affect, Privacy Concerns and Behavioral Intentions

The structural model analysis assesses the impact that AFF has on PC and BI using a twofold hypothesis: a) AFF has an impact on PC and therefore influences the level of impact on BI, and b) AFF has a direct impact on BI. Formative indicators for AFF proved that Aff2_IAT has the most significance with Aff1_WAT having no relevance. Removing Aff_WAT would result in a single indicator construct but prior research (Dohle et al., 2010; Slovic, 2010) suggested both indicators do measure AFF. Thus, the affect measured in this study maybe different then what was intended.

This part of the analysis uses the reflective measurement of PC and BI and the formative measurement of AFF to confirm the nomological link between these constructs

(Lowry & Gaskin, 2014). Collinearity values were examined using SPSS statistics to evaluate the exogenous variable, AFF, on the endogenous variables PC and BI. The tolerance levels below .2 and VIF above 5.0 is indicative of collinearity. In this case, there are no collinearity issues between the two constructs, AFF and PC, as shown in Table 9 below.

Table 9. Collinearity Statistics of AFF and BI Constructs

	Tolerance	VIF
AFF	.980	1.020
PC	.980	1.020

a. Dependent Variable: BI

The path coefficient for the relationship between PC → BI was $\rho = 0.658$ ($p < .001$) (Hair et al., 2014, p172) which was significant. The path coefficient of AFF → PC was minor with a negative influence of $\rho = -0.203$ and not statistically significant. The path coefficient of AFF → BI was negligible at $\rho = 0.069$ and not statistically significant. Therefore, AFF has no influence on BI (see Table 10 and Figure 13).

Table 10. Path Coefficients and Significance of AFF, PC and BI Constructs

Path	Path Coefficients (ρ)	p Values	Significance Level
PC → BI	0.658	0.000	***
AFF → PC	-0.203	0.097	NS
AFF → BI	0.069	0.593	NS

* $p < .05$, ** $p < .01$, *** $p < .001$

Note: NS = not significant

Table 11. Coefficient of Determination and Relevance of AFF and PC Constructs on BI Construct

Endogenous Latent Variable	R ²	Q ²
PC (AFF -> PC)	0.041	0.027
BI (AFF + PC ->BI)	0.420	0.220

To understand the impact of the predictor variables, PC and AFF, on the endogenous construct, BI, an examination of the f^2 effect size may be prudent. According to Hair et al., the effect size, allows assessing an exogenous construct contribution to the endogenous latent variable. The f^2 value of 0.02, 0.15 and 0.35 indicate respectively the construct's small, medium, and large effect on the endogenous variable. In this structural model, AFF has no effect whereas PC has a large effect on BI as shown in Table 12.

Table 12. Effect size f^2 of BI

	<i>BI</i>
	f^2
PC (removed AFF)	.684
AFF (removed PC)	.005

Summary of Results

The hypotheses that a negative affect leads to lower disclosure of private information online and that a positive affect leads to a higher disclosure was not substantiated as shown in Tables 9 through 12. The hypotheses that a negative affect causes higher privacy concerns and a positive affect causes lower privacy concerns were not supported. Finally, the hypothesis that privacy concerns mediates the relationship between affect and

behavioral intentions was not supported. Based on the comprehensive analysis, affect does not have influence on privacy concerns or behavioral intentions. The findings are summarized in Table 13 below.

Higher privacy concerns led to less disclosure of private information online hence, privacy concerns significantly predicted behavioral intentions as shown in Table 10.

There is demonstrated moderate predictive accuracy based on the R^2 value (.417) of BI that has an acceptable predictive relevance Q^2 value (.220). The hypothesis that lower privacy concerns led to more disclosure of private information online was not supported since this study did not vary the scenario to elicit lower privacy concerns.

Table 13. Summary of Findings for Research Hypotheses

Hypothesis	Hypothesis Description	Results
Hypothesis 1a	<i>Higher privacy concerns lead to less disclosure of private information online (a privacy behavioral intention)</i>	Supported
Hypothesis 1b	<i>Lower privacy concerns lead to more disclosure of private information online (a privacy behavioral intention)</i>	Not Supported
Hypothesis 2a	<i>Negative affect leads to lower disclosure (a privacy behavioral intention)</i>	Not Supported
Hypothesis 2b	<i>Positive affect leads to a higher disclosure (a privacy behavioral intention)</i>	Not Supported
Hypothesis 3a	<i>Negative affect causes higher privacy concerns.</i>	Not Supported
Hypothesis 3b	<i>Positive affect causes lower privacy concerns.</i>	Not Supported
Hypothesis 4	<i>The relationship between affect and behavior intentions (privacy behavior) is mediated by privacy concerns.</i>	Not Supported

Analysis suggests that, consistent with the standard model, privacy concerns affect behavioral intentions. When a subject was exposed to the privacy scenario, it was hypothesized that affect, a “faint whisper of emotion,” would have two effects. First, it was hypothesized that affect would influence privacy concerns. However, this link was not supported by data. Second, the hypothesis that affect directly influences behavioral intentions was not supported either.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

This chapter begins with the conclusions of this study. The research goals and questions are stated and the limitations are addressed. Next, the study's implications and contributions to the existing body of knowledge are discussed. The chapter ends with a summary that contains recommendations for future research followed by a summary of this chapter.

Conclusion

The purpose of this study was to examine how affect influences privacy behavioral intentions with the assumption that privacy concerns would mediate the effect.

The primary goals of this research were as follows:

1. Conceptualize privacy risk in terms of affect.
2. Compare and contrast affective and cognitive view of privacy decision-making.
3. Understand the role of affective vs. cognitive consequentialist factors on privacy concerns and privacy behavioral intentions.

This study was guided by the following research questions:

1. Do privacy concerns mediate privacy behavioral intentions?
2. How does affect, "a faint whisper of emotion," affect privacy concerns?
3. Does affect have an independent effect on privacy behavioral intentions?

All of these research questions were answered based on the findings showing that PC does have an effect on BI, AFF does not have any effect on PC and AFF did not have any effect on BI. It seemed contrary to the results of this study that affect did not have any influence based on previous research conducted by Slovic et al., 2010, Dohle et al., 2010 and Rubaltelli et al., 2010.

A review of the literature revealed that privacy concerns acting as a proxy for privacy was influenced by a cognitive consequentialist approach and only cognitive processes had been addressed in previous research. This research sought out to determine the extent to which affect, defined as “a faint whisper of emotion” (Slovic et al., 2004), would influence privacy behaviors. Previous research has shown that there are contextual settings that would influence the cognitive decision (John et al., 2011), which thus influences privacy behaviors. Additionally, phenomena such as the privacy paradox suggested other reasons people acted differently from what they stated (Belanger & Crossler, 2011; Rifon et al., 2007; Smith et al., 2011).

To understand these research questions, a quantitative study was designed using previous research and then a new model was proposed for predicting the influence of affect on privacy behaviors. In this research, because privacy behaviors are difficult to measure directly, behavioral intentions were measured instead (Malhotra et al 2004; Smith et al., 1996). A research model was developed that included an independent variable formative construct (AFF) and two dependent reflective constructs (PC and BI). Two distinct methods were used to measure affect: SC-IAT was developed and used to collect implicit affect data and the Word Association Test (WAT) was developed and used to collect explicit affect data. A 24-question survey instrument was developed and

used to collect data for privacy concerns and behavioral intentions. Eighty validated samples were collected for analysis and evaluation.

Two instruments were used to measure AFF: AFF1_WAT and AFF2_IAT. The Aff1_WAT measure was based on Slovic's (2010) affect heuristic. The psychological process implied in his model was summarized as follows: when a subject sees a stimulus, a network of "images" related to the stimulus is activated. Relying on Damasio (1994), Slovic (2010) argues that each of the nodes in the activation network ("images") has a positive/negative valence attached to it. For example, in this study, Subject 2 lists "cloud", "leaks", "safety", "breach", and "Internet" as five words that came to the participant's mind in the privacy-relevant scenario and correspond to "images". The feeling associated with the five words were rated by the subject 2 as "-1", "-1", "+1", "-1" and "0" respectively indicating the valence and strength of feeling associated with the "image". The summed score of "-2" then serves as a measure of an overall affect. Thus, on exposure to the privacy scenario, Subject 2 experiences a strong, negative affect (-2) which then influences further information processing.

Aff2_IAT measure, used by Dohle et al. (2010) relies on well-established findings from social psychology assuming people have an "implicit" evaluation of attitude objects different from their "explicit" evaluations. The implicit evaluations are discussed in an earlier chapter – briefly, the amount of time taken to associate a word with a universally "good" word (e.g., flower) versus universally "bad" word (e.g., insect) is used as a proxy measure for the sign and strength of the implicit evaluation. A key psychological insight is that such implicit evaluations do not involve careful deliberation.

The study found the two measures unrelated. Because both Aff1_WAT and Aff2_IAT were intended to measure an evaluative feeling (affect and implicit evaluation), it seemed somewhat surprising that they were uncorrelated. In the risk psychology literature, Slovic et al. (2010) relies on Aff1_WAT type measures and Dohle et al. (2010) use Aff2_IAT measures to conclude that affect matters. In this study, affect was a formative construct and thus, both Aff1_WAT and Aff2_IAT contributed independently to affect (AFF) as a whole. Since AFF is a formative construct, it was not necessary the measurements correlated and therefore, a PLS model was constructed using both measures as indicators of AFF.

PLS-SEM was used to assess the causal model and validate the hypotheses. The first hypothesis was supported. There was a definite relationship between PC and BI. The path coefficient between PC and BI was acceptable and significant. The BI construct R^2 value of .417 demonstrated moderate predictive accuracy and the Q^2 predictive relevance of .22 was acceptable. The second hypothesis was not supported since the study did not vary the scenario to elicit lower privacy concerns. The remaining hypotheses were not supported. Based on the final structural model analysis, AFF does not influence PC nor does it influence BI directly. Summary of hypotheses results are show in Table 13.

This study employed multiple new techniques, including conducting the entire study over the Internet, instead of using a traditional classroom or lab venue. Several limitations were unforeseeable. The use of two accepted standards of measurements (i.e., SC-IAT and WAT) were never used or validated in IS or Privacy research previously. The researcher could not confirm that the Web application survey was delivered effectively as the participant could not be directly monitored. The scenario was only

presented to the participant once at beginning of the study and not presented subsequent times to ensure the participant remembered the initial feeling. The scenario may have been too generic and not salient enough to elicit any privacy feeling or “affect”. Finally, the population sample used may have not been large enough to provide sufficient data. Although, PLS-SEM does allow for smaller samples (Hair et al., 2014), measuring affect may have required a larger sample.

Implications

This study has several implications for the existing body of knowledge in the Information Systems and Privacy fields. The causal model was developed using a new construct, AFF, as a new antecedent to PC and to BI, setting a precedent for further research. The model suggested that affect is the predominant influence in decision-making.

Until this study, the combination of SC-IAT and WAT to capture attitudes and correlate these variables had not been investigated. This research measured SC-IAT and WAT by allowing the participants to take the survey in the convenience of their home, simulating real-life online experience, in contrast to traditional lab settings.

Recommendations for Future Research

It was confirmed that privacy concerns do influence behavioral intentions by causal model analysis and PLS-SEM method. More research is in order to improve the instrument to measure affect and develop the causal model. The introduction of the new influential antecedent, “affect”, clearly needs to be addressed in the IS and Privacy field. Future study should include the use of a more salient privacy scenario that respondents

react to more strongly. Another recommendation is to conduct the study using a sample population larger than 80, to detect small effect sizes. Measuring AFF is novel in IS and requires further analysis to develop the AFF construct better when using SC-IAT and identifying appropriate target and attitude words associated with privacy. This study was conducted in participants' private environments and may be needed to be duplicated in a lab setting to ensure more control over the instrument administration.

Summary

Previous privacy concern research has addressed the cognitive consequentialist assumption that people deliberately evaluate the cost and benefits prior to risky activity. It identified antecedents such as perceived information control, ease of information access, perceived vulnerability and others. These antecedents have been more extensively researched than privacy concern outcomes such as privacy control practices, protective behavior, trust, privacy calculus, regulations and other concepts. The research, using standard survey measures, described the empirical cognitive processes to explain how privacy concerns impact intentions and behaviors to protect privacy.

This dissertation studied the influence of affect on privacy behavioral intentions and why previous privacy concern research does not adequately predict privacy behavioral intentions. Empirical observations have shown consumers behave in ways that do not match stated intentions. Further research is needed to address the role of affect in privacy decision-making.

Three primary goals of this study were: a) conceptualize privacy risk in terms of affect, b) compare and contrast affective and cognitive view of privacy decision making and c) understand the role of affective vs. cognitive-consequentialist factors on privacy

concerns and privacy behaviors. The following research questions were formulated to achieve these goals:

RQ1. Do privacy concerns mediate privacy behavioral intentions?

RQ2. How does affect, “a faint whisper of emotion,” affect privacy concerns?

RQ3. Does affect have an independent effect on privacy behavioral intentions?

Building upon cognitive consequentialist models, affect was introduced as a new construct. This subsequent affective model hypothesized that affect influences privacy concerns, privacy behaviors, both or neither. This could only be determined by modeling the following hypotheses:

H1a: Higher privacy concerns lead to less disclosure of private information online (a privacy behavioral intention).

H1b: Lower privacy concerns lead to more disclosure of private information online (a privacy behavioral intention).

H2a: Negative affect leads to lower disclosure (a privacy behavior intention).

H2b: Positive affect leads to a higher disclosure (a privacy behavior intention).

H3a: Negative affect causes higher privacy concerns.

H3b: Positive affect causes lower privacy concerns.

H4: The relationship between affect and behavioral intentions (privacy behavior) mediated by privacy concerns.

A Web application was used to collect data from 80 study participants exposed to a privacy scenario and then subjects were required to complete an implicit and explicit attitude test along with a standard survey. SPSS analyzed the affect measures, WAT and SC-IAT. Privacy concerns and behavior intentions were measured, analyzed and confirmed by the PLS-SEM method. The structural model was analyzed to determine the relationship between affect, privacy concerns and behavioral intentions. The analysis

included identifying and confirming the relationship between affect and behavioral intentions and then determining if privacy concerns influenced or mediated the relationship.

The finding indicated that affect did not have any impact on behavioral intentions nor privacy concerns thus privacy concerns does not mediate affect. The study did confirm that privacy concerns does have a relationship with behavioral intentions. Several limitations were evident in this study. Conducting the study over the Internet could not confirm effective delivery of the web application. The two measurements of affect not previously used in IS research was another limitation. The privacy scenario may not have been salient enough to invoke a privacy affect. Repeating the scenario several times may have mitigated this limitation. Finally, a larger sample could have added more data, analysis and validity to the study.

The study has valuable implications and contributions for IS and Privacy research. The causal model framework introduced a new construct, affect, acting as an antecedent to privacy concerns and behavioral intentions. Future research can employ this study to a) refine measurement instruments to measure affect better, b) increase the study sample to detect small effect sizes and c) ensure more control over the instrument administration instead of using an online survey. By understanding how affect is measured in the IS and Privacy domain, professionals can further research how consumers react to privacy hazards.

Appendix A

Introduction

A scenario will be presented to you and we want to know the images and associations that you have for the scenario. For example, If someone mentions the word *football*, several thoughts may come to mind such as “Super Bowl”, “college”, “Giants”, “winter” or “pizza.” We are interested in the first three to five thoughts are images that come to mind when you think of each of these words presented. After reading the scenario write the **first** thought or image that comes to mind in the space provided. Then, think of another *word* and provide the **second** thought or image that comes to mind. Then think of another *word* again and write down the **third** thought or image that comes to mind. Continue to this process until you have approximately have 5 words that fit the scenario. Do not spend too much time trying to come up with a thought or image. We want your initial reaction.

Appendix B

Word Association Test

Word Association Test Web Page 1

Add the first thoughts or images that come to mind in the blank section

Images/Words	
1 st Thought	
2 nd Thought	
3 rd Thought	
4 th Thought	
5 th Thought	

Word Association Web Page 2

Rate the Images and Words

The next step is to rate the words you wrote in the questionnaire on a scale from -2 to +2, with -2 being a most negative, and +2 being the most positive. Click on the rating that best fits.

	Images/Words	Ratings				
		Most Negative	Negative	Neither Negative or Positive	Positive	Most Positive
1 st Thought		-2	-1	0	1	2
2 nd Thought		-2	-1	0	1	2
3 rd Thought		-2	-1	0	1	2
4 th Thought		-2	-1	0	1	2
5 th Thought		-2	-1	0	1	2

Appendix C
Single Category Implicit Attitude Test

Block	Trials	Function	Left-key response	Right-Key response
1	24	Practice	Good words + “disclose” words	Bad Words
2	72	Test	Good words + ‘disclose’ words	Bad Words
3	24	Practice	Good Words	Bad words + ‘disclose’
4	72	Test	Good words	Bad words + disclose words

Appendix D

Attitude Object Words used in the SC-IAT

Attitude Words

Disclose

Divulge

Reveal

Upload

Appendix E

Target Object Words used in the SC-IAT

SC – IAT Target Words

Good Words		Bad Words
Safe		Unsafe
Wonderful		Dangerous
Stable		Terrible
Secure		Shaky
Protected		Vulnerable

Appendix H

Demographics Survey

“About You” Web Page

Please select the responses representing the most appropriate answer for you:

1	Gender	Male <input type="radio"/>	Female <input type="radio"/>					
2	Age	Under 18 <input type="radio"/>	18-25 <input type="radio"/>	26-35 <input type="radio"/>	36-45 <input type="radio"/>	46-55 <input type="radio"/>	56-65 <input type="radio"/>	Over 65 <input type="radio"/>
3	Education Level	Some School, no degree <input type="radio"/>	High School Graduate <input type="radio"/>	Some College, No Degree <input type="radio"/>	Bachelor's Degree <input type="radio"/>	Master's Degree <input type="radio"/>	Doctorate Degree <input type="radio"/>	Post Doctorate <input type="radio"/>
4	Internet Experience	Less than a year <input type="radio"/>	Less than 2 years <input type="radio"/>	Less than 3 years <input type="radio"/>	Less than 4 years <input type="radio"/>	Less than 5 years <input type="radio"/>	Less than 6 years <input type="radio"/>	More than 6 years <input type="radio"/>

Appendix I

IRB Approval Letter from Nova Southeastern University



NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: David Castano
From: Ling Wang, Ph.D.
Institutional Review Board

Date: Sep. 5, 2014

Re: *Affect and Online Privacy Concerns*

IRB Approval Number: wang08151402

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. 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 these 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 REACTIONS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 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: Protocol File

Appendix J

Mturk Advertisement

Online Decision Processing Academic Study			
Requester: David Castano	Reward: \$5.00 per HIT	HITs available: 0	Duration: 25 Minutes
Qualifications Required: Masters has been granted			

HIT Preview

Instructions

We are conducting an **Academic Study** about how you use the Internet to conduct online transactions. Select the link below to complete the survey. At the end of the survey, you will receive a Mturk Task number to paste into the box below to receive \$5.00 credit for taking our survey. *If you have any problems during this survey, please contact dcastano@nova.edu. We will respond within a few hours if you have any issues. This survey will be closely monitored.*

This is an **Academic Study conducted by a PhD candidate at Nova Southeastern University**. You will also be presented with a "consent" form and you have the option to back out if you deem necessary. *Note: This study will not collect any personal information such as names, address, ssn, etc.* This is an anonymous study only!! We just want to understand how people make decisions online.

Make sure to leave this window open as you complete the survey. When you are finished, you will return to this page to paste the code into the box.

Description of the surveys to be completed.

The surveys are voluntary and conducted by a PhD candidate at Nova Southeastern University as part of a candidate's dissertation requirements.

You will be participating in a series of online surveys that will take a total of **10 to 15 minutes to complete** (average has been 12 minutes).

- The first test is a Word Association Test (dynamic survey) that ask you to present words you think about and then rate them based on a scenario presented to you.
- The second test is a Single Category Association test (dynamic survey) that ask you to match words based on a specific "word". This is a timed test that requires the use of a standard English keyboard.
- The final portion of the study is a grouping of standard surveys that ask you about your concerns with using the Internet and standard demographic information such as your age, education and Internet experience.
- **Note: This study cannot be completed using an Tablet (Ipad, etc.) or Smartphone (Android, iPhone, etc.). Use of standard Laptop or Desktop (Windows or Mac) with latest browser preferred.**

Appendix K

Overview and Loadings of Second Order PC and First Order BI Constructs

Overview

	AVE	Composite Reliability	R Square	Cronbach's Alpha	Communality	Redundancy
ACC	0.8936	0.9618	0.7803	0.9404	0.8936	0.6972
AWA	0.8584	0.9479	0.7805	0.9174	0.8584	0.6696
BI	0.5479	0.858	0.4169	0.797	0.5479	0.2156
COL	0.8077	0.9264	0.8418	0.8812	0.8077	0.6753
CON	0.8066	0.926	0.7906	0.8798	0.8066	0.6371
ERR	0.8138	0.9291	0.588	0.8858	0.8138	0.4688
PC	0.6551	0.9714	0	0.9684	0.6551	0
SEC	0.9294	0.9753	0.8337	0.962	0.9294	0.7748

First Order Loadings

	ACC	AWA	BI	COL	CON	ERR	PC	SEC
ACC-3							0.8315	
ACC-3	0.9512							
ACC_1							0.8322	
ACC_1	0.9286							
ACC_2							0.8414	
ACC_2	0.9559							
AWA_1							0.8111	
AWA_1		0.9054						
AWA_2							0.8361	
AWA_2		0.9366						
AWA_3							0.8077	
AWA_3		0.9372						
COL-3							0.8764	
COL-3				0.9088				
COL_1							0.7388	
COL_1				0.8805				
COL_2							0.8479	
COL_2				0.9065				
CON_1							0.8041	

Appendix L

Cross Loadings of First Order PC and First Order BI Constructs

	ACC	AWA	COL	CON	ERR	SEC	BI
ACC-3	0.9512	0.6868	0.7076	0.687	0.6305	0.701	0.5104
ACC_1	0.9286	0.6884	0.72	0.6933	0.5438	0.7733	0.3669
ACC_2	0.9559	0.6671	0.6891	0.6663	0.6505	0.7803	0.488
AWA_1	0.6196	0.9054	0.7268	0.7257	0.584	0.6976	0.5879
AWA_2	0.6878	0.9366	0.78	0.7548	0.4863	0.7239	0.5822
AWA_3	0.6937	0.9372	0.7394	0.736	0.4786	0.6424	0.5666
COL-3	0.6842	0.776	0.9088	0.7737	0.6322	0.8234	0.5816
COL_1	0.596	0.6457	0.8805	0.5532	0.5292	0.6701	0.5343
COL_2	0.7238	0.7479	0.9065	0.7416	0.5698	0.7554	0.5621
CON_1	0.6969	0.6636	0.7042	0.8816	0.5685	0.7115	0.5374
CON_2	0.5974	0.6895	0.723	0.9288	0.5742	0.7082	0.5667
CON_3	0.6495	0.797	0.6579	0.8831	0.552	0.6135	0.5808
ERR_1	0.6798	0.5577	0.6239	0.6223	0.8681	0.6825	0.4242
ERR_2	0.5022	0.4937	0.569	0.5658	0.9229	0.5149	0.4744
ERR_3	0.54	0.4423	0.5398	0.5005	0.9144	0.494	0.4156
SEC_1	0.7828	0.7105	0.8248	0.7188	0.6392	0.9637	0.4949
SEC_2	0.7359	0.7431	0.7979	0.7131	0.5991	0.9611	0.5475
SEC_3	0.7806	0.6957	0.8015	0.7522	0.5934	0.9674	0.566
I_1	0.392	0.5044	0.5016	0.442	0.2967	0.4157	0.713
I_2	0.3951	0.4601	0.4963	0.5467	0.4509	0.5624	0.7358
I_3	0.3101	0.4455	0.462	0.401	0.4309	0.3966	0.7885
I_4	0.1595	0.2927	0.2989	0.2871	0.2832	0.2216	0.6829
I_5	0.4414	0.5461	0.4869	0.5569	0.3098	0.3749	0.7757

Appendix M

Fornell-Larcker Discriminant Validity for PC

Fornell-Larcker Criterion	Correlation	Corr. Sq.	Sqrt AVE
SEC&COL	0.8382	0.70257924	
SEC			0.964054
COL			0.898721
COL&CON	0.7743	0.59954049	
COL			0.898721
CON			0.898109

Appendix N

Overview, Loadings and Weights of First Order AFF on Second Order PC and First Order BI Constructs

Overview

	AVE	Composite Reliability	R Square	Cronbach's Alpha	Communality	Redundancy
ACC	0.8936	0.9618	0.7804	0.9404	0.8936	0.6972
AFF	0	0	0	0	0.5088	0
AWA	0.8584	0.9479	0.7806	0.9174	0.8584	0.6697
BI	0.5486	0.8584	0.4197	0.797	0.5486	-0.0065
COL	0.8077	0.9264	0.8418	0.8812	0.8077	0.6753
CON	0.8066	0.926	0.791	0.8798	0.8066	0.6373
ERR	0.8138	0.9291	0.5872	0.8858	0.8138	0.4681
PC	0.6551	0.9714	0.0411	0.9684	0.6551	0.0269
SEC	0.9294	0.9753	0.8339	0.962	0.9294	0.775

Outer Loadings

	ACC	AFF	AWA	BI	COL	CON	ERR	PC	SEC
ACC-3								0.8314	
ACC-3	0.9512								
ACC_1								0.8324	
ACC_1	0.9286								
ACC_2								0.8413	
ACC_2	0.9559								
AWA_1								0.8111	
AWA_1			0.9054						
AWA_2								0.8363	
AWA_2			0.9366						
AWA_3								0.8078	
AWA_3			0.9372						
Aff1		0.4627							
Aff2		0.8964							
COL-3								0.8764	
COL-3					0.9088				
COL_1								0.7387	

COL_1					0.8805				
COL_2								0.848	
COL_2					0.9065				
CON_1								0.8043	
CON_1						0.8817			
CON_2								0.8023	
CON_2						0.9288			
CON_3								0.789	
CON_3						0.8831			
ERR_1								0.758	
ERR_1							0.8682		
ERR_2								0.6626	
ERR_2							0.9229		
ERR_3								0.6367	
ERR_3							0.9144		
I_1				0.7125					
I_2				0.7321					
I_3				0.7929					
I_4				0.6873					
I_5				0.7736					
SEC_1								0.8883	
SEC_1									0.9637
SEC_2								0.8724	
SEC_2									0.9611
SEC_3								0.8804	
SEC_3									0.9674

Outer Weights

	ACC	AFF	AWA	BI	COL	CON	ERR	PC	SEC
ACC-3								0.0702	
ACC-3	0.3511								
ACC_1								0.0689	
ACC_1	0.3515								
ACC_2								0.0704	
ACC_2	0.3553								
AWA_1								0.0695	
AWA_1			0.3566						
AWA_2								0.0713	
AWA_2			0.3676						

Appendix O

Path Coefficient of First Order AFF on Second Order PC and First Order BI Constructs

	Original Sample (O)	Sample Mean (M)	Standard Deviation (SD)	Standard Error (STERR)	T Statistics (O/STERR)
AFF -> BI	0.0686	0.0621	0.1282	0.1282	0.535
AFF -> PC	-0.2026	-0.2075	0.1208	0.1208	1.677
PC -> ACC	0.8834	0.8797	0.0415	0.0415	21.2639
PC -> AWA	0.8835	0.8808	0.0288	0.0288	30.6461
PC -> BI	0.6582	0.6589	0.0692	0.0692	9.5171
PC -> COL	0.9175	0.9163	0.0214	0.0214	42.8335
PC -> CON	0.8894	0.8886	0.0386	0.0386	23.0106
PC -> ERR	0.7663	0.7675	0.0504	0.0504	15.198
PC -> SEC	0.9132	0.9133	0.0238	0.0238	38.3641

Appendix P

Cross Loadings of First Order AFF on Second Order PC and First Order BI
Constructs

	ACC	AFF	AWA	BI	COL	CON	ERR	PC	SEC
ACC-3	0.9512	-0.1813	0.6868	0.5092	0.7076	0.687	0.6305	0.8314	0.701
ACC_1	0.9286	-0.2605	0.6884	0.3652	0.72	0.6933	0.5438	0.8324	0.7733
ACC_2	0.9559	-0.131	0.6671	0.4868	0.6891	0.6663	0.6505	0.8413	0.7803
AWA_1	0.6196	-0.1742	0.9054	0.5878	0.7268	0.7257	0.584	0.8111	0.6976
AWA_2	0.6878	-0.1684	0.9366	0.5809	0.78	0.7548	0.4863	0.8363	0.7239
AWA_3	0.6937	-0.1194	0.9372	0.5652	0.7394	0.736	0.4786	0.8078	0.6424
Aff1	-0.1294	0.4627	-0.1394	0.0157	-0.1514	-0.0742	0.0194	-0.1084	-0.0768
Aff2	-0.1628	0.8964	-0.118	-0.081	-0.125	-0.2618	-0.0289	-0.1743	-0.1991
COL-3	0.6842	-0.1869	0.776	0.5804	0.9088	0.7737	0.6322	0.8764	0.8234
COL_1	0.5959	-0.1364	0.6457	0.5341	0.8805	0.5532	0.5292	0.7387	0.6701
COL_2	0.7238	-0.1529	0.7479	0.5613	0.9065	0.7416	0.5698	0.848	0.7554
CON_1	0.6969	-0.2645	0.6636	0.5358	0.7042	0.8817	0.5685	0.8043	0.7115
CON_2	0.5974	-0.265	0.6895	0.5644	0.723	0.9288	0.5743	0.8023	0.7082
CON_3	0.6495	-0.1835	0.797	0.5797	0.6579	0.8831	0.5521	0.789	0.6135
ERR_1	0.6798	-0.0859	0.5577	0.4235	0.6239	0.6223	0.8682	0.758	0.6825
ERR_2	0.5022	-0.0173	0.4937	0.4748	0.569	0.5658	0.9229	0.6626	0.5149
ERR_3	0.54	0.0709	0.4423	0.4156	0.5398	0.5005	0.9144	0.6367	0.494
I_1	0.392	-0.0418	0.5044	0.7125	0.5016	0.442	0.2967	0.4878	0.4157
I_2	0.3951	-0.1513	0.4601	0.7321	0.4963	0.5467	0.4509	0.5537	0.5624
I_3	0.3101	0.0827	0.4455	0.7929	0.462	0.401	0.4309	0.4621	0.3966
I_4	0.1595	0.0174	0.2927	0.6873	0.2989	0.2871	0.2832	0.29	0.2216
I_5	0.4413	-0.1043	0.5461	0.7736	0.4869	0.5568	0.3098	0.5175	0.375
SEC_1	0.7828	-0.1638	0.7105	0.4939	0.8248	0.7188	0.6393	0.8883	0.9637
SEC_2	0.7359	-0.222	0.7431	0.5461	0.7979	0.7131	0.5991	0.8724	0.9611
SEC_3	0.7806	-0.2239	0.6957	0.5642	0.8015	0.7522	0.5934	0.8804	0.9674

Appendix Q

Outer Loadings and Weights Mean, SD & T Stats of First Order AFF on Second Order PC and First Order BI Constructs

Outer Loadings

	Original Sample (O)	Sample Mean (M)	Standard Deviation (SD)	Standard Error (STERR)	T Statistics (O/STERR)
ACC-3 <- PC	0.8314	0.8249	0.0532	0.0532	15.6421
ACC-3 <- ACC	0.9512	0.9494	0.0147	0.0147	64.7611
ACC_1 <- PC	0.8324	0.8258	0.05	0.05	16.6569
ACC_1 <- ACC	0.9286	0.9253	0.0247	0.0247	37.5519
ACC_2 <- PC	0.8413	0.8381	0.0435	0.0435	19.3506
ACC_2 <- ACC	0.9559	0.9544	0.0152	0.0152	62.8702
AWA_1 <- PC	0.8111	0.8068	0.0471	0.0471	17.2297
AWA_1 <- AWA	0.9054	0.9026	0.0256	0.0256	35.3497
AWA_2 <- PC	0.8363	0.829	0.0477	0.0477	17.5502
AWA_2 <- AWA	0.9366	0.9344	0.0177	0.0177	52.9361
AWA_3 <- PC	0.8078	0.8048	0.0512	0.0512	15.7735
AWA_3 <- AWA	0.9372	0.9356	0.0229	0.0229	40.943
Aff1 -> AFF	0.4627	0.4607	0.4023	0.4023	1.1502
Aff2 -> AFF	0.8964	0.7042	0.3668	0.3668	2.4439
COL-3 <- PC	0.8764	0.8739	0.034	0.034	25.7894
COL-3 <- COL	0.9088	0.9074	0.0217	0.0217	41.9255
COL_1 <- PC	0.7387	0.7367	0.0738	0.0738	10.0042
COL_1 <- COL	0.8805	0.8784	0.0465	0.0465	18.9464
COL_2 <- PC	0.848	0.8429	0.0432	0.0432	19.6527
COL_2 <- COL	0.9065	0.905	0.0248	0.0248	36.5213
CON_1 <- PC	0.8043	0.8014	0.0443	0.0443	18.1747
CON_1 <- CON	0.8817	0.8828	0.0277	0.0277	31.8002
CON_2 <- PC	0.8023	0.8029	0.0658	0.0658	12.1929
CON_2 <- CON	0.9288	0.9283	0.0192	0.0192	48.3476
CON_3 <- PC	0.789	0.7875	0.0582	0.0582	13.5463
CON_3 <- CON	0.8831	0.8825	0.0391	0.0391	22.586
ERR_1 <- PC	0.758	0.7591	0.0552	0.0552	13.7313
ERR_1 <- ERR	0.8682	0.8707	0.0287	0.0287	30.2812
ERR_2 <- PC	0.6626	0.6564	0.0864	0.0864	7.6704
ERR_2 <- ERR	0.9229	0.9193	0.0254	0.0254	36.2904

ERR_3 <- PC	0.6367	0.6324	0.0732	0.0732	8.6953
ERR_3 <- ERR	0.9144	0.9113	0.0225	0.0225	40.5997
I_1 <- BI	0.7125	0.7078	0.0692	0.0692	10.2948
I_2 <- BI	0.7321	0.7245	0.0838	0.0838	8.7413
I_3 <- BI	0.7929	0.7877	0.0586	0.0586	13.53
I_4 <- BI	0.6873	0.6834	0.078	0.078	8.8146
I_5 <- BI	0.7736	0.7739	0.049	0.049	15.7929
SEC_1 <- PC	0.8883	0.8868	0.0321	0.0321	27.6354
SEC_1 <- SEC	0.9637	0.9624	0.0117	0.0117	82.2616
SEC_2 <- PC	0.8724	0.872	0.0298	0.0298	29.2822
SEC_2 <- SEC	0.9611	0.9599	0.0112	0.0112	85.6614
SEC_3 <- PC	0.8804	0.8791	0.0308	0.0308	28.5414
SEC_3 <- SEC	0.9674	0.9662	0.0102	0.0102	94.7856

Outer Weights

	Original Sample (O)	Sample Mean (M)	Standard Deviation (SD)	Standard Error (STERR)	T Statistics (O/STERR)
ACC-3 <- PC	0.0702	0.07	0.0033	0.0033	21.1915
ACC-3 <- ACC	0.3511	0.3514	0.0095	0.0095	36.9875
ACC_1 <- PC	0.0689	0.0687	0.0034	0.0034	19.9789
ACC_1 <- ACC	0.3515	0.3518	0.0095	0.0095	37.0476
ACC_2 <- PC	0.0704	0.0706	0.0037	0.0037	19.2195
ACC_2 <- ACC	0.3553	0.3573	0.0102	0.0102	34.6811
AWA_1 <- PC	0.0695	0.0697	0.0042	0.0042	16.3724
AWA_1 <- AWA	0.3566	0.3579	0.017	0.017	21.0128
AWA_2 <- PC	0.0713	0.0711	0.0037	0.0037	19.4928
AWA_2 <- AWA	0.3676	0.3676	0.015	0.015	24.4593
AWA_3 <- PC	0.0688	0.0691	0.004	0.004	17.0825
AWA_3 <- AWA	0.3551	0.3567	0.0121	0.0121	29.4615
Aff1 -> AFF	0.4434	0.4483	0.4167	0.4167	1.0641
Aff2 -> AFF	0.8867	0.6999	0.3799	0.3799	2.3341
COL-3 <- PC	0.0746	0.0749	0.0044	0.0044	16.8613
COL-3 <- COL	0.3956	0.3972	0.0228	0.0228	17.3789
COL_1 <- PC	0.0633	0.0635	0.0058	0.0058	10.9966
COL_1 <- COL	0.3334	0.3333	0.0185	0.0185	18.0501
COL_2 <- PC	0.0721	0.0721	0.0039	0.0039	18.4428
COL_2 <- COL	0.3827	0.3828	0.0196	0.0196	19.5621
CON_1 <- PC	0.0688	0.0689	0.0036	0.0036	19.2256
CON_1 <- CON	0.3739	0.3737	0.0212	0.0212	17.6594

CON_2 <- PC	0.0691	0.0695	0.0066	0.0066	10.5242
CON_2 <- CON	0.373	0.3737	0.0211	0.0211	17.7026
CON_3 <- PC	0.0679	0.0682	0.0042	0.0042	16.1285
CON_3 <- CON	0.3668	0.3663	0.0114	0.0114	32.2806
ERR_1 <- PC	0.0635	0.064	0.0054	0.0054	11.7833
ERR_1 <- ERR	0.4093	0.4147	0.0421	0.0421	9.7192
ERR_2 <- PC	0.0567	0.0564	0.0059	0.0059	9.5719
ERR_2 <- ERR	0.3578	0.3551	0.0225	0.0225	15.8787
ERR_3 <- PC	0.0537	0.0537	0.0052	0.0052	10.2806
ERR_3 <- ERR	0.3438	0.3427	0.0168	0.0168	20.461
I_1 <- BI	0.2837	0.2815	0.0402	0.0402	7.0495
I_2 <- BI	0.3157	0.3122	0.0609	0.0609	5.187
I_3 <- BI	0.2762	0.2746	0.0409	0.0409	6.7603
I_4 <- BI	0.1713	0.1733	0.0447	0.0447	3.8331
I_5 <- BI	0.2973	0.2974	0.047	0.047	6.3262
SEC_1 <- PC	0.0742	0.0745	0.0041	0.0041	18.1047
SEC_1 <- SEC	0.3489	0.3492	0.0068	0.0068	51.6494
SEC_2 <- PC	0.0737	0.0741	0.0044	0.0044	16.6023
SEC_2 <- SEC	0.3426	0.3434	0.0062	0.0062	55.3156
SEC_3 <- PC	0.0745	0.0748	0.0043	0.0043	17.5307
SEC_3 <- SEC	0.3458	0.3461	0.0061	0.0061	56.5722

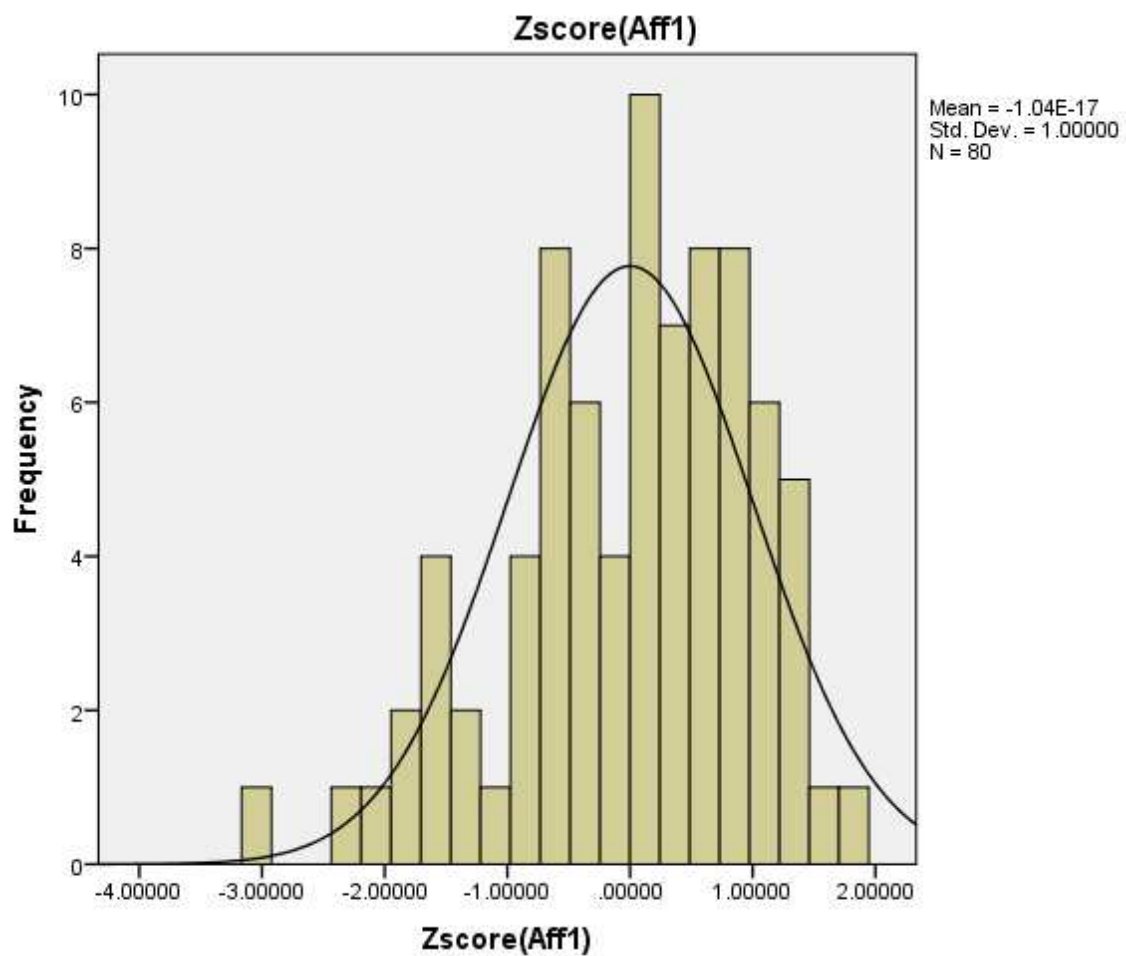
Appendix R

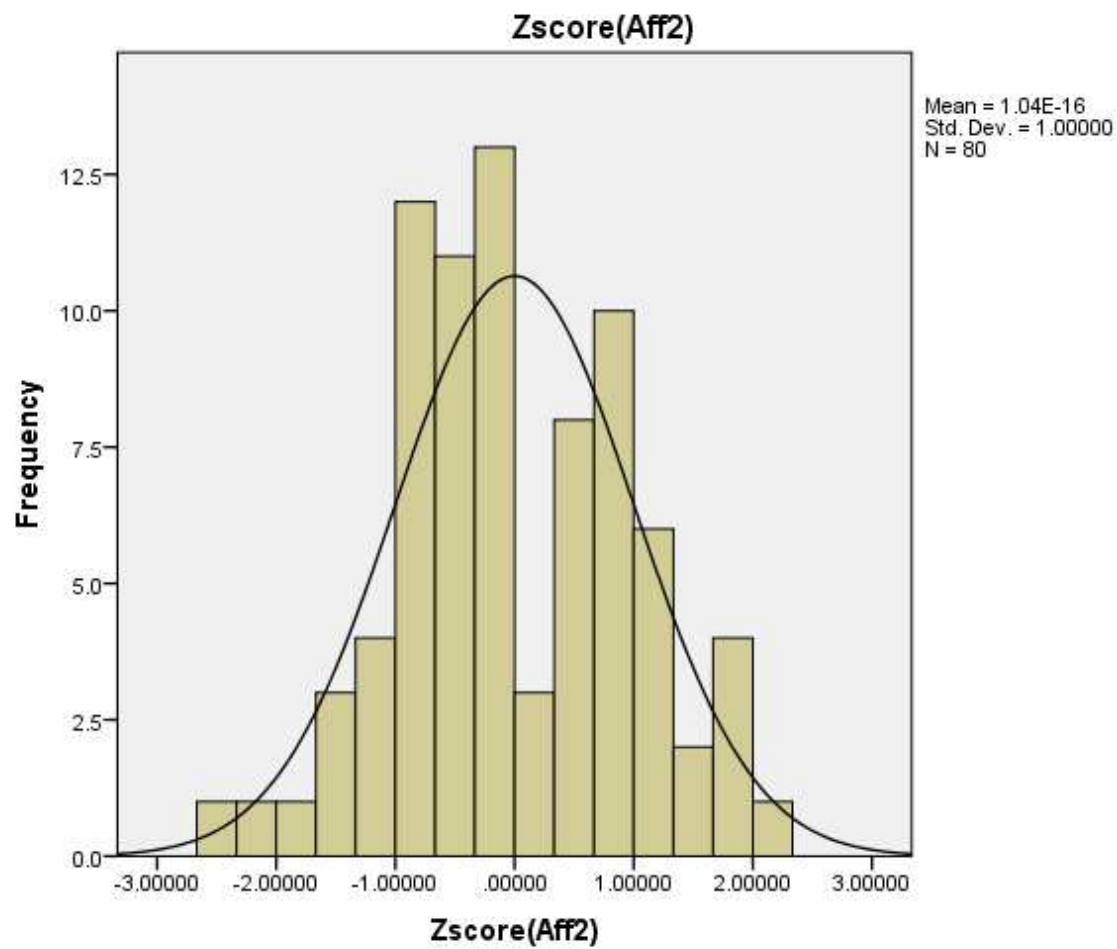
Latent Variable Correlations of First Order AFF on Second Order PC and First Order BI Constructs

	ACC	AFF	AWA	BI	COL	CON	ERR	PC	SEC
ACC	1	0	0	0	0	0	0	0	0
AFF	-0.2018	1	0	0	0	0	0	0	0
AWA	0.7201	-0.1664	1	0	0	0	0	0	0
BI	0.4801	-0.0648	0.6239	1	0	0	0	0	0
COL	0.7464	-0.1779	0.8085	0.6225	1	0	0	0	0
CON	0.7216	-0.265	0.7976	0.6235	0.7743	1	0	0	0
ERR	0.6436	-0.017	0.557	0.4862	0.6446	0.6293	1	0	0
PC	0.8834	-0.2026	0.8835	0.6443	0.9175	0.8894	0.7663	1	0
SEC	0.7951	-0.2106	0.743	0.5545	0.8382	0.7552	0.6335	0.9132	1

Appendix S

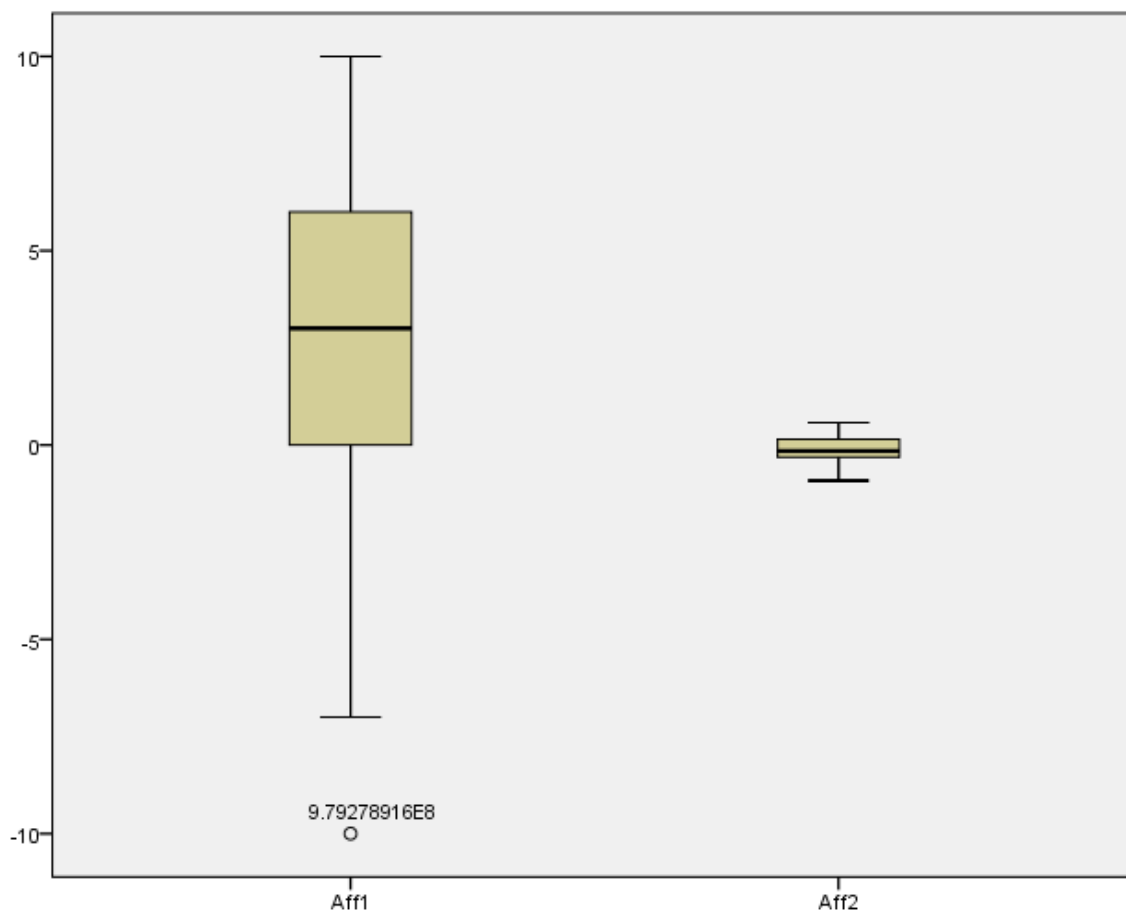
Frequency Histograms for the z score of Aff1 and Aff2





Appendix T

Outlier Boxplot of AFF1 and AFF2



References

- Amazon Mechanical Turk – Welcome. (n.d). Retrieved August 22, 2014 from <https://www.mturk.com/mturk/welcome>
- Anderson, L. A., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal information. *Information System Research, 22*(3), 469-490.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211.
- Barret, L.F., & Bliss-Moreau, E. (2009). Affect as a psychological primitive. *Adv Exp Soc Psychol. 41*, 167-218
- Belanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1041.
- Berendt, B., Oliver Gunther, & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM, 48*(4), 101-106.
- Castaneda, J. A., Montoso, F. J., & Luque, T. (2007). The dimensionality of customer privacy concern on the internet. *Online Information Review, 31*(4), 420.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104 - 115.
- Damasio, A.R., (1994). *Descarte's Error: Emotion, Reason and the Human Brain*, Avon: New York.
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behavior & Information Technology, 23*(6), 413-422.
- Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61-82.
- Dinev, T. & Hart, P. (2006b). Privacy concerns and levels of information exchange: An empirical investigation of intended e-Services use. *E-Service Journal. 4*(3), p.25 - 58.
- Dohle, S., Keller, C., Siegrist, M. (2010). Examining the relationship between affect and implicit associations: Implications for risk perception. *Risk Analysis, 30*(7), 1116-1128.

- Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust and commitment. *Journal of Business Research, 59*(8), 877-886.
- Epstein, S. (1994). Integration of the cognitive and psychodynamic unconscious. *American Psychologist, 49*, 709-724.
- Fischhoff, B., Slovic, P., Read, S., & Lichtenstein, S. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Science, 9*, 127-152.
- Finucane, M. L., Alhakami, A., Slovic, P., Johnson, S.M. (2000). The affect heuristic in judgments of risk and benefits. *Journal of Behavioral Decision Making, 13*(1), 1-17.
- Glover, S. & Benbasat, I. (2011). A model of e-commerce transaction perceived risk, *International journal of electronic commerce, 15*(2), 47-78.
- Graeff, Timothy R. & Harmon, Susan (2002). Collecting and using personal data: Consumer awareness and concerns. *The Journal of Consumer Marketing, 19*(4/5), 302-318.
- Greenwald, A. G., Banaji, M. R., Nosek, B. (2003). Understanding and using the implicit association test: I. An improved scoring algorithm. *Journal of personality and social psychology, 85*(2), 197-216.
- Greenwald, A. G., McGhee, D., & Schwartz, J. (1998). Measuring individual differences in implicit cognition: The implicit association test. *Journal of personality and social psychology, 74*(6), 1464-1480.
- Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS – SEM)*. Sage Publications.
- Hoadley, C. M., Xu, H., Lee, J. L., & Rosson, M. B. (2009). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications, 9*(1), 50-60.
- Hong, W., & Thong, J. Y. (2012). Internet privacy concerns: An integrated conceptualization and four empirical tests. *MIS Quarterly*.
- Hsee, C. K. (1996). Elastic justification: How unjustifiable factors influence judgments. *Organizational Behavior and Human Decision Processes, 67*, 242-257.

- John, L. K., Acquisiti, A., Lowenstein, G. (2011). The best of strangers: Context-dependent willingness to divulge personal information. *Journal of Consumer Research*, 37(5), 858-873.
- Johnston, A. C., & Warkenstin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.
- Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux: New York.
- Karpinski, A. & Hilton, J. L. (2001). Attitudes and the implicit association test. *Journal of Personality and Social Psychology*, 81(5), 774-788.
- Karpinski, A., Steinman, R.B, & Hilton, J.L. (2005). Attitude importance as a moderator of the relationship between implicit and explicit attitude measures. *Personality Social Psychology Bulletin*, 31(7), 949-962.
- Korzan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *The Journal of Computer Information Systems*, 48(4), 15-25.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: planning and design*. Upper Saddle River: Pearson Education Inc.
- Li, Y. (2011). *Developing a dichotomy of information privacy concerns*. Paper presented at the AMCIS 2011 Proceedings.
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54, 471-481.
- Liebowitz, M. (2011). Credit-Card skimmers found in Silicon Valley supermarkets. Retrieved on November 3, 2012, from <http://www.technewsdaily.com/7349-atm-skimmers-silicon-valley-supermarkets.html>
- Locke, L. F., Spirduso, W. W., & Silverman, S. J. (2000). *Proposals that work: A guide for planning dissertations and grant proposal* (4 ed.). Thousand Oaks, CA: Sage Publications.
- Lowenstein, G. F., Weber, E.U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, 127(2), 267-286.
- MacGregor, D.G., Slovic, P., Dreman, D., & Berry, M. (2000). Imagery, affect and financial judgment. *The Journal of Psychology and Financial Markets*, 1(2), 104-110.

- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale and a casual model. *Information Systems Research, 15*(4), 336-355.
- Mehta, A. (1994). How advertising response modelling (ARM) can increase ad effectiveness. *Journal of Advertising Research, 62-74*.
- Nosek, B. A. & Banaji, M.R. (2009). Implicit attitude. In P. Wilken, T. Bayne, & A. Cleeremans (Eds), *Oxford Companion to Consciousness*. Oxford, UK: Oxford University Press.
- Nosek, B. A., Greenwald, A.G., & Banaji, M. R. (2007). The implicit association test at age 7: A methodological and conceptual review. In J. A. Bargh (Ed), *Automatic processes in social thinking and behavior*.
- Nyshadham, E. & Castano, D. (2012). Affect and online privacy concerns. Proceeding of the Thirty Third International Conference on Information Systems. Orlando, Florida. Retrieved July 25, 2013 from <http://ssrn.com/abstract=2051044>.
- Nyshadham, E. & Gabriel, I. (2011). Perception of risk due to online hazards. Retrieved July 25, 2013 from <http://ssrn.com/abstract=1953929>.
- Nyshadham, E. & Minton, R. (2013). Affect and risks in IS research. Proceedings of the Sixteenth Annual Conference for the Southern Association of Information Systems. Retrieved March 5, 2013, from <http://ssrn.com/abstract=2225446>.
- Office of Management and Budget. (2007). Memorandum for the heads of executive departments and agencies: Safeguarding against and responding to the breach of personally identifiable information. Retrieved March 28, 2014 from <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>
- Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.
- Pham, M. T. (2011). Emotion and rationality. A critical review of empirical evidence. *Review of General Psychology, 11*(2), 157-178.
- Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.
- Phelps, J., D'Souza, G., & Nowak, G. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 16.

- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy Marketing*, 19(1), 27-41.
- Reiss, S., Peterson, R. A., Gursky, D. M., & McNally, R. J. (1986). Anxiety sensitivity, anxiety frequency and the prediction of fearfulness. *Behavioral Research Theory*, 24(1), 1-9.
- Rifon, N. J., LaRose, R., & Lewis, M. L. (2007). Resolving the Privacy Paradox: Toward a social-cognitive theory of consumer privacy protections. Retrieved from <https://www.msu.edu/~wirthch1/privacyparadox07.pdf>.
- Rivenbark, D. (2012). Valuing the risk from privacy loss: Experimentally elicited beliefs explain privacy behavior. Retrieved from http://cear.gsu.edu/workshops/10/papers/Rivenbark_The%20Value%20of%20Privacy%20--%20Subjective%20Beliefs%20Explain%20Behavior_15.pdf
- Rubaltelli, E., Pasini, G., Rumiati, R., Olsen, R., Slovic, P. (2010). The influence of affective reactions on investment decisions. *Journal of Behavioral Finance*, 11(3), 168-176.
- Schiff, J. L., (2014, April 16). 9 Things you need to know before you store data in the cloud. Retrieved April 17, 2014 from http://www.cio.com/article/751584/9_Things_You_Need_to_Know_Before_You_Store_Data_in_the_Cloud?page=1&taxonomyId=3024
- Sekaran, U. (2003). *Research methods for business: A skill building approach* (4 ed). John Wiley & Sons.
- Shafir, E., Simonsen, L., & Tversky, A. (1993). Reason-based choice. *Cognition*, 49, 11-36.
- Sheehan, K. & Hoy, M., (1999). Flaming, complaining, and abstaining: How online users respond to privacy concerns. *Journal of Advertising*, 28(3), 37-51.
- Slovic, P. (1986). Informing and educating the public about risk. *Risk Analysis*, 6(4), 403-415.
- Slovic, P. E. (2000). *The perception of risk*. Earthscan Publications.
- Slovic, P. (2010). *The feeling of risk: New perspectives on risk perception*. Earthscan publications.
- Slovic, P., Finucane, M.L., Peters, E., & MacGregor (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and rationality. *Risk Analysis*, 24(4), 311-322.

- Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, 177, 1333-1352.
- Slovic, P., Peters, E., Finucane, M.L., & MacGregor, D.G. (2005). Affect, risk and decision-making. *Health Psychology*, 24(4), S35-S40.
- Smith, J. H., Dinev, T., & Xu, H. (2011). Information Privacy Research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.
- Smith, J. H., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.
- Wall Street Journal. "Google's iPhone Tracking" (2012)
http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDIwNjEYNDYyWj.html?mod=wsj_share_email
- Westin, A. F. (1967). *Privacy and Freedom*. Atheneum, New York: McClelland & Stewart.
- Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2008). *Examining the formation of individual's privacy concerns: Toward an integrative view*. Paper presented at the ICIS 2008 Proceedings, Paris.
- Xu, H., Dinev, T., Smith, J. H., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), 798-824.
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of American Society for Information Science and Technology*, 58(5), 710-722.
- Zajonc, R. B. (1980). Feeling and thinking: Preferences need no inferences. *American Psychologist*, 35, 151-175.
- Zeithaml, V., Berry, L., Parasuraman, A. (1996). The behavioral consequences of service quality. *Journal of Marketing*, 60(2), 31-46.
- Zukowski, T., & Brown, I. (2007). *Examining the influence of demographic factors on Internet users' information privacy concerns*. Paper presented at the South African Institute of Computer Scientist and Information Technologist on IT Research in Developing Countries.