

**ESSAYS IN INFORMATION PRIVACY:  
DEFINING & ANALYZING ONLINE EQUIVOCATION**

---

A Dissertation  
Submitted to the  
Temple University Graduate School

---

In Partial Fulfillment  
of the Requirements for the Degree  
Executive Doctorate of Business Administration

---

By  
Irene Graff  
May, 2018

Review Committee:

Susan Mudambi  
*Advisory Chair, Research Professor, Marketing & Supply Chain Management  
Academic Director, Executive DBA Program*

Paul Pavlou  
*Senior Associate Dean  
Milton F. Stauffer Professor  
Co-Director, Data Science Institute*

Detmar W. Straub  
*Professor and IBIT Research Fellow, Fox School of Business  
Regents Professor Emeritus, University System of Georgia and Georgia State University*

Eric M. Eisenstein  
*Director, MS Business Analytics, Department of Statistical Science  
Director of Graduate Programs, Department of Marketing*

©

Copyright  
2018

By

Irene Graff  
All Rights Reserved

## ABSTRACT

As quickly as individuals engage in new ways to share personal information online, their concerns over privacy are increasing. Online engagement is not just “to share or not to share,” but a continuum of the disclosure. To remain engaged online and to avoid privacy exposure, individuals sometimes omit or provide inaccurate information. This process is defined as *online equivocation*. Drawing on privacy calculus research, this study investigates how individuals use online equivocation to lower privacy concerns in mobile computing, essentially reducing the costs of online disclosure. Several studies are used to explain and analyze online equivocation and draw out the implications for theory, firms, society, and individuals. To achieve this a qualitative questionnaire was distributed among 547 individuals across the United States asking subjects to report whether they had provided inaccurate data online in privacy-concerned situations and to detail the various strategies used. The results indicate that online equivocation can be categorized into five distinct strategies organized on a continuum of level of effort: omission, abbreviation, substitution, combined substitution, and alternative persona. A follow-up questionnaire was completed with 582 respondents that showed individuals use one more online equivocation strategy in the majority of personal information sharing. This result provides a framework for further study of online equivocation. A third and final survey tested a new conceptual model constructed from the results of the previous questionnaires to examine the effects of online equivocation on privacy concerns, collecting 2,947 responses. The final survey analysis found that individuals employed online equivocation strategies to help reduce privacy concerns in mobile computing and contributed to

privacy calculus theory, contending that individuals will make a cost-benefit analysis regarding whether to disclose inaccurate personal information to reduce privacy concerns. However, the research shows that the behavior of online equivocation positively effects mobile privacy concerns, implying that the more that individuals online equivocate, the more likely they are to be concerned about privacy. Overall, the study shows that online equivocation is a fairly common strategy, leading to high percentages of inaccurate data collected by businesses. Inaccurate personal information from consumers can misinform companies and lead to incorrect business decisions, affecting the nature of the products or services offered. Firms aiming to compete online depend on the quality of the information they collect from consumers and may view understanding this phenomenon as strategically crucial to competitiveness.

## TABLE OF CONTENTS

ABSTRACT.....	iii
INTRODUCTION.....	x
 CHAPTER 1: DEFINING & CATEGORIZING ONLINE EQUIVOCATION	
Abstract.....	1
Introduction.....	2
Literature Review.....	5
Information Privacy.....	5
Internet-Related Privacy.....	7
Conceptual Foundations.....	12
Online Equivocation.....	12
Mobile Disclosure Context.....	13
Application Category.....	13
Data Elements Collected.....	14
Privacy Policy Characteristics.....	15
Field Study.....	17
Analysis.....	19
Online Equivocation.....	19
Mobile Disclosure Context Definition.....	27
Application Platforms.....	29
Application Selection.....	33

Data Elements.....	36
Privacy Policy Characteristics.....	38
Mobile Disclosure Context.....	41
Conclusion.....	43

## CHAPTER 2: MOBILE ONLINE EQUIVOCATION IN THE UNITED STATES

Abstract.....	44
Introduction.....	45
Literature Review.....	48
Information Privacy Concerns.....	48
Mobile Privacy.....	51
Online Equivocation.....	57
Conceptual Model & Hypotheses.....	64
Mobile Disclosure Context.....	67
Research Framework.....	70
Methodology.....	71
Measures.....	71
Participants.....	77
Procedures.....	82
Results.....	85
Discussion.....	103
Conclusion.....	107

Managerial Insights.....	109
Contribution.....	118
Future Research.....	120
REFERENCES CITED.....	122
APPENDICES	
APPENDIX A: MOBILE PRIVACY CONCERN STUDIES 2007-2017.....	146
APPENDIX B: ONLINE DECEPTION STUDIES.....	148
APPENDIX C: MOBILE PRIVACY CONCERNS PLS-SEM MODEL (REPEATED INDICATORS APPROACH .....	151
APPENDIX D: ONLINE EQUIVOCATION PLS-SEM MODEL (REPEATED INDICATORS APPROACH).....	152
APPENDIX E: IRB SUBMISSION.....	153
APPENDIX F: QUESTIONNAIRE #1.....	159
APPENDIX G: QUESTIONNAIRE #2.....	161
APPENDIX H: SURVEY.....	165

## LIST OF TABLES

Table 1.	Questionnaire One Coding Results.....	19
Table 2.	Continuum Definition of Online Equivocation.....	21
Table 3.	Questionnaire Two Measures.....	23
Table 4.	Subject Responses on Online Equivocation Frequencies.....	23
Table 5.	Demographics for Questionnaire Two.....	25
Table 6.	Mobile Experience Control Variables.....	26
Table 7.	Smartphone User Share by Operating System in the United States 2014 to 2016 by Percentage.....	28
Table 8.	Google Play Application Categories.....	30
Table 9.	Apple iOS Application Categories.....	31
Table 10.	Google Play and Apple iOS Application Category Grouping..	32
Table 11.	Top Ranking Groups & Sensitivity Flag .....	34
Table 12.	Top Five Ranked Applications by Category.....	36
Table 13.	Application Data Type Matrix (correlated from review of Table 10 applications).....	37
Table 14.	Privacy Policy Characteristics Description.....	39
Table 15.	Privacy Policy Continuum by Increasing Risk of Exposure.....	40
Table 16.	Mobile Disclosure Context Scenarios.....	41
Table 17.	Influential Definitions and Measures of Privacy Concerns.....	51
Table 18.	Construct and indicator breakdown.....	72
Table 19.	Survey Items and Sources.....	74

Table 20.	Demographics for Survey.....	80
Table 21.	Mobile Experience Control Variables.....	80
Table 22.	Scenario Descriptions and Respondent Counts.....	83
Table 23.	Outer Weights for Online Equivocation Measures.....	88
Table 24.	Outer Weights for Online Equivocation Measures.....	89
Table 25.	Outer Weights for Mobile Privacy Concern Measures.....	90
Table 26.	Outer Loadings for Mobile Privacy Concerns Measures.....	91
Table 27.	Common Method Bias Measures.....	94
Table 28.	Summary of Path Coefficients and Results. Significant results in bold.....	96
Table 29.	Summary of Online Equivocation Measure Relevance and Significance.....	96
Table 30.	Summary of Mobile Privacy Concerns Measure Relevance and Significance.....	97
Table 31.	Path Coefficients of Mobile Disclosure Context (Scenarios) as Moderators of Mobile Privacy Concerns.....	98
Table 32.	Summary of Hypotheses Tested.....	99
Table 33.	Likelihood to Offer Optional Information.....	100
Table 34.	Subject Responses on Scenario Ranking.....	101

## LIST OF FIGURES

Figure 1. Questionnaire One Results Defining on Online Equivocation..	20
Figure 2. Questionnaire One Detail on Fictitious Information.....	20
Figure 3. Stack Chart of Online Equivocation Frequencies.....	24
Figure 4. Diagram of the Conceptual Model.....	70
Figure 5. Online Equivocation (Formative Model).....	86
Figure 6. Mobile Privacy Concerns (Formative Model).....	87
Figure 7. High Order Unidimensional Model.....	92
Figure 8. High Order Unidimensional Model (Formative Path Coefficients).....	93
Figure 9. High Order Unidimensional Model (Reflective Path Coefficients).....	93
Figure 10. High Order Unidimensional Model (Empirical Study Results)	95
Figure 11. High Order Unidimensional Model with Moderating Effect (Empirical Study Results).....	97
Figure 12. Likelihood to Provide Information.....	100
Figure 13. Stacked Bar Chart Illustration of Ranking.....	101
Figure 14. Social Networking Ranking from Highest to Lowest in Comparison.....	102

## INTRODUCTION

In the last 2 decades, the Internet has ushered in an Information Revolution. The Internet's extensive and growing collection of information and personal information has become the most abundant untapped "natural resource" for business (IBM, 2016). The Information Revolution has heralded an entirely new category of billion-dollar companies that produce no tangible product other than a repository of harvested and repurposed data (Dwoskin, 2013). Through data insights and personalization, firms can drive personal loyalty, innovate products and services, streamline manufacturing and delivery, and create efficiencies previously unseen (Dinev, & Hart, 2003). Harvesting data and knowing how to use it competitively is not only a strategic advantage, but also imperative to firm survival (Brahim, & Martiz, 2015; Greengard, 2015; Morey, Forbath, & Schoop, 2015).

With all new things bright and shiny, there also tend to be some dark spots and one of those is privacy. This refers not to physical privacy where a person goes into another room and shuts the door to be alone, but the type of privacy that is psychological and revolves around the disclosure of personal information. When an individual participates in e-commerce, social networking, and other data-sharing activities online, they actively disclose information about themselves (Dinev, & Hart, 2003). That disclosure creates benefits, but has personal costs, and individuals have come to understand and resent that large quantities of data are collected about them (Smith, Milberg, & Burke, 1996). This phenomenon is amplified by the explosion of digital technologies including connected products such as fitness trackers and home systems in which data collection involves not only the application capabilities but also an individual's whereabouts, behaviors, and

biometric data (Morey et al., 2015). Individuals who engage in activities online worry about the impression their data leave behind. They are concerned that the collection of data creates a mosaic effect used to uniquely identify them (Acquisti, Brandimarte, & Loewenstein, 2015; U.S. Department of Health, Education and Welfare, 1973; Laudon, 1986; Malhotra, Kim, & Agarwal, 2004; Privacy P, 1977).

Fundamentally, personal information has become the new currency used as a basis for exchange online. Every time an individuals disclose personal information about themselves, they make a decision, a “privacy calculation,” evaluating the costs and benefits of that act of disclosure (Culnan, & Armstrong, 1999; Glazer, 1991; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990). Individuals often balance the perceived benefits of self-fulfillment, the need for immediate gratification, and the natural tendency to socialize against their perceived costs (Acquisti, & Grossklags, 2004). In a privacy calculation, individuals will work to maximize benefits and keep personal costs low (Becker, 1981; Vroom, 1964). When individuals feel concerned about their privacy, they look for ways to reduce personal costs, which sometimes results in individuals’ changing the value of the data currency (i.e. exchanging the truth for a falsehood to protect themselves online; Horne, Norber, & Cernal, 2007; Kobsa, 2002; Malheiros, Preibusch, & Sasse, 2013).

Often, the decision to be truthful or untruthful is driven by the context of the disclosure, and that extends online to mobile computing. Specifically, the mobile application type, the data elements collected, and the privacy policy characteristics that influence how information is stored and used can affect individuals’ attitudes about

disclosure (Drouin, Miller, Wehle, & Hernandez, 2016). Individuals expect value in return for sharing, increasingly so when companies are known to share collected information with third parties. The value of personal information increases as the sensitivity and breadth of exposure increases (Morey et al., 2015). When individuals feel that an application asks for too much and costs are too high, then everything proclaimed in *Hamlet* goes for naught. Instead of following “above all, to thine own self to be true and . . . not then be false to any man,” individuals will create a fabrication of the self, wherein shared truths are deceptive (Almeryda, & Shakespeare, 2000).

Motivations for fabricating personal information are not exclusive to privacy concerns. The desire to be liked, to promote a personal agenda, and to support creative expression are all motivations to misrepresent (Van Kleek, Murray-Rust, Guy, Smith, O’Hara, & Shadbolt, 2015). Self-presentation is also a key motivation for individuals to mislead or falsify information. A typical example is an online dating application where participants are motivated to put their “best data forward” to attract others. Several studies have reported that over 80% of online dating application participant profiles contain some personal deception (Dumas, Maxwell-Smith, Davis, Ciulietti, 2017; Hancock, Toma, & Ellison, 2007a). Popular social networking applications often allow individuals to modify their photos to enhance their images (Sass, 2017). Some applications centered on popularity offer individuals the opportunity to purchase “likes,” which can help boost ratings (Dumas et al., 2017; Wang, Duong, & Chen, 2016; Wang, Yan, Lin, & Cui, 2017). Researchers have shown that individuals who are sensation-seekers, have high Internet usage and exhibit positive attitudes toward deception, thus

being more likely to fabricate personal information (Caspi, & Gorsky, 2006; Lu, 2008; Lwin, & Williams, 2003; Steinel, Utz, & Koning, 2010). Online misrepresentation is often a push-pull between the desires to self-present and self-protect (Pak, & Zhou, 2014; Son, & Kim, 2008).

Research also tells us that individuals do not often act rationally when it comes to disclosure. Individuals report high concerns regarding privacy and state that they have low intentions to disclose, but they demonstrate increased disclosure, the opposite of their stated intentions (Acquisti, & Gross, 2006; Acquisti, & Grossklags, 2004; Norberg, Horne, & Horne, 2007). There is a disconnect between the expression of concerns and actual disclosure behavior. The contradiction is a privacy paradox in which individuals' behavior exhibits the reverse of their stated opinions (Acquisti, 2004; Barnes, 2006; Debatin, Lovejoy, Horn, & Hughes, 2009). Some researchers have stated that this behavior occurs because individuals are not fully aware of the potential consequences of their behavior, especially if they have never experienced any negative consequences of personal information disclosure (Felt, Edelman, & Wagner, 2012a; Kelley, 2012; Lin, Amini, Hong, Sadeh, Lindqvist, & Zhang, 2012). Other research studies have pointed to an individuals' desire for immediate gratification, which can influence the adoption of a mobile application and subsequent sharing of personal information to gain prompt benefits (Acquisti, 2004; Felt, Ha, Egelman, Haney, Chin, & Wagner, 2012b; Kelley, & Bertenthal, 2015; Lin et al., 2012). Humans have a natural need to be social, and personal disclosure is central to how they conduct themselves. Personal disclosure online can meet intrinsic needs to make connections and even address the need for recognition (Acquisti

et al., 2015; Frattaroli, 2006; Steinfield, Ellison, & Lampe, 2008; Toma, & Hancock, 2013). The online world provides an extraordinary opportunity to act on natural human instincts (Toma, & Hancock, 2013; Steinfield et al., 2008). Overall, research has shown that people do not always live up to their stated privacy viewpoints (Spiekermann, Grossklags, & Berendt, 2001).

The era of data has arrived, and gathering consumer data will continue to grow as a competitive advantage. This means that the information collected is more important than ever before. Consumer data not only drives marketing programs online, in mobile, and across social media outlets but also have become the basis for integral parts of product composition (Morey et al., 2015). Personalization based on individual information sharing is fundamentally built upon correct input and then customizing the interactive experience based on that information (Adomavicius, & Tuzhilin, 2005; Yang, & Jun, 2002). When the input is wrong, the output is wrong, too (Wirth, & Sweet, 2017). False pretenses can create personal online experiences that miss the mark and leave the individual dissatisfied. Millions of mobile applications are available for individuals, and the competition is fierce (Levenson, 2017). Mobile applications can distinguish themselves not just through design but also through content. The way in which applications can deliver the most relevant experience often depends on personal information (Yang, & Jun 2002). Today's successful businesses rely on quality information to exceed consumer expectations and develop longer-term relationships (Adomavicius, & Tuzhilin, 2005).

Regardless of the desire for personalization, consumers have an avid sense regarding the risks around data security and privacy and do not view the benefits of personalization as outweighing the risks of personal information sharing (Conroy, & Narula, 2014; Morey et al., 2015; Teltzrow, & Kobsa, 2004). Businesses often idealistically state that they are meeting consumer expectations with regard to privacy and tend to overestimate the quality of data they collect (Conroy, & Narula, 2014; Wirth, & Sweet, 2017). When incorrect data are collected it can create disappointing experiences for consumers that over time undermine the believability and reputation of the business (Strong, Lee, & Wang, 1997; Wang, Lee, Pipino, & Strong, 1998; Wang, & Strong, 1996). If a business generates income solely from its collected consumer information, then the inherent value of that data is crucial.

When individuals share personal information with a business, the business generally assumes that the information shared is accurate. This is an idyllic assumption. Either individuals are not concerned about privacy and are at ease sharing their personal details openly and honestly, or they are concerned about privacy but are so motivated to gain the advantages of the application services that they share their personal details despite their beliefs. Alternatively, it could be that individuals share inaccurate personal information that modifies the exchange in favor of the individual. Fundamentally, the individuals gains access to the capabilities of the application but do so by hiding their real data and protecting their privacy.

The question prompts further exploration into the relationship of mobile privacy concerns and the possible replacement of accurate data with inaccurate data. Do

individuals engage in online equivocation to offer personal information at a lower value and balance the exchange of personal information for an application's capabilities? Is there a relationship between online privacy concerns and online equivocation? In other words, do individuals engage in online equivocation to protect their privacy? Are there some mobile application contexts in which individuals are motivated to engage in online equivocation more than others? More broadly, to what extent is the privacy paradox evident; that is, despite expressing privacy concerns, how much are individuals still likely to be truthful in mobile applications?

This study adopts a multi-method approach to examine the effect of online equivocation, the act of avoiding disclosure through the substitution or falsification of personal information, upon individual privacy concerns in mobile computing. First, I used a qualitative questionnaire to examine the various strategies individuals employ to protect their privacy online through equivocation. Second, I used a follow-up quantitative survey to precisely leverage the initial online equivocation categorization and measure individual behaviors regarding equivocation. I then used the resulting categorization to support the third and final survey to examine a new conceptual model to test the effect of online equivocation on mobile privacy concerns.

The expected result is not only a categorization of the various online equivocation strategies exhibited by individuals but also a deeper understanding of the use of online equivocation in mobile computing driven by privacy concerns. As a conclusion, this study offers insights on how firms can respond to the various forms of online equivocation and how firms can offer potential solutions to encourage truthful disclosure.

As an outcome, the dissertation research aims to categorize online equivocation as a continuum of effort and demonstrate that online equivocation is used as a personal strategy to reduce individual costs of disclosure that as a consequence may or may not reduce mobile privacy concerns. This categorization of online equivocation within mobile computing, as well as its potential impact on individual engagement, could provide firms insight regarding individuals' tendency to provide truthful information and the subsequent value of the collected data. The implications for business strategy and the alignment to emerging public policy are discussed within managerial insights.

# **CHAPTER 1**

## **DEFINING AND CATEGORIZING MOBILE ONLINE EQUIVOCATION**

### **Abstract**

The purpose of this study is to discover the various strategies that individuals adopt to misrepresent their personal information online when they are concerned about their privacy. To achieve this goal a qualitative questionnaire was distributed to 547 individuals across the United States asking subjects to report whether they had provided inaccurate data online in privacy-concerned situations and to detail the various strategies used. The results indicate that online equivocation can be categorized into five distinct strategies organized on a continuum of level of effort: omission, abbreviation, substitution, combined substitution, and alternative persona. A second follow-up questionnaire was completed with 582 respondents, which revealed that individuals use one more online equivocation strategy in the majority of personal information sharing. The result provides a framework for further study of online equivocation. In addition, this study conducted a secondary analysis to identify the leading mobile disclosure context variables across application types, data elements collected, and privacy policy characteristics. The resulting mobile disclosure context categorizations are intended for future research on topics related to mobile computing.

## Introduction

Data collection is a natural by-product of the growing computing revolution. In the last 25 years of Internet computing society has moved from an online paradigm focused on the search for information to a wide variety of uses such as e-commerce, banking, and social networking (Keith, Lowry, Babb, & Furner, 2017; Xu, Gupta, Rosson, & Carroll, 2012a). It is hard to imagine work and personal life without a connection to the wide world of the web. Being disconnected from this world is like having the electricity cut off leaving us feeling handicapped and alone. The phenomenon of the Internet and its integration into everyday life has been accelerated with the inception of the smartphone, which ushered in a decade of data connectivity that extends beyond any desktop environment. The present day is a world in which we are connected 24/7 almost wherever we are located, with the world at our fingertips inside our pockets in a computer that is no bigger than a few inches (Lenhart, Purcell, Smith, & Zickuhr, 2010; Nafus, & Tracey, 2002; Oksman, & Rautiainen, 2003).

The power of mobile Internet devices has created other challenges. Knowingly or unknowingly, individuals use mobile applications that collect and track personal data (Almuhimedi, Schaub, Sadeh, Adjerid, Acquisti, Gluck, & Agarwal, 2015; Baarsiaq, Alan, Gomer, Liccardi, Marreiros, & Gerding, 2016; Chellappa, & Sin, 2005; Egelman, Felt, & Wagner, 2013; Greenwald, 2014). Mobile applications collect data for the services they offer and often identify users uniquely, stripping users of anonymity and exposing them to third-party entities unknown. This unparalleled collection of information about our personal selves is often correlated with other applications and

services providers, exposing data for analysis and purchase (Angwin, & Valentino-Devries, 2011; Brahim, & Martiz, 2015; Greengard, 2015; Keith et al., 2017; Smith, Milberg, & Burke, 1996; Thurm, & Kane, 2010; Xu et al., 2012a).

As mobile computing becomes a more pervasive part of our lives, our privacy concerns increase, and subsequently the strategies that individuals employ to protect themselves also accelerate (Beinat, 2001; Shklovski, Mainwaring, Skúladóttir, & Borgthorsson, 2014; Xu, 2007; Xu, Teo, Tan, & Agarwal, 2012b). One of those strategies is to misrepresent our personal information online. When faced with a disclosure context where an individual feels concerned about privacy but still wants to engage some people opt for a control technique to manage the exchange by providing inaccurate information, thereby limiting overall personal exposure (DePaulo, Lindsay, Malone, Muhlenbruck, Charlton, & Cooper, 2003; Earp, & Baumer, 2003; Sheehan, & Hoy, 2000; Tian, & Keep, 2002). When faced with privacy-concerning situations individuals, essentially conduct a privacy calculus, weighing the costs and benefits of the personal disclosure. The result of this privacy calculus may motivate a person to exchange the value of the information offered by replacing accurate information with inaccurate information (Horne, Norberg, & Cemal, 2007).

The goal of this study is to examine the various ways in which individuals can misrepresent their information online and to derive a categorization of online equivocation. To achieve this I conducted a qualitative online survey to help define the categorization of online equivocation, and a follow-on survey to examine the frequency of the categorization and use. The resulting definition of online equivocation is used in a

third study to examine the effect of online equivocation on privacy concerns in mobile computing. The third study is complimented with a secondary analysis evaluating popular types of applications, data elements collected within those applications, and their privacy policy characteristics. The secondary research defines seven mobile disclosure context variables that are used as moderating variables and control measures to ensure that the final study results cover the breadth of popular application scenarios used in the everyday lives of the population.

The remaining parts of the paper are organized with a review of the relevant literature, a presentation of propositions around online equivocation and the mobile disclosure context, and then a description of the study's methodology. Finally, the results of the analysis are offered along with a discussion and conclusion.

## **Literature Review**

The topic of privacy has generated an extensive collection of multidisciplinary studies that includes normative studies focused on ethics, descriptive studies that work to explain, and empirical studies testing theories using scientific methods (Smith, Dinev, & Xu, 2011). This literature review reflects on four themes from these foundations: information privacy, Internet-related privacy concerns, mobile privacy, and the economics of personal disclosure.

### ***Information Privacy***

Personal privacy is not a new source of controversy. Allegations of privacy violations are peppered throughout history and have been the subject of debate for as long as human society been recorded (Ghazinour, Razavi, & Barker, 2014). The first documented complaint about a privacy violation occurred in the 1300s over eavesdropping, and since then, the subject of personal privacy has continued to gain relevancy as society has advanced communication through the inception of print, photography, and today's Internet. What makes online privacy such a compelling topic is the remarkable shift in our behaviors around technology. In the last century, technology has become the great protagonist of personal boundaries. We have moved from being a society concerned about a particular tidbit overheard in a market to one where a private secret may be exposed to large numbers of people in an instant. In the 1300s' broadcasting, a secret was limited to how clearly the tone and depth of a single person's voice could carry a message. Today, the same message could be distributed to hundreds of thousands, perhaps millions, in a matter of seconds. As humans, we find ourselves in a

sort of conundrum, grappling with both our desire for personal privacy and also our desire to access the broad and immediate benefits of technology-empowered communications.

Information privacy is centered on personal information disclosure. Alan Westin (1968), a former professor of public law and government at Columbia University who is widely respected for his work on individual data, privacy, and data protection, said that information privacy is the “claim of individuals, groups, and institutions to determine for themselves when, how and to what extent information about them is commented to others” (p. 7). Westin’s premise creates a challenging requirement for technology providers who depend on data collection for their livelihoods (Davies, 1997). Today, personal online information is considered a rich natural resource and a byproduct that can be traded and marketed, which has elevated it in the law and in commerce. It has moved from the realm of something very personal to an exchangeable currency and, as a result, has become an unwieldy resource to manage (Culnan, & Armstrong, 1999; Dinev, & Hart, 2006; Läufer, & Wolfe, 1977). Although leading technology-based firms fully supported Westin’s definition, the undertaking to deliver this type of control maybe economically unattainable by the latest standards.

When we describe information privacy, it is within the dynamics of personal disclosure. *Disclosure* is the process of an individuals’ sharing information about themselves to other persons and is often measured as the amount of information divulged and the degree of intimacy in sharing (Wheless, & Grotz, 1976). The first is measured by the breadth of the information, and the second is measured in regard to the honesty of

the interaction. Individuals manage their breadth of information disclosure through a boundary regulation process (Altman, 1975; Petronio, 2012; Xu, 2007). This process is less like a spigot that can be turned on and off more of a continuum of regulation that helps people achieve their desired privacy level around information they disclose and receive (Altman, 1975; Shklovski, 2014). Disclosure demonstrates a natural tension between the desire for information and the sharing of it. Disclosure tends to be more flexible, depending upon the context in which information is shared (Altman, 1977; Läufer, & Wolfe, 1977; Xu, Dinev, Smith, & Hart, 2008).

### *Internet-Related Privacy*

The capability to communicate through the Internet adds a new dimension to information privacy and disclosure. With one social networking account an individual can instantly disclose personal and private information to many others with little cost and sometimes little forethought. Every second, thousands of instant messages are broadcast, and millions of emails are sent (Pappas, 2016). With Internet access, individuals share more about themselves than ever before because they post, comment, blog, and share photos and videos including intimate details of their lives with known and unknown people (Granryd, 2016). The past paradigms of managing information privacy have become difficult to maintain. The current world facilitates personal disclosure with the “Submit” button.

The Internet is where consumers hang-out, and companies looking for new market opportunities are certain to follow. The Internet has been and continues to be the new horizon for business growth, in particularly for personalized goods and services (Brahim,

& Martiz 2015; Greengard, 2015). The result of personalization is the collection of personal data. Companies have become adept at collecting huge quantities of information regarding individuals' personalities, backgrounds, and actions, often accumulated in personal profiles that leave many individuals concerned about the trail of data they are leaving behind (Acquisti et al., 2015; H.E.W., 1973; Laudon, 1986; Malhotra et al., 2004; Privacy Protection Study Commission, 1977; Smith et al., 1996). Personal information collection has become the fuel of competitive growth; marketers have an insatiable appetite for consumer data, and there is no sign of the trend's reversing (Dinev, & Hart, 2003; Keith et al., 2017). In fact, the direction of data collection is only multiplying with the use of mobile devices. Over two-thirds of a billion Internet users are accessing the Internet through mobile devices. The expansion of the number of mobile devices and their use has tripled over the last 5 years with no sign of decreasing (Granryd, 2016).

With mobile devices come some unique aspects regarding personal disclosure and information privacy. First, the modality of mobile computing is different from that of desktop computing. Individuals carry their mobile devices all day, viewing them as extensions their personal selves (Ling, 2008; Nafus, & Tracey, 2002). Applications are infinitely personalized and allow for the collection of unprecedented combinations of personal information, from logging health-related information to tracking location (Angwin, & Valentino-Devries, 2011; Boyd, 2008; Keith et al., 2017; Xu et al., 2012b). A significant amount of data is actively or passively disclosed by individuals in real all-the-time (Keith et al., 2017). Concerns about data collection have increased at the same rate that data collection has increased. Individuals perceive that a considerable amount of data

is collected about them and they feel they have lost control over how this information is collected and used by companies (Felt et al., 2012b; Lin et al., 2012; Rainie, & Madden, 2015) The increase in new technical capabilities has offered unique advantages to both consumers and companies; but, this has escalated privacy concerns within society overall (Westin, 2003).

### *Economics of Personal Disclosure*

Despite the growing negative social views regarding online privacy concerns, individuals still engage in active personal disclosure online. There is a distinct discrepancy between their attitudes about disclosure and information privacy and their actual behavior. This discrepancy is described as a *privacy paradox*, which occurs when individuals demonstrate low intention to disclose but show higher levels of disclosure such that their privacy concerns do not reflect their actual behavior (Acquisti, & Gross, 2006; Acquisti, & Grossklags, 2004; Dinev, & Hart, 2006; Norberg et al., 2007). Essentially, individuals report that privacy is important to them, but their online behavior contradicts their stated views (Acquisti et al., 2015; Barnes, 2006; Debatin et al., 2009). Although the privacy paradox is still an active topic of debate among researchers some propose that this is just human behavior and that individuals are social animals who create connections by disclosing personal information (Acquisti et al., 2015). People are sometimes unclear about their preferences and often choose immediate gratification first by downloading an application and sharing their information to receive the immediate benefits (Acquisti et al., 2015; Singer, Mathiowetz, & Couper, 1993; Solvic, 1995).

Perhaps individual disclosure behavior is not a paradox but a matter of making a

choice—a cost-benefit analysis—where individuals are willing to disclose information in exchange for an economic or social benefit (Culnan, & Armstrong, 1999; Glazer, 1991; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990). Data exchange for application benefits is analogous to a nonmonetary exchange; instead of money, personal data are exchanged to receive online benefits. Individuals conduct a privacy calculus looking for a fair deal, weighing the cost of data in return for the benefit of the application, to make a conscious choice regarding their disclosure exchange (Donaldson, & Dunfee, 1994; Milne, & Gordon, 1993).

The assessment of fairness is influenced by the context in which the individual is making the disclosure. The context is defined by the components of the engagement influencing the views of relevance and fairness: the application, the data requested by the application to access the functionality, and the privacy characteristics of the application. Individuals evaluate the dynamics of the exchange within the mobile disclosure context, as well as how comfortable they feel disclosing personal data based on their assessment of the situation (Acquisti et al., 2015; Boyd, 2014; Nissenbaum, 2009; Stutzman, Gross, & Acquisti, 2013; Thibaut, & Kelley, 1959). Individuals rarely interact with information in the abstract because it is embedded in the social context in which the individual is engaged. A context is defined by the activities, relationships, norms, rules, and values individuals hold, and it influences decision-making and behavior (Barkhuus, 2012; Nissenbaum, 2009; Shklovski, 2014). Mobile devices and applications that run on an individual's device contribute to the context circumstances for disclosure, with behavior as a mirror of the individual's personal contextual viewpoint. These circumstances and

individuals' viewpoint on whether they are being treated fairly will influence the cost-benefit analysis made before disclosing (Bansal, & Zahedi, 2008; Culnan, & Armstrong, 1999).

Disclosure within applications creates a market interaction where the exchange of personal information is made in trade for application services (Horne, 2007; Milne, & Gordon, 1993; Sheehan, & Hoy, 2000). The class economy theory states that the ultimate goal of an exchange is to maximize outcome. For an individual, this maximization may control the amount of disclosure at any given time (Granovetter, 1995). Individuals will not want to release their information if they feel it will result in a negative outcome. Economic theory suggests that individuals faced with giving up personal information where they bear most of the costs will look for a way to balance the exchange (Cohen 1985; Malhotra et al., 2004). One of those methods is to change the value of the personal information, essentially to misrepresent the data and to reduce exposure and overall costs to the individual. Individuals may perceive that falsifying information will change the cost-benefit equation in their favor, motivating them to offer inaccurate personal data. Individuals may believe that lying can protect their privacy and balance the deal, changing the perception of fairness (Jiang, Heng, & Choi, 2013; Tian, & Keep, 2002). When individuals can determine the currency of exchange, switching truth for deception, they can balance the economics in their favor. Some individuals may view this strategy as an advantage and subsequently provide false information whenever possible (DePaulo et al., 2003; Earp, & Baumer, 2003).

## **Conceptual Foundations**

### ***Online Equivocation***

The study of deception is not new to the Internet and mobile computing.

Researchers have delved into topics such as lying online to positively self-present, which is common on social network sites; lying is a strategy for dealing with privacy concerns as well as hiding sensitive information to avoid harassment or discrimination (Drouin et al., 2016; Dumas et al., 2017; Pak, & Zhou, 2013; Steinel et al., 2010; Van Kleek et al., 2015). People employ a range of strategies from omission to providing inaccurate information when disclosing online (Caspi, & Gorsky, 2006; Horne et al., 2007; Van Kleek et al., 2015; Lwin, & Williams, 2003; Page, Knijnenburg, & Kobsa, 2013; Pak, & Zhou, 2013; Son, & Kim, 2008). The literature recognizes that deception is a strategy commonly employed by individuals when privacy concerns exist, but there is little information on the various strategies used by individuals to switch accurate for inaccurate personal information. Therein lies the opportunity to further understand this type of exchange, defined in this study as online equivocation. I contend that online equivocation can be categorized by the types of common strategies used to offer inaccurate personal information within disclosure exchange, and these categories can be organized by the level of effort required to apply them. This study uses both qualitative and quantitative methods to examine and define online equivocation.

### ***Mobile Disclosure Context***

Personal information disclosure is never abstract; it is always embedded within a social context (Alge, 2001; Campbell, 1997; Malhotra et al., 2004). When individuals define a framework, they examine the activities, relationships, structures, and rules that govern the setting (Barkhuus, 2012; Nissenbaum, 2009; Norberg et al., 2007; Shklovski et al., 2014). The disclosure context has been shown to play a significant role in individuals' intention to disclose, including their cost and benefit calculation (Bansal et al., 2010). The mobile disclosure context is especially relevant for studies in mobile computing. When examining mobile computing the fundamental aspect of the study is mobile applications. Individuals have multiple applications on mobile devices, each with a purpose—location discovery through maps, providing details about the weather, social networking to connect with friends, and messaging applications to communicate. To examine context within mobile computing it is crucial to examine three components of applications: (a) the category of mobile application with which the individual is engaged (e.g., a social networking application); (b) the type of data elements requested in the exchange of capability for information (e.g., a full name, birth date, gender, preferences, and application usage); and (c) the characteristics of the privacy policy regarding data collection and use. Together these factors comprise the essential attributes of mobile application and thus help in defining mobile disclosure context.

#### ***Application Category***

Mobile devices are setup to run applications that have a singular purpose, offering a key capability such as managing a contact list, providing a music listening

service, or offering details on weather the forecast. Millions of applications are available from application stores (e.g., Apple's App Store, or Google Play Store) from which users download and use daily, averaging 30 different applications per month (Perez, 2017; Statista, 2017). These applications fall within typical categories that are the most used and most popular, such as social networking, shopping, messaging, or entertainment (Rajput, 2017). These applications can be commonly categorized and used as an important variables for studying mobile computing (Gu, Xu, Y.C., Xu, Zhang, & Ling, 2017; Keith et al., 2017; Xu et al., 2012b).

### ***Data Elements Collected***

With mobile applications, individuals have expectations about what type of data should be required to function within the application. If the purpose of the application, its role in providing a benefit to the individual, and the individuals' preconceived ideas regarding the personal information required within the application make sense to them, they are less likely to be concerned about privacy and disclosure personally (Culnan, & Armstrong, 1999). This is especially true if they also feel that they can control the information collected and understand how it is going to be used in the future to make reliable and valid conjectures about their actions (Culnan, & Armstrong, 1999; Culnan, & Bies, 2003; Stone, & Stone, 1990; Smith et al., 1996).

Because applications have different purposes, they often require different data inputs to be efficient. Most applications require some common data for account setup; however, based on the service provided by the application, tracking and usage data may differ. For example, a music listening application may collect the individual's music

listening history to personalize a suggested artist list. A health application focused on aiding sleep may collect statistics on an individual's sleep habits.

Given personal tendencies, not all data are valued in the same manner by each person; some data are considered more sensitive than others (Ackerman, Cranor, & Reagle, 1999; Milne, & Boza, 1999; Patil, & Kobsa, 2005; Phelps, Nowak, & Ferrell, 2000). In particular, data such as geolocation can pinpoint the specifics of an individual's location, increasing a person's privacy concern (Almuhimedi et al., 2015; Angwin, & Valentino-Devries, 2011). A mobile identification number associated with a mobile device can also track all actions that an individual performs within that application or across multiple applications when data are shared. This type of correlation creates a fingerprint of an individual's activities, potentially resulting in increased personal exposure (Zhang, Chen, Xue, & Wei, 2015). Understanding computing context is vital to the study of behavior in mobile computing that includes identifying the variety of data elements collected (Xu et al., 2012b).

### ***Privacy Policy Characteristics***

Privacy policies inform users about how an application provider handles the data collected about the individual (Awad, & Krishnan, 2006; Mai, Menon, & Sarkar, 2010). When e-commerce was first developed for the Internet, privacy policies were structured to reduce uncertainty and increase trust and the likelihood of online purchasing. Some studies have demonstrated that strong privacy policies can positively affect purchase behavior and information disclosure (Hann, Hui, Lee, & Png, 2007; Hui, Teo, & Lee, 2007; Miyazaki, & Fernandez, 2000; Xie, Teo, & Wan, 2006). However, beyond e-

commerce, new business models have emerged where application businesses provide free, highly valued services in exchange for collecting personal data. These types of free applications are particularly popular among mobile device users. Many of these applications can provide just-in-time services like navigation, money management, peer-to-peer transactions, and connection to personal friends and family around the clock. Privacy policies within these applications have mutated from the attitude of garnering trust for consumer purchasing to protecting the application provider's permissions for data collection, use, and rights to monetize user data (Gerlach, Widjaja, & Buxmann, 2015). The privacy policies of application businesses that offer free services have common, distinctive characteristics around data collection, use, and sharing with a focus toward permissiveness. These characteristics can be defined by the type of data collected and how wide the distribution of that collected data will be enacted by the application business once collected. The more data are collected, the more personally identifiable the data are to the individual, the wider the potential distribution of the data, and the higher the risk of personal exposure. To study behavior in mobile computing, it is also relevant to describe and categorize privacy policy characteristics of mobile applications when discerning individuals' attitudes toward disclosure and privacy (Eastin, Brinson, Doorey, & Wilcox, 2016; Keith et al., 2017; Xu et al., 2012a; Xu et al., 2012b).

### **Field Study**

To lay the foundation for defining online equivocation, a field study was conducted, organized into three phases (Stone, 1978). The first phase focused on the categorization of online equivocation through a qualitative questionnaire using real-world respondents answering questions about their data-sharing behavior when online privacy was a concern. The questionnaire was conducted on Amazon Mechanical Turk (MTurk), an online survey service, resulting in 547 responses. The questionnaire asks simple, open-ended questions to subjects to describe the various ways the respondents may omit or falsify information online when concerned about their personal privacy. Subjects were asked if they had ever misrepresented their information online either on their on a mobile device to protect their personal privacy. The open-ended questions included, “Have you ever misrepresented your information online to protect your personal privacy?” and, “Please tell us what types of things you do to your protect your privacy online.” The responses were coded and grouped resulting in a continuum based on the level of effort used to define online equivocation strategies.

The resulting online equivocation strategies were used for a second questionnaire to validate online equivocation strategies and explore the frequency of use. The questionnaire was conducted on Amazon MTurk, resulting in 582 responses. The second questionnaire focused on the extent to which the subjects had exhibited the specific types of online equivocation. The combination of the qualitative data from the first questionnaire and the quantitative data from the follow-on survey supports the

categorization of online equivocation behaviors, which are leveraged in the subsequent study named, Essay Two.

The last phase of this study was to define the mobile disclosure context used the Essay Two final survey. This was accomplished through examination of secondary data sources regarding application type, data elements collected with applications, and privacy policy characteristics of popular mobile applications. To complete this study, data were sourced from App Annie, an online statistics collector and aggregator widely used in the software industry for tracking mobile application downloads and popularity. App Annie offers statistics as well as application type standardization within and across mobile application platforms. To complete the analysis, App Annie statistics were examined over one calendar year (2016) to determine popular application categories as well as applications types within those categories. After the initial analysis was completed, 100 of the top application types defined through the App Annie statistics were used for further examination. From these top applications, data elements requested for personalization and use of the applications were assembled, grouped, and categorized to form a framework for popular application and data usage. The groundwork for applications and data collected was supplemented with a detailed review of the identified applications' privacy policies. The application policies were read, dissected, and categorized into attributes. Taken together this final analysis defined a framework for correlating application type, data collection and use, and privacy policy characteristics to inform the primary mobile disclosure contexts for further study.

## Analysis

### *Online Equivocation*

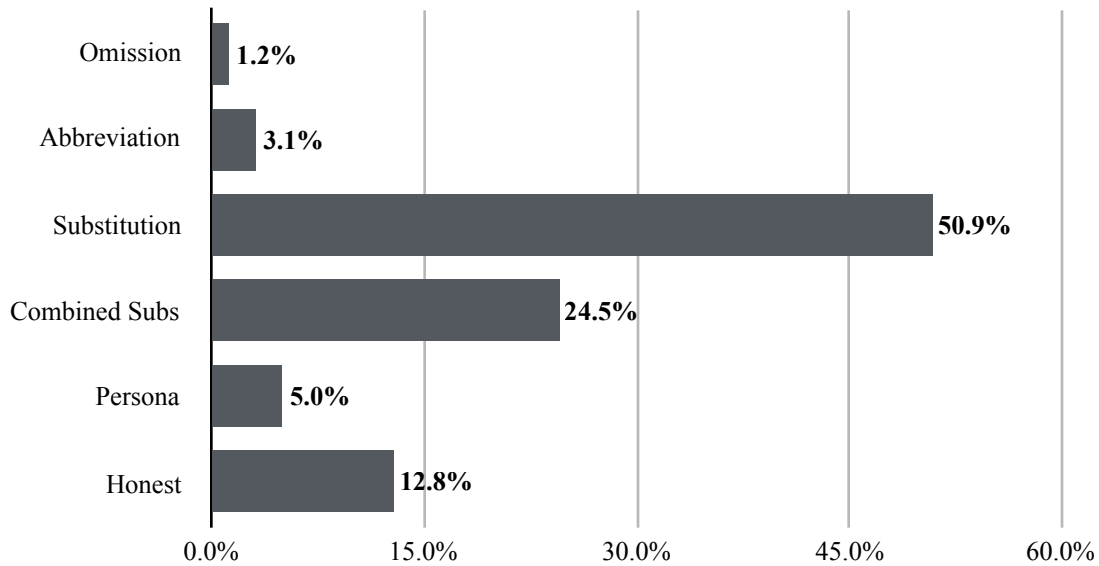
Responses to the open-ended questions about the misrepresentation of online information to protect privacy revealed a wide range of topics and behaviors. After coding the data, five distinct strategies emerged: (a) omission; (b) abbreviation; (c) substitution; (d) combined substitution, and (e) the development of an alternative persona (see Tables 1 and 2). The responses in Questionnaire One were counted for each coded strategy (illustrated in Figure 1). Details of the types of field data (name, address, phone) replaced with fictitious information are outlined in Figure 2.

**Table 1**

*Questionnaire One Coding Results*

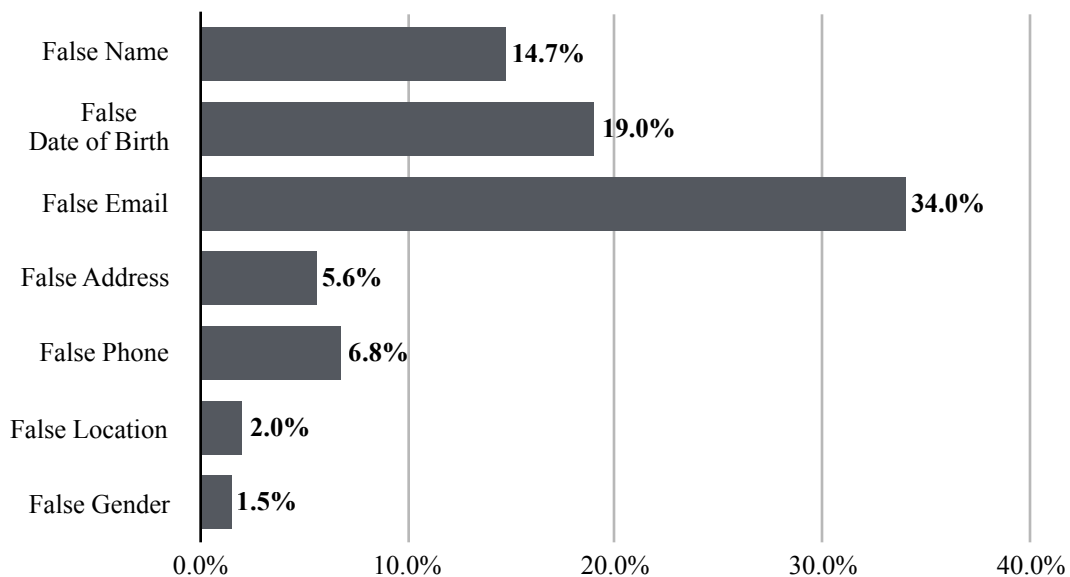
<b>Response Categorizations</b>	<b>Percentage of Responses</b>
Omission	1.2%
Abbreviation	3.1%
Substitution	50.9%
Combined Substitution	24.5%
Persona	5%
Always Honest	12.8%

*Omission* is a strategy used to withhold information. With omission, individuals skip providing data details by leaving blanks or refusing to participate in the functionality of the site, such as refusing to post photos. Omission also includes turning off features such as location awareness, or access to contact lists and photos. Omission is a strategy that is possible only for data that the firm considers optional.



**Figure 1. Questionnaire One Results Defining On Online Equivocation**

*Abbreviation* is a strategy of reducing responses such as supplying abbreviations or only partial segments of the expected information. Examples of these include providing initials, part of a name, or a partial address.



**Figure 2. Questionnaire One Detail on Fictitious Information**

*Substitution* is a method to supply information that may have been truthful at one point but is no longer valid information that is truthful but unused, or just plainly false information. The information is often seen as a substitute for more operable information.

**Table 2.**

*Continuum Definition of Online Equivocation.*

Level of Effort	1	2	3			4	5
	Omission	Abbreviation	Old Data	Unused Data	False Data	Combined Substitution	Alternative Persona
<b>Definition</b>	Providing no value, blank or space.	The use of initials or shortened values in place of full.	Replacement of current value with old, outdated value.	Value that is irrelevant, not checked and ignored.	Value is that is made up, false in place of real value.	A combination of false values used together consistently.	A completely fabricated set of values to represent a fictitious person.
<b>Examples</b>	Skipping if optional, or providing blank space.	Instead of a full name, abbreviated nam. e.g. John Smith is J.S.	Use of an old address, last name, or phone number.	Use of an email that is never checked.	A false name, false email, false phone number.	A combination of false email, false date of birth and false phone number consistently across applications	A false name, contact information and other details to create a false persona.

Examples are using a maiden name, an old personal address, and an active but unchecked email address. Subjects often referenced the use of a substitute email address as a “burner” email that is supplied as personal data but rarely monitored or used. Many subjects stated they had more than one substitute email account, and they rarely or never check those separate accounts. Substitute information such as false names, old physical addresses, and never-checked email addresses are not usable by firms and may affect application functions as well as the customer-focused strategies of business. Substitution is the most popular method of online equivocation.

*Combined substitution* is the action of supplying one or more substituted values that are consistently used in combination, such as a false name and email address together. The most typical application of a combined substitution is a false email plus a false phone number or a false birth date. In some cases, subjects also admitted to combining other false information by posing as the opposite gender.

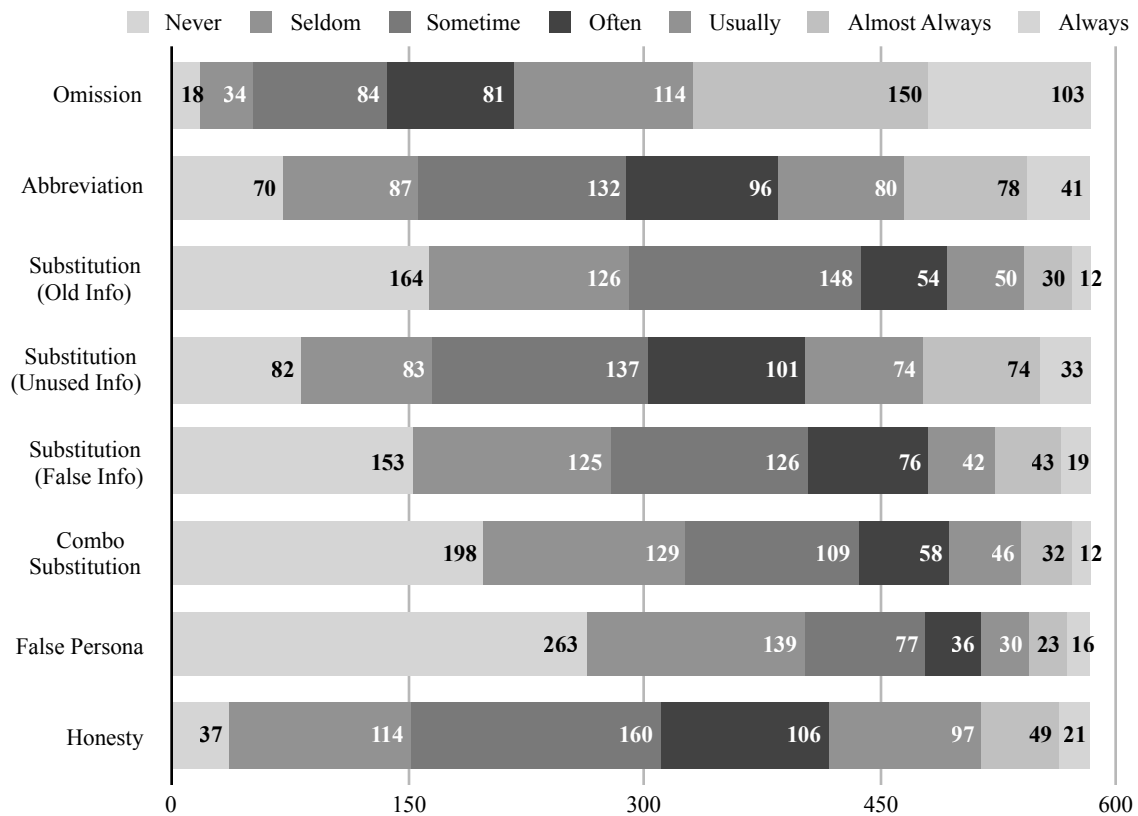
Another strategy, less popular and most difficult to implement, is the creation of an *alternative persona*, a data disguise. An alternative persona is the development of a completely fabricated profile with at least three types of false information. Some individuals stated that they regularly created a full separate persona. In most cases, the alternative persona is used on social networking accounts to hide from others. Questionnaire 2 asked, “When signing up for a mobile application, describe how often you have done the following?” The frequency of online equivocation strategies was measured (see Table 3). Subjects were asked to rate the likelihood of using any of the listed strategies. Likelihood was measured using a frequency interval scale from one to seven (see Table 4 and Figure 3). Responses demonstrated that individuals were more likely to use omission and abbreviation over others. The rate of frequency aligns with the level of effort required for online equivocation and our assumptions about how individuals use them. The data also shows us that there is a great deal of in-between behavior from always honest to always participating in online equivocation. In summary, most people engage in some form of online equivocation depending on the strategy.

**Table 3***Questionnaire Two Measures*

<b>Variable</b>	<b>Item</b>	<b>Measure</b>
<b>Frequency</b>	When signing up for a mobile application, describe how often you have done the following?	Interval scale 1-7: Never (1), Seldom (2), Sometimes (3), Often (4), Usually (5), Almost Always (6), and Always (7)
<b>Omission</b>	Left out or skipped personal information if it was optional.	Concern scale 1-7 as noted above.
<b>Abbreviation</b>	Abbreviated some personal information, such as initials for a name or only given part of an address.	Concern scale 1-7 as noted above.
<b>Substitution (Old Info)</b>	Provided personal information that was accurate in the past, but is not current, such as an old address, old email, or a previous name.	Concern scale 1-7 as noted above.
<b>Substitution (Unused Info)</b>	Provided an email address that you rarely or never check.	Concern scale 1-7 as noted above.
<b>Substitution (False Info)</b>	Provided some fictional personal information, such as a false name, birth date, address, phone number, gender or email address.	Concern scale 1-7 as noted above.
<b>Combo Substitution (False Combination)</b>	Provided more than one form of old or fictional information, such as a combination of an old address and a false birth date.	Concern scale 1-7 as noted above.
<b>False Persona</b>	Completely made up a new false persona.	Concern scale 1-7 as noted above.
<b>Honesty</b>	Fully cooperated with all requests for personal information.	Concern scale 1-7 as noted above.

**Table 4***Subject Responses on Online Equivocation Frequencies*

	<b>Never</b>	<b>Seldom</b>	<b>Sometime</b>	<b>Often</b>	<b>Usually</b>	<b>Almost Always</b>	<b>Always</b>
<b>Omission</b>	18	34	84	81	114	150	103
<b>Abbreviation</b>	70	87	132	96	80	78	41
<b>Substitution (Old Info)</b>	164	126	148	54	50	30	12
<b>Substitution (Unused Info)</b>	82	83	137	101	74	74	33
<b>Substitution (False Info)</b>	153	125	126	76	42	43	19
<b>Combo Substitution (False Combination)</b>	198	129	109	58	46	32	12
<b>False Persona</b>	263	139	77	36	30	23	16
<b>Honesty</b>	37	114	160	106	97	49	21



**Figure 3. Stack Chart of Online Equivocation Frequencies**

In Questionnaire 2, additional demographic information was collected for control purposes (see Table 5). The data had a reasonable distribution for gender and education; however, respondents within the generation y age group composed 68% of the sample, so the responses are oriented more toward this particular age group. Additional factors were collected, such as smartphone experience, total applications owned and application consumption (see Table 6). From these results, we can confirm our definition of online equivocation strategies and derive a sense of the potential impact. Among the subject responses existed a small percentage of individuals who stated that they always were truthful online and never falsified information. Across the online equivocation strategies, over half the responses indicated some use of online equivocation.

**Table 5.**

<i>Demographics for Questionnaire Two</i>		<b>Count</b>	<b>Percentage</b>
<b>Gender</b>	Female	262	45%
	Male	322	55%
	Non Conforming	0	0%
<b>Age*</b>	Gen Z (14-23**)	38	7%
	Gen Y (24-41)	393	68%
	Gen X (42-51)	86	15%
	Baby Boomers (53-72)	65	11%
<b>Education Level</b>	Less than High School	0	0%
	High school or equivalent	68	12%
	Some college but no degree	122	21%
	Associate degree	66	11%
	Bachelor degree	240	41%
	Graduate degree	85	15%

\* Age groupings as defined by WJ Schroder (2017)

\*\* No respondents were under the age of 18 in this study.

Most firms start with the assumption that consumers will be faithfully honest in their responses and may believe that only a small percentage of data may be inaccurate; however, these data show that this assumption is unlikely. Understanding that online equivocation is a phenomenon that affects the quality of collected consumer data is an important insight for business rooted in the acknowledgment that accuracy is not the norm.

**Table 6**

<i>Mobile Experience Control Variables</i>		<b>Count</b>	<b>Percentage</b>
<b>Smart Phone Experience in Years</b>			
	0 - Less than one year, 2018	0	0%
	1 - Since 2017	10	2%
	2 - Since 2016	25	4%
	3 - Since 2015	25	4%
	4 - Since 2014	40	7%
	5 - Since 2013	54	9%
	6 - Since 2012	46	8%
	7 - Since 2011	75	13%
	8 - Since 2010	95	16%
	9 - Since 2009	76	13%
	10 - Since 2008	66	11%
	11 - Since 2007	70	12%
<b>Application Consumption per Month on Average</b>			
	0 app per month	44	8%
	1 app per month	163	28%
	2 app per month	145	25%
	3 app per month	84	14%
	4 app per month	52	9%
	5 app per month	50	9%
	6 app per month	21	4%
	7 app per month	25	4%
<b>Total Applications on Smart Phone</b>			
	0-99	300	52%
	100-199	119	20%
	200-299	77	13%
	300-399	50	9%
	400-499	19	3%
	500-700	19	3%

### *Mobile Disclosure Context Definition*

The second part of this study aims to define a set of scenarios that represent everyday mobile disclosure contexts in mobile computing. I define the mobile disclosure context as a scenario in which an individual discloses personal information through an application on a mobile device. The objective of this inquiry is to define typical and daily application disclosure scenarios of mobile device users. The result would be a set of defined mobile disclosure contexts that could be used in instrument design and data collection for mobile computing studies.

To understand the circumstances in which individuals disclose personal information using their mobile devices, it is important to examine mobile applications. Mobile devices are essentially a collection of applications fit for various purposes such as making a phone call, organizing a contact list, finding a location, or communicating with others through texting. The analysis starts with identifying the types of applications that mobile device owners typically download over 1 calendar year (2016) across widely used mobile operating systems within the United States. Using industry-acknowledged secondary sources concerning application popularity, I narrow application selections to the top 100 applications across the popular mobile operating system platforms. I further examine those applications by inspecting the type of personal data collected by each and the privacy policies of this applications in regard to data collection, data usage, and third-party sharing. The outcome is a compendium of applications, data collection, and privacy policies that help to narrow down the most accepted mobile disclosure context scenarios experienced by mobile device users. The scenarios are intended for survey instrument

development and data collection in Essay Two. Primarily, the scenarios are used as a control to ensure that the survey instrument asks for responses in the most typical personal data-sharing situations that smartphone users experience. Secondly, the scenarios are used to categorize responses and to use those categories to examine each specific scenario as a moderating variable in a future study.

The mobile disclosure context scenario inquiry uses purposive sampling by selecting data based on the characteristics of the population (mobile device users) and the objective of this study. It is a judgmental, selective, and subjective method to define typical mobile computing situations that individuals face and require them to make personal disclosure decisions. I use data sources that describe favored, typical behavior of mobile smartphone users in regard to application popularity detailed in the subsequent sections (Trochim, 2006).

### ***Application Platforms***

Applications for mobile devices are available from two primary platform provider stores: (a) the Apple App Store for iOS; and (b) Google Play for Android (eMarketer, 2016). Blackberry, Windows Phone, and other application stores are minor platforms not holding a significant share of the market so applications on these platforms are not included in the analysis (see Table 7).

**Table 7**

*Smartphone User Share by Operating System in the United States 2014 to 2016 by Percentage Reported by eMarketer, 2016 (Statista, 2017)*

<b>Market Percentage</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>
<b>Google Play</b>	51.3	51.7	52
<b>Apple Application Store</b>	42.3	43.3	43.5
<b>Windows Phone</b>	1.7	1.1	0.8
<b>BlackBerry</b>	3.1	2.8	2.6
<b>Other</b>	1.6	1.1	1.1

### ***Application Category Selection***

The first variables to define are the application categories. There are many categories of mobile applications, but for the initial study, it is practical to limit data collection to 5-10 application categories. To select the application categories, I used several criteria: (a) a high level of category popularity, (b) category presence on both the Apple App Store for iOS and Google Play for Android, and (c) categories that involve information that consumers consider to be of a sensitive nature or have some concern about disclosing.

The first step was to identify the most popular application categories. Google Play and Apple group their many applications into application categories that have standard definitions, but the two application platforms use slightly different naming conventions. To examine popularity data, two industry sources were used: Shared2You and Statista 2017. Statista is a data analysis and statistics reporting aggregation service that uses secondary review by experts, ensuring the highest quality of data used both by practitioners and by academics to derive valuable insights for research and teaching. Shared2You is one of the sources aggregated within the Statista service. The 2016 popularity rankings for Google Play are listed in Table 8, and Table 9 presents the 2016 rankings for Apple (Statista, 2017).

**Table 8**

*Google Play Application Categories as reported by Shared2You (Statista, 2017).*

<b>Google Play Application Categories</b>	<b>Rank 2016</b>	<b>Definition</b>
Tools	1	Virus, Backup, Battery, Security.
Communication	2	Mail apps, messaging apps, video calling.
Video Players & Edit	3	Video playback, editing tools.
Travel & Local	4	Maps, Trails, Boating, Backroads.
Music & Audio	5	Music listening, singing, instrument learning, tuning, DJ tools.
Social	6	Social networking in general.
Productivity	7	Storage (dropbox, one drive), notes, scanners, keyboards, other task managers.
Entertainment	8	Online entertainment applications (streaming), some games.
News & Magazines	9	News and magazine apps, news aggregation applications and subscriptions.
Books & Reference	10	Dictionaries, Reference books, Bibles.
Lifestyle	11	Mix of applications from dating, family, alarm clocks, diary, planning, prayers, and horoscopes.
Personalization	12	Launching applications (app), keyboard tools, Emojis, Icons.
Photo	13	Photo editing, photo capture, photo collections.
Shopping	14	Coupon, grocery lists, deal apps, exchange (sharing economy).
Weather	15	Weather monitoring, radars, water currents and levels.
Business	16	Scanners, PDF readers, Office apps, Accounting apps
Finance	17	Accounting apps, credit checking, stock managers, budgeting, banking apps.
Education	18	Learning apps, brain trainers.
Sports	19	Sports applications to keep track of scores, some learning applications around golf, fishing etc.
Maps & Navigation	20	Navigation, transit, truck, traffic, maps.
Food & Drink	21	Calorie counters, diet apps, meal planning, cookbooks.
Medical	22	Variety of applications for messing conditions (sleep, blood pressure) to reference materials and managing events like pregnancy.
Art & Design	23	Coloring apps, design tools.
House & Home	24	Home security, Lighting, gardening, thermostat apps.
Comics	25	Cartoons and comics, drawing apps.
Libraries & Demo	26	Library apps, demo applications for specific products.
Dating	28	Dating apps.
Auto & Vehicles	29	Driving license study apps, auto reference, car maintenance apps.
Transportation	30	Ride apps, transit apps.
Family	31	Family connection apps, children's apps.
Parenting	32	Child applications (baby and kid management), family connection apps.
Events	33	One time applications related to events.
Android Wear	n/a	General all purpose category.
Beauty	n/a	Selfie tools, color palette apps, nail designs.
Health & Fitness	n/a	Diet apps, calorie counters, workout, meditation, health tracking.
Live Wallpaper	n/a	Backgrounds for mobile devices.

**Table 9**

*Apple iOS Application Categories as reported by Shared2You (Statista, 2017).*

<b>Apple Application Categories</b>	<b>iOS Rank 2016</b>	<b>Definition</b>
Photo & Video	1	Rich content sharing upload, watch, follow. Photo/video capture and editing.
Social Networking	2	Video phone, messaging apps.
Music	3	Music listening, singing, instrument learning, tuning, DJ tools.
Games	4	All sorts of games.
Entertainment	5	Video streaming Netflix, Hulu.
Lifestyle	6	Dating apps, chat rooms, coaching.
Productivity	7	Storage, mail, office tools, calendars.
News	8	Singular news outlets (NY Times, Wall Street Journal) and news aggregators.
Shopping	9	Sharing economy apps.
Reference	10	Bible, Dictionary, singular reference sources such as Bird guides, Sky guides.
Travel	11	Air and land trackers, navigation, travel apps, maps and some transit.
Education	12	Educational apps, brain trainers.
Business	13	Scanners, PDF readers, Office apps, Accounting apps.
Health & Fitness	14	Diet apps, calorie counters, workout, meditation, health tracking.
Books	15	Books, Bibles, Chat Stories.
Navigation	16	Transit apps, navigation, maps.
Finance	17	Budget, Credit scores, Bills manager, Personal Accounting
Food and Drink	18	Calorie counters, diet apps, meal planning, cookbooks.
Weather	19	Weather channels, weather affected sports applications (fishing, surfing), radar apps.
Sports	20	Sports news channels MLB, NBA etc. Sports news aggregators.
Medical	21	Variety of applications for messing conditions (sleep, blood pressure) to reference materials and managing events like pregnancy.
Catalogs	23	Ringtones etc, Add ons, Selfie apps, Collector apps.
Kids	n/a	Children's apps, games, learning.
Magazines & Newspapers	n/a	News and magazine apps, news aggregation applications and subscriptions.
Utilities	n/a	Virus, speed, calculators, payment apps.

The second step was to limit the categories to those that are popular on both Google Play and the Apple App Store. I cross-compared the ranking lists and grouped similar categories. Next, I created a list of the application categories that appear in the top twenty of both Google Play and the Apple App Store in 2016 (see Table 10).

**Table 10***Google Play and Apple iOS Application Category Grouping*

Google Play Application Categories	Rank 2016	Apple Application iOS Categories	Rank 2016
Photo	13	Photo & Video	1
Social	6	Social Networking	2
Music & Audio	5	Music	3
Entertainment	8	Entertainment (+ Games #4)	5
Lifestyle	11	Lifestyle	6
Productivity	7	Productivity	7
Shopping	14	Shopping	9
Travel & Local	4	Travel	11
Education	18	Education	12
Business	16	Business	13
Health & Fitness	n/a	Health & Fitness	14
Books & Reference	10	Books (+ Reference #10)	15
Maps & Navigation	20	Navigation	16
Finance	17	Finance	17
Food & Drink	21	Food and Drink	18
Weather	15	Weather	19
Sports	19	Sports	20
Medical	22	Medical	21
Libraries & Demo	26	Catalogs	23
Tools	1	Utilities	n/a
News & Magazines	9	Magazines & Newspapers (+ News #8)	n/a
Family	31	Kids	n/a
Communication	2		
Video Players & Edit	3	See Photo & Video above	
Personalization	12		
Art & Design	23		
House & Home	24		
Comics	25		
Dating	28		
Auto & Vehicles	29		
Transportation	30		
Parenting	32		
Events	33		
Android Wear	n/a		
Beauty	n/a		
Live Wallpaper	n/a		

The third and last step was to narrow the application category selection to those oriented to collecting personal information as part of their function in contrast to application categories that are more about the distribution of general knowledge. Since individuals

are more likely to feel sensitive to disclosure in applications that require their personal information to be collected. Personal information involving health, finance, location data, personal photos, videos, and social communications have been established as especially sensitive (Liccardi, Pato, & Weitzner, 2014; Olmstead, 2014). Application categories that have a loosely defined mix of applications, such as games, which includes entertainment-viewing applications, and lifestyle, which has a broad definition with an inconsistent mix of applications, were eliminated from the selection. Also removed from the selection were shopping applications focused on e-commerce with defined limits on data collection regarding payment.

Last, both family and children application categories were removed because the analysis is concentrates on adult behaviors. The information sensitivity of the application categories was incorporated into the list of the most popular application categories, as shown in Table 11. This inclusion led to the identification of the seven most relevant categories for further analysis. Our attention will be on the applications that fall into the following seven categories: (a) photo & video, (b) social networking, (c) music, (d) productivity, (e) travel/transportation, (f) health & fitness, and (g) finance.

### ***Application Selection***

After selecting the application categories, the next step in the analysis was to determine which applications to analyze within each of the seven categories. The three main selection criteria for the selection of applications were: (a) applications within each category ranked highest with wide usage; (b) applications that appeared in both platforms to avoid bias toward one platform over another, and (c) applications that are free to

**Table 11***Top Ranking Groups & Sensitivity Flag**Sensitivity in categories likely to require personal data collected to function with categories elected (E)**(Adapted from Liccardi et al., 2014; Olmstead, 2014)*

Google Play Application Categories	Rank 2016	Apple Application iOS Categories	Rank 2016	Sensitive (y/n)	E
Photo	13	Photo & Video	1	y	★
Social	6	Social Networking	2	y	★
Music & Audio	5	Music	3	y	★
Entertainment	8	Entertainment (+ Games #4)	5	n(1)	
Lifestyle	11	Lifestyle	6	n(2)	
Productivity	7	Productivity	7	y	★
Shopping	14	Shopping	9	n(3)	
Travel & Local	4	Travel	11	y	★
Education	18	Education	12	n	
Business	16	Business	13	n	
Health & Fitness	n/a	Health & Fitness	14	y	★
Books & Reference	10	Books (+ Reference #10)	15	n	
Maps & Navigation	20	Navigation	16	n	
Finance	17	Finance	17	y	★
Food & Drink	21	Food and Drink	18	n	
Weather	15	Weather	19	n	
Sports	19	Sports	20	n	
Medical	22	Medical	21	n	
Libraries & Demo	26	Catalogs	23	n	
News & Magazines	9	Magazines & Newspapers (+ News #8)	n/a	n	
Family	31	Kids	n/a	n(4)	
Video Players & Edit	3	See Photo & Video above		y	

(1) Eliminated as sensitive because this category is mixed with a wide variety of streaming applications (watching).

(2) Eliminated as sensitive because these Lifestyle categories on both platforms vary widely in mix of applications and are loosely defined.

(3) Eliminated as sensitive because shopping applications require seller and buyer purchase details, and reviews, but less likely to collect a wider variety of personal content as a main function of the application.

(4) Eliminated as sensitive for this study which excludes examining children's issues.

download without purchase. To narrow the application list to those highly ranked and widely used across platforms, I examined each category ranking of applications within the same calendar year and in the United States across both platforms using a statistics service called App Annie. App Annie (2017) is a universally respected application statistics service used by 94 of the top 100 application publishers worldwide and considered the primary source for cross-platform statistics and analysis.

Application selection represents the most often favored application choice across all smartphone users in the United States over the calendar year of 2016. Of the set of popular applications, only free applications are included because free applications are more frequently downloaded and on average collect more sensitive data than paid apps. This is most likely because many free applications require personal information to personalize advertising and support application developers using advertising business models that leverage the sale of collected data versus the sale of application downloads (Liccardi, 2014).

The only other adjustment made was in the financial application category. Banking applications used by individuals with pre-existing accounts are excluded because they do not qualify for the study condition of first account setup. Mobile banking applications require the individual to have an account set up by the bank with an established username and password. After applying the outlined criteria for application selection, a list of popular applications downloaded by smartphone users in the United States emerged (see Table 12).

## Data Elements

After the applications were selected, each application was downloaded and analyzed according to the type of data requested for use and required at the time of sign-up. I compiled a matrix of data types to determine the data collection themes among the

**Table 12**

*Top Five Ranked Applications by Category; annual year 2016, United States. Reported from Application (Annie Store Stats, 2017).*

Category	App	Description
<b>Photo &amp; Video</b>	<a href="http://musical.ly">musical.ly</a>	Music listening and sing-a-long
	Snapchat	Photo messages
	Instagram	Photo messages
	YouTube	Video sharing
	GooglePhotos	Photo sharing
<b>Social</b>	Facebook	Social networking with friends
	Facebook Messenger	Messaging Facebook friends
	WhatsApp Messenger	Messaging application
	Pinterest	Social lists and sharing
	Twitter	Message broadcasting
<b>Music</b>	Pandora Music	Music listening
	iHeart Radio	Music listening
	SoundCloud	Music listening
	Spotify Music	Music listening
	Sing! Karaoke	Music listening and sing-a-long
<b>Productivity</b>	DropBox	File storage and sharing
	Microsoft Outlook	Email software
	Google Docs	File storage and sharing
	Google Drive	File storage and sharing
	Gmail	Email software
<b>Travel/Transportation</b>	Airbnb	Sharing economy of places
	Uber	Sharing economy of cars
	Lyft	Sharing economy of cars
	TripAdvisor	Travel booking & sharing
	Waze	Way finding
<b>Health &amp; Fitness</b>	MyFitness	Diet and fitness tracker
	Fitbit	Fitness tracker
	LoseIt	Diet and fitness tracker
	Google Fit	Fitness tracker
	Running	Fitness tracker
<b>Finance</b>	PayPal	Payments
	Credit Karma	Personal credit management
	Venmo	Peer-to-peer payments
	Mint	Personal budgeting
	Square cash	Peer-to-peer payments

applications and define the typical data requested for that category of application. Most applications within and across categories had very similar strategies for collecting data.

**Table 13**

*Application Data Type Matrix (correlated from review of Table 10 applications)*

Category	Data types	Description
<b>Common data types across categories</b>	Full name	Application asks for full name including both first and last name.
	Email	Application asks for email address.
	Phone Number	Application asks for phone number.
	Billing Address	Application requires full address for payments (purchases available)
	Birth Year	Application requires to understand age.
	Gender	Application asks for gender (required).
	Personal Photos	Application includes the ability to add personal photos to profile and sharing account.
	User Activity	Any tracking on user activities such as listening to music, communications (messages, chats, emails between accounts), health tracking (workout statistics, health monitoring), payment details, money transfer actions/details.
	Community Postings	Postings that are made publicly the application and intended for wider distribution.
	Personal Contacts / Friends	Access to your friends list or personal contact information stored on your device.
	Social Media Accounts	In addition to a federated login, or in place of access to other social media accounts.
	Device Details	Collection of device specifics such as unique identification, phone number, carrier type, operating system etc.
	Location Tracking	General calculated location as well as specific GPS location.
Technical Tracking	Ability to track activities on the Internet such as sites visited by the device browser etc.	
<b>Distinctions</b>	Health Information	Details about health, statistics such as weight, height, medical conditions. This is above and beyond health monitoring and tracking user activities.
	Financial Information	Account information that allows the application to link to bank accounts or other resources combined together. This is above and beyond the financial transaction records created by user activities.

For example, applications commonly collected the name, email, phone number, address, birth year, and gender. Other common requests were for personal photos, access to contacts or friends, location, and, in some cases, other applications such as social media accounts. In addition, applications track and collect user activities, community postings, and device details. The noted exceptions were health and fitness and finance applications, which asked for very specific types of data related to their services. The matrix of data types across application categories is presented in Table 13.

### ***Privacy Policy Characteristics***

In addition to examining the application categories and data types requested, it is critical to include the privacy policy conditions of the applications. Most privacy policies outline four aspects regarding data collection concerning: (a) what data are collected; (b) how these data are used by the application developer; (c) third-party sharing of collected data; and (d) when third-party data are acquired by the application publisher to combine with other data collected for expanding personal profiles.

Data collection policies of companies also can be categorized into the types of data they collect. These fall into six groupings: (a) aggregated statistics, (b) registration and contact information, (c) user activities, (d) device information, (e) location information, and (f) technical tracking. In addition, some application developers purchase data from third parties to combined with the data they collect on their user accounts to build a stronger profile of the account holder. These policy characteristics are defined in Table 14. Given the general structure of privacy policies, it is relatively straightforward to

**Table 14***Privacy Policy Characteristics Description*

<b>Policy Sharing Characteristic</b>	<b>Description</b>
Aggregated Statistics	Generalized statistics collected about user activities on apps, usually anonymized, referred to as Big Data.
Registration & Contact Information	Registration and contact information are data items that compose your account and general identification such as name, email, contact phone number and billing address
User Activities	User tracking information is data collection related to individuals activities on the application which may include what individuals view and listen to, whom individuals correspond and what they may say.
Device Information	Device information are details that identify the unique device such as it's device identification number, type, operating system, browser types, Internet Protocol address, phone carrier, phone number and related information.
Location Information	Location information is composed of your zip or postal code, approximated location such as your GPS location.
Technical Tracking	This includes technical tracking related to the use of application, Internet Service provider, computer addresses, files downloaded, and other similar statistics.
Outside Third Party Data	As noted, application businesses outline in their policies if they share collected data with third parties. They also outline if they are receiving any third party data about individuals to combine that into a method of understanding the individuals profile. Most application businesses also aggregate data collection to derive reports and analytics as well.

deconstruct the applications' privacy policies into these characteristic groupings and to organize them into a continuum of increasing risk of exposure. I have outlined the privacy policy continuum in Table 15.

**Table 15***Privacy Policy Continuum by Increasing Risk of Exposure*

<b>Policy Sharing Characteristic</b>	<b>Shared with Application business, Third Parties</b>	<b>Risk of Increasing Exposure</b>	<b>Description</b>
<b>Aggregated Statistics</b>	Application business Only	1	Anonymized statistics, no personal connection to account holder, near zero risk of exposure.
<b>Aggregated Statistics</b>	Application business & Third Parties	2	Anonymized statistics shared externally with their parties, low risk of exposure.
<b>Registration &amp; Contact Information</b>	Application business Only	3	Registration information within aPp.
<b>Technical Tracking</b>	Application business Only	4	Technical tracking information collected by application business to assist in functions.
<b>User Activities</b>	Application business Only	5	User activities only used within aPp.
<b>Device Information</b>	Application business Only	6	Device information collected by application business to assist in functions.
<b>Location Information</b>	Application business Only	7	Location information collected by application business to assist in functions.
<b>Outside Third Party Data</b>	Application business Only	8	Application business seeks outside information to assist account holder, possible correlation to credit systems, fraud, payment processing.
<b>Registration &amp; Contact Information</b>	Application business & Third Parties	9	Shared with third parties increasing exposure for contact details. e.g. selling names for mailing lists.
<b>Technical Tracking</b>	Application business & Third Parties	10	Collection of technical tracking information to correlate activity use of this account to other web (browsers) sites visited, or sites with widgets that can make those connections, or applications that can cross correlate.
<b>User Activities</b>	Application business & Third Parties	11	Collection of user activities which are shared with third parties (e.g. sharing user music listening preferences with Facebook)
<b>Device Information</b>	Application business & Third Parties	12	Collection of user device information for cross correlation with third parties (e.g. device unique id correlated payment activities across merchants).
<b>Location Information</b>	Application business & Third Parties	13	Collection of location information for cross correlation with third parties (e.g. location based advertising).
<b>Outside Third Party Data</b>	Application business & Third Parties	14	Use of third party data by the application business to build a personal profile of the account holder (e.g., Facebook account, friends correlated to the music listening account).

### *Mobile Disclosure Context*

I combined the results of the examination of popular application types, data collection, and privacy policy characteristics to identify the top seven mobile disclosure contexts: photo and video sharing, social networking, music listening, productivity, travel/transportation, health and fitness, and financial management (see Table 16). The seven scenarios represent the typical uses for mobile devices and the most often

**Table 16**

*Mobile Disclosure Context Scenarios*

<b>Mobile Disclosure Context Scenario</b>	<b>Application Category</b>	<b>Data Types</b>	<b>Privacy Policy Risk Level (typical for this scenario)</b>
Photo viewing & sharing	Photo & Video	Common data types across categories.	14
Social networking with friends	Social	Common data types across categories.	14
Music listening & sharing	Music	Common data types across categories.	13
Office tools include email, file sharing and calendar	Productivity	Common data types across categories.	8
Transportation through car service	Travel/ Transportation	Common data types across categories.	14
Fitness tracking that include diet and exercise	Health & Fitness	Common data types across categories, including health information.	13
Financial application that accesses bank accounts and allows for transactions	Finance	Common data types across categories, including financial information.	8

experienced application situations. For these applications, the data types collected also represent the most universal personal information collected, with the exceptions of health and finance, where additional data are often used. Also, most of these applications have

similar privacy policy characteristics such as collecting and sharing data with third parties routinely, as it reflecting the privacy orientation of the majority of these types of applications and what individuals experience in regard to personal information sharing.

## **Conclusion**

This objective of the study was to define and understand online equivocation behaviors at a more detailed level, using the words of consumers as they described their own behavior. The study results support a categorization of online equivocation behaviors that reflect the common strategies employed by individuals today.

The study also contributes by defining mobile disclosure contexts through a thorough examination of the various applications, data elements collected, and privacy policy characteristics of popularly applications. The process to define the proposed seven typical mobile disclosure context scenarios could provide future researchers with a framework to develop a set of scenarios relevant for mobile computing studies.

**CHAPTER 2**  
**MOBILE ONLINE EQUIVOCATION**  
**IN THE UNITED STATES**

**Abstract**

The purpose of this proposed study is to examine online equivocation and privacy concerns in the mobile computing environment. This study builds upon the conceptual foundations of online equivocation and mobile disclosure context defined in Essay One. An online survey using a scenario-based approach tested a new conceptual model constructed from the results of previous questionnaires to examine the effects of online equivocation on privacy concerns, collecting 2,947 responses. The results demonstrate that individuals deploy online equivocation strategies to reduce privacy concerns in mobile computing and contribute to the privacy calculus theory, further indicating that individuals will make a trade-off regarding the accuracy of personal information disclosure to reduce privacy concerns. This study also provides insight into the types of online equivocation strategies used in mobile computing. Understanding the extent of online equivocation and its effects on privacy concerns also provides useful insights for managers who rely on the accuracy of personal data collected from consumers through mobile applications.

## Introduction

It is getting loud out there when it comes to the topic of privacy, which is intensified by the fact that the populace continues to express concern over their privacy within the online context. With data serving as the new currency, individuals are walking around with their most valuable resource in their pocket—their mobile device—a money-making data machine. Most individuals spend their personal data currency as fast as they can make it and, in the process, sacrifice their privacy. The cost to the individual is rarely realized at the moment of the impulsive disclosure, yet they still voice their privacy concerns. Online disclosure and privacy concerns almost feed on themselves; the more online activity occurs, the more concerned the population becomes (Boyd, 2008; Felt et al., 2012a; Lin et al., 2012; Rainie, 2015; Shin, 2010; Yahoo, 2011).

Privacy concerns have become a central construct proxy for privacy concerns in much of information systems research (Malhotra, 2004; Smith et al., 2011; Stewart, & Segars, 2002). Around the concept of privacy concerns and personal disclosure online, many studies have examined the effects of negative privacy experiences (Smith et al., 1996), data collection awareness (Malhotra et al., 2004; Phelps et al., 2000), personality differences (Bansal et al., 2010; Dinev, & Hart, 2006; Liu, Marchewka, & Ku, 2004; Xu, 2007), demographic differences, and variations of behavior between cultures (Chen, & Rea, 2004; Culnan, & Armstrong, 1999; Sheehan, & Hoy, 2000). Social scientists have developed theories to address why individuals share their personal details despite their concerns as described in the phenomenon, called the privacy paradox (Acquisti, & Grossklags 2005; Läufer, & Wolfe, 1977; Norberg et al., 2007; Posner, 1981; Stone, &

Stone, 1990). Other studies have asserted that individuals conduct a privacy calculus to make a cost-benefit-based decision whether to disclose or not to disclose (Campbell, & Carlson, 2002; Davies, 1997). The privacy calculus theory asserts that individuals make a calculation when faced with revealing personal data, weighing costs and benefits, influenced by trust and perceived risks, to determine how much they are willing to disclose online. In addition to these studies, researchers have examined the impact of regulation (Milberg, Smith, & Burke, 2000), privacy policies, and trust seals as well as the nuances of context where privacy concerns can vary across electronic commerce, social networking, communication (messaging and email), financial management, and healthcare in both the desktop and mobile computing environments; researchers have also examined the resulting influence on online behavior (Altman, 1975; Dinev, & Hart, 2006; Läufer, & Wolfe, 1977; Malhotra et al., 2004, Margulis, 1977, 2003; Milne, & Gordon, 1993; Phelps et al., 2000; Solove, 2008; Westin 1967, 2001, 2003; Xu et al., 2008).

With the advent of the smartphone in 2007, several studies have emerged on the specific aspects of mobile computing and privacy, ranging from application selection and privacy awareness (Eastin et al., 2016; Felt et al., 2012b; Gu et al., 2017; Shklovski, et al. 2014; Zhang, Ying, Aafer, Qiu, & Du, 2016), to the role of personalization and disclosure in mobile applications to the effects of location-based technologies that allow the unique tracking of users' locations within feet (Fodor, & Brem, 2015; Sun, Wang, Shen, & Zhang, 2015; Xu et al., 2012; Zhao et al., 2012).

Other work has examined privacy concerns regarding online equivocation (lying or deception online). Themes center on the different mobile disclosure contexts outlining

when and how an individual is motivated to lie. Individuals misrepresent information for a variety of reasons with two key motivators: self-presentation (the desire to create a positive impression) and privacy concerns (Drouin et al., 2016; Hancock, Curry, Goorha, & Woodworth, 2007b; Hancock, Toma, & Ellison, 2007; Horne et al., 2007; Koenený, 2009; Lu, 2008; Page et al., 2013; Van Kleek et al., 2015). Multiple studies have shown that when users face privacy concerns, they are more likely to omit the truth or fabricate information (Horne et al., 2007; Page et al., 2013; Pak, & Zhou, 2013; Son, & Kim, 2008; Van Kleek et al., 2015).

The focus of this study is to build on the foundations that privacy researchers have previously achieved building on successful measures of antecedents of privacy concerns and extending those measures to address the unique aspects of mobile computing. Furthermore, it extends a conceptual model to include a more categorized view of the phenomenon of online equivocation in personal disclosure. Specifically, this study focuses on when individuals choose to hide or falsify information to protect their privacy. To achieve this, the study will build on previous privacy concern measures by Smith et al. (1996), Malhotra et al. (2004), and Xu et al. (2012a), adding new variables to address the mobile disclosure context. Also, to address the categorization of online equivocation, this study will leverage the measures previously developed in the analysis completed in Essay One. This study is organized as follows. A discussion of the relevant literature is followed by a description of the conceptual model and hypotheses, the methodology for the study, a review of the data collected and results, discussion of the findings, conclusion, managerial insights and recommendations for future research.

## Literature Review

### *Information Privacy Concerns*

Privacy, as previously described, can be difficult to define, with many different points of view. For academics, information privacy concerns act as a proxy for the concept of information privacy within research. Smith et al. (1996) defined *Concerns for Information Privacy* (CFIP) as an instrument to measure privacy concerns both offline and online. Smith et al. (1996) described privacy concerns with four dimensions: collection, unauthorized use, errors, and improper access.

*Collection* is defined as the amount and type of information gathered about individuals. Collection is a concern that is accentuated by the perception that significant quantities of information are collected about individuals' personal habits, background, and actions (Acquisti et al., 2015; Smith et al., 1996).

*Unauthorized use* refers to the repurposing of information collected for a different purpose. Specifically, individuals are concerned that information gathered may be used outside of its original intent and about how that information is transferred without their approval (Milne, 2000). In general, this reflects the fact individuals feel they lack control over the data collected and its subsequent use by third parties (Nowak, & Phelps, 1992; Sheehan, & Hoy, 2000).

*Errors* involve personal information that is recorded incorrectly. These errors are difficult to notice and change. Many online situations are a “once and done” scenario; data are entered once, never to be updated. Many people express concerns that organizations do not provide enough capability to allow them to minimize problems in

their personal entries. After it is “out there” it becomes a part of the growing digital footprint with little or no ability to be corrected (H.E.W., 1973; P.P.S.C., 1977; Smith, 1994). With little legislation to protect individuals, data errors are like bad credit scores that are never corrected.

*Improper access* refers to individual concerns over information collected for one purpose but used for a secondary purpose without a clear understanding of the secondary purpose acknowledged by the individual. This feeds into an individual’s sense of uncertainty regarding the protection of the information that has been collected about them and their perception that the information is not being managed correctly (Chellappa, & Sin 2005; Smith et al., 1996; Stewart, & Segars, 2002).

Privacy concerns are accentuated by continued media attention on identity theft, credit card fraud, and unauthorized access to their personal records. It is a common for an individual to get a letter in the mail regarding a firm's recent data breach and personal data exposure. These events lead individuals to worry about the loss of their information for inappropriate and unknown purposes (Dwyer, 2007; Saunders, & Zucker, 1999).

Malhotra et al. (2004) built upon Smith et al.’s (1996) CFIP measures to more deeply understand the nature of individual privacy concerns online regarding e-commerce. Malhotra et al. (2004) developed the *Internet Users Information Privacy Concerns* (IUIPC). The central theme of IUIPC is that information exchange is based on a social contract. Malhotra et al. (2004) used social contract theory to understand the phenomenon of individual-firm relationships to help explain individual behavior regarding their privacy concerns (Dunfee, Smith, & Ross, 1999). Malhotra et al. (2004)

felt that we cannot understand privacy concerns without looking at how individuals define the fairness of information exchange.

IUIPC has three major dimensions: collection, control, and awareness. A collection reflects of Smith et al.'s (1996) definition. However, Malhotra et al. (2004) elaborated on that definition by asserting that information collection is only fair when the individual is granted control over it. Control is rooted in procedural justice (Gilliland, 1993; Thibaut, & Walker, 1975; Tyler, 1994), which contends that procedures are fair when individuals have control over processes.

Control is one of the principal foundations of information exchange and essential when there is a perceived high risk of disclosure (Malhotra et al., 2004). Individuals have control when they can determine how their information is used, either by their approval, modification, or the ability to exit the relationship (Caudill, & Murphy, 2000). As a self-management method individuals desire to control disclosure online because it is fundamental to their subjective view of privacy management (Altman, 1977). With control, privacy concerns are reduced, and without it individuals feel invaded (Sheehan, & Hoy, 2000; Xu, Teo, Tan, & Agarwal, 2009). Control is critical to privacy protection (Westin, 1968).

Awareness centers on the transparency of how information is used. *Awareness* is defined by the extent to which individuals understand how their data are used by the application and organization (Culnan, 1993; Foxman, & Kilcoyne, 1993). Kilcoyne (1993) argued that information privacy only exists when people are aware of sound collection practices and are given control over their personal information.

### *Mobile Privacy*

Both Smith et al.'s (1996) and Malhotra et al.'s (2004) instruments were developed before the mobile Internet transformation. For a summary of the instruments, (see Table 17). Although consumer mobile devices existed from 1996, it was not until January 2007, when Steve Jobs announced the arrival of the mobile smartphone, that the emergence of applications using the mobile Internet accelerated. Jobs (2007) was distinct in his definition of his smartphone when he defined the iPhone as a phone, an Internet

**Table 17**

*Influential Definitions and Measures of Privacy Concerns  
(Adapted from Smith et al., 1996; Malhotra et al., 2004; and Xu et al., 2012)*

<b>Measures</b>	<b>CFIP</b>	<b>IUIPC</b>	<b>MUIPC</b>
<b>Name</b>	Concerns for Information Privacy	Internet Users Information Privacy Concerns	Mobile Users Information Privacy Concerns
<b>Purpose</b>	To examine individual concerns about organizations information privacy practices.	To examine Internet users' concerns about information privacy.	To examine mobile users concerns about information privacy.
<b>Focus</b>	Organizations handling of customer information.	Individual perceptions of fairness/justice in context of information privacy.	Individuals feelings that one has a right to own private information, either personally or collectively.
<b>Context</b>	Offline, direct marketing	Online (prior to mobile computing)	Connected (Internet) mobile computing
<b>Dimensions</b>	Collection Improper Access Unauthorized Secondary Use Error	Collection Control Awareness of privacy practices	Perceived surveillance Perceived intrusion Secondary use of information
<b>Representation</b>	Correlated first-order factors; could be represented as second-order factor (Stewart and Segars, 2002)	Second-order factor	Second-order factor
<b>Theoretical Foundation</b>	Fair Information Practice Principles	Social Contract and Justice theories	Communication Privacy Management theory
<b>References</b>	Smith et al., 1996	Malhotra et al., 2004	Xu et al, 2012

device, and a music player (Jobs, 2007). Jobs' definition noted the largest divergence from existing mobile phone products; the ability to access the Internet. Thus dawned the age of the smartphone, which ushered in a computing platform unmistakably different from desktop computing regarding personal privacy.

Mobile computing differs from fixed-location computing in five specific ways: location awareness, data sharing between applications, off-device (cloud) storage, always online behavior, and unique device identifiers (Liccardi et al., 2014; Xu, 2007; Xu 2012b). First, most mobile devices have location awareness that uses positioning technologies to provide individuals with reachability and accessibility. Location-based services provide an individuals with capabilities to tie their specific location to actions such as way-finding through the use of maps, offering travel directions, point of interest details, estimated time of arrival, and even traffic alerts, all possibly related to the exposure of the device's unique location (Beinat, 2001; Shklovski, 2014; Xu, 2007). Location-based services research has demonstrated that individuals who have privacy concerns are less likely to adopt the use of location-based applications and these same individuals often express that sharing location data is a top most concern (Felt et al., 2012a; Fodor, & Brem, 2015, Zhao, Lu, & Gupta, 2012). Privacy calculus research has shown that privacy concerns negatively affect the willingness of individuals to disclose information in newly downloaded applications (Dinev, & Hart, 2006; Keith et al., 2010; Xu, Tang, Hu, & Du, 2010). Additional studies have shown that the effect of privacy concerns on location sharing is weak; however, it is heavily moderated by the practice of disclosing false data (Keith, Thompson, Hale, Lowry, & Greer, 2013).

Second, mobile devices, such as smartphone contain a collection of applications that can be augmented by users' adding new applications through application stores. Few personal possessions track more about an individual than a smartphone which include phone numbers, location, email, messages, photos, and a varied collection of personal information about that individual's daily life and activities (Thrum, & Kane, 2010). The application collection on a mobile device itself gives interesting information about the person using the device; which applications are downloaded, kept over long periods, and updated regularly speak volumes about an individuals interests. However, the interaction of data from many applications combined can create an exclusive fingerprint for people their behaviors (Baarslag et al., 2016; Xu et al., 2012b). For instance, it is not uncommon for an application to ask for access to the contact list, personal photos, or location (Felt et al., 2012b; Shklovski, 2014; Xu et al., 2012). In permitting such access, individuals are not always aware of the data collected and shared between applications on devices. A data element often shared is location, and when correlated to personal contacts, phone numbers, social media accounts, notifications, and personal photos, it can offer a more invasive view of a person's life. Even when individuals become aware of these data collection aspects, very few know how to change the sharing settings of applications, and individuals often opt into whatever default settings are presented to them at sign-up (Enck, Gilbert, Han, Tendulkar, Chun, & Cox, 2014). In general, there is little to no visibility on what is shared or not shared among applications. Research has shown that when individuals become aware of this type of data sharing, in most cases, they prefer to reduce access (Almuhimedi et al., 2015; Baarslag et al., 2016; Liccardi et al., 2014).

A third attribute is the transition from applications storing personal information locally in the device to cloud-based services, essentially personal data stored in third-party services off the local device. This technology started to be in demand when the design of application capabilities exceeded the storage capacity of mobile devices. To extend the usefulness of applications, developers started building applications with cloud-based storage. Today, most applications use cloud-based services to house data from personal media such as photos and videos to financial records and health data. To compete, device makers and application developers integrate with cloud-based storage to offer sizable storage features to individuals, even unlimited storage in some cases. This application design strategy is pervasive and has made it common to trust personal data to applications with service-based storage (Angwin, & Valentino-Devries, 2011).

Fourth is the personal shift in computing behavior toward being constantly online. With mobile devices, individuals have veered from an average of 20 hours per month surfing the Internet on desktop computers to computing all day on their mobile devices. Society has changed. Individuals rarely leave home without their mobile devices. With “in-hand” mobile computing, the temptation and desire to be online are even greater (Nafus, & Tracey, 2002; Turkle, 2008). This constant activity enhances the capabilities of applications to track usage to a fingerprint of actions of individuals to more closely identify aspects of their behavior and personalities (Coonay, 2016). The collection of this data feeds into the personalization of the application services aimed to solidify the relationship between the individual and application, thus increasing the application’s value.

Last, with mobile devices, data collection is amplified. All mobile devices have a unique identifier that links the device, applications, services and personal data stored in the cloud or locally together. This unique identifier allows any firm to connect the various forms of communication to the individuals location and related mobile computing activities (Angwin, & Valentino-Devries, 2011; Keith et al., 2017; Xu et al., 2012b). Most smartphones have unique identifiers that individuals cannot opt out of tracking. Although some device makers will mask or hide unique numbers, is not widely applied.

These and other unique aspects of mobile computing have increased the debate regarding the importance of privacy violations within mobile devices (Shklovski et al., 2014). Michael Becker of the Mobile Marketing Association stated that “in the world of mobile, there is no anonymity”; phones are always with us and always on (Thrum, & Kane, 2010, p. 1). The easiest identifier is a person’s phone number and when tied to a mobile phone, it provides all that is required for application developers to follow the digital trail left by the owner. Even without phone numbers, many application developers leave behind a hidden cookie that is challenging to find and delete on a mobile device, which allows them to collect and correlate a myriad of data regarding behavior (Thrum, & Kane, 2010). Application developers build their solutions on the foundation of a connection between the application, person, and device. Developers can create a “mosaic” of information that defines a personal profile (Baarslag, 2016; Xu et al., 2012b). Some applications are built solely on the use of that data, and without access to the individual’s, personal data, the individual cannot enjoy the benefits of what is offered (Angwin, & Valentino-Devries, 2011). Given this demand for sharing to receive, privacy

concerns are aggravated in the mobile environment in particularly around unique identification numbers and location tracking (Xu et al., 2012a).

Within the last decade, multiple studies have provided insights into individuals' reactions to data collection, perceptions of risk, and intention to disclose within the mobile context (refer to Appendix A for a summary of studies). These studies have elevated the discussions around a variety of topics such as location-based awareness, application policy, permission awareness, application adoption, perceived risks, and trust. For example, Shkovski et al. (2014) and Xu et al. (2012b) demonstrated that individuals using mobile applications are concerned about data collection and tracking, and when they are informed about information leaking, privacy concerns and application adoption increase. Keith et al. (2017) and Gu et al. (2016) demonstrated that application popularity and network size (user adoption) increases the perceived benefits and reduce risk, lowering mobile privacy concerns.

In general, when the mobile application context and the inherent benefits of the application are understood, mobile privacy concerns are lowered (Aloudat, & Michael, 2011; Eastin et al., 2016; FTC, 2009; Keith et al., 2013; Keith et al., 2017; Kehr, Kowatsch, Wentzel, & Fleisch, 2015). In both desktop and mobile computing environments when individuals have had previous negative experiences regarding personal disclosure, it can increase privacy concerns and affect behavior (Cohen, 1985; Gu et al., 2017). In addition, previous studies have shown that individual awareness of data collection and the extent of data collection can increase privacy concerns (Acquisti et al., 2015; H.E.W. 1973; Keith 2017; Laudon, 1986; Malhotra et al., 2004; P.P.S.C.

1977; Smith et al., 1996; Thurm, & Kane, 2010; Xu et al., 2012b), whereas increasing control over data collection and management help in reducing those concerns (Liu, Shan, Bonazzi, & Pigneur, 2014; Malhotra et al., 2004; Xu et al., 2009).

### ***Online Equivocation***

The Internet has created an information exchange market where people trade personal information for tangible and intangible benefits (Houston, & Gassenheimer, 1987). There is some argument that this exchange mimics the boundary control continuum posed by Altman (1975) in which economic and social exchange is based on a continuum of information disclosure (Altman, 1975). Individuals disclose information when they feel that an exchange will benefit them. Individuals do not want to release information if they expect an adverse outcome (Horne, 2007; Milne, & Gordon, 1993; Sheehan, & Hoy, 2000). In all cases, individuals seek to manipulate the deal so that the exchange is of maximum benefit to them (Granovetter, 1995).

Individuals view disclosure as a social contract where they exchange information for benefits. The social contracts theory states that individuals require the exchange to be fair (Donaldson, 1989; Donaldson, & Dunfee, 1994; Dunfee et al., 1999). When individuals evaluate the issue of fairness, they move along the continuum of disclosure seeking the lowest possible cost to themselves while balancing the need to disclose. They are influenced by a desire for immediate gratification as well as the disclosure context. This is all weighted against privacy concerns to make a calculated decision (Horne, 2007; Milne, & Gordon, 1993; Sheehan, & Hoy, 2000). The privacy calculus model argues that individuals perform a cost-benefit analysis before self-disclosure (Dinev, & Hart, 2006).

In exchange for application benefits such as immediate traffic alerts and quicker directions, finding the closest location to use a time-based discount, or the social rewards of a responsive connection to personal friends and family, individuals will weigh and decide whether the benefits balance against the costs of disclosure of personal information. Individuals actively conduct a privacy calculus measuring costs and benefits before disclosing information (Culnan, & Armstrong, 1999; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990).

However, there is one more aspect to consider—online equivocation. Instead of offering genuine data, individuals can provide counterfeit data. During the process of conducting a cost-benefit calculus, if individuals determine the exchange to be unfair, they can employ an alternative strategy of providing an inaccurate response (DePaulo et al., 2003; Earp, & Baumer, 2003; Horne 2007; Tian, & Keep, 2002). Although it is seemingly socially undesirable tactic, it can be a convenient and easy strategy for information disclosure, particularly if information is required immediately by the mobile application.

Online equivocation is a method of guarding against high-risk situations and can be a way of relieving anxiety in stressful ones (Hancock et al., 2009). Approximately one-third of personal interactions involve some deception (Buller, & Burgoon, 1996; Hancock, Thom-Santelli, & Ritchie, 2004). It is not uncommon to lie; lies are used in everyday life for all sorts of topics to avoid interacting at a particular level. Lies come in all forms, from outright deception to nondisclosure, and they are as frequent online as offline (Birchmeier, Dietz-Uhler, & Stasser, 2010; Hancock et al., 2004; O’Sullivan,

2000). Deception is a personal strategy that allows control of information access and can reduce anxiety in computing environments. If firms cannot or do not provide adequate control for information management, individuals can control the exchange by withholding information or providing inaccurate personal information. In extreme cases, they can protect their anonymity by pretending to be someone completely different (DePaulo, Kashy, Kirkendol, Wyer, & Epstein, 1996; DePaulo et al., 2003; Zwick, & Dholakia, 2004).

Researchers have stated that many individuals omit information or falsify information online and have shown that the occurrence is as high as 50% of all responses (Cavoukian, & Hamilton, 2002; Hoffman, Novak, & Peralta, 1999). When information is perceived to be more sensitive than others, individuals will lie more often (Horne, 2007). Falsifying information is known to be a response strategy to address for privacy concerns (Fox, Rainie, Horrigan, Lenhart, Spooner, & Carter, 2000) and it is exacerbated in the mobile context when location and other unique real-time data can be collected and disseminated to individuals. DePaulo (1996) stated that, in real life, people lie about a range of topics, their location being one of most common. It is often acceptable to communicate an expected location versus a real location to avoid the stigma of being purposefully late. For instance, it is common to hear someone report they are right around the corner while still being miles away. If the same person were using a mobile friend connection application, it could allow any of the connected friends to track the person's whereabouts, making any misrepresentation of location moot.

Researchers have been paying more attention to the phenomenon of online deception in the last decade (refer to Appendix B for a summary of studies). Studies show that lying occurs more often in email and instant messaging than face-to-face (Van Kleek et al., 2015). The psychological and physical distance of activities online versus in-person connection influences the occurrence and amount of deception (Pak, & Zhou, 2013; Tsikerdekis, & Zeadally, 2014; Zimbler, & Feldman, 2011). In addition, individuals who already have a propensity for lying in person are more likely to lie online (Drouin et al., 2016; Lwin, & Williams, 2003).

Online equivocation is influenced by context, and individuals will lie online based on the types of activities they may be engaged in. For instance, individuals are more likely to lie on dating sites than during any other online activity. Lying online is more common than one might think, with more than one study reporting over that 80% of online dating sites are populated with equivocations (Drouin et al., 2016; Hancock et al., 2007a). A third of individuals report some online deception (Caspi, & Gorsky, 2006). Individuals have a numerous reasons for such deception, ranging from privacy concerns, discrimination, and hiding to self-presentation (Dumas et al., 2017; Hancock et al., 2007b; Pak, & Zhou, 2013; Son, & Kim, 2008; Van Kleek et al., 2015). Researchers are just beginning to probe the motivations behind equivocation online; even so, privacy concerns are prevalent in many studies as motivators for deception (Caspi, & Gorsky, 2006; Horne et al, 2007; Page et al., 2013; Pak, & Zhou, 2013; Son, & Kim, 2008; Steinel et al., 2010; Van Kleek et al., 2015).

It is reasonably straightforward to understand privacy calculus theory because it reflects the idea of fairness and exchange seen in everyday life. Individuals are motivated to balance the equation and seek the best result (Bok, 1999; Tian, & Keep, 2002). The use of online equivocation to aid in this balancing act seems a likely outcome in situations where privacy concerns are high and individuals are squeamish about sharing personal details but still desire to use an application's capabilities (Burgoon, Parrott, Le Poire, Kelley, Walther, & Perry, 1989; Jiang, 2013).

This may be more prevalent in the online world because individuals tend to put distance between themselves and the recipient of the deception; individuals feel more social distance with online connections (Argo, White, & Dahl, 2006; DePaulo et al. 1996). This is more prominent when the relationship is between an individual and an application that has no specific identifiable person attached; it is more often observed with an organization that may be unknown to the individual (Tsikerdekis, & Zeadally, 2014; Zimbler, & Feldman, 2011).

However, another phenomenon that may be influence this privacy calculus is the privacy paradox. The privacy paradox asserts that individuals will show higher levels of disclosure even after stating their privacy concerns and expressing a lower intention to disclose information (Acquisti, & Gross, 2006; Acquisti, & Grossklags, 2004; Norberg et al., 2007). The privacy paradox demonstrates that privacy concerns rarely affect actual personal disclosure behavior (Acquisti, & Grossklags, 2005; Dinev, & Hart, 2006; Youn, & Hall, 2008). The privacy paradox appears to contradict the expectation of the privacy calculus. The effect of the privacy paradox could negate the impact of the privacy

calculus theory and asserts that individuals will share their personal data regardless of privacy concerns. This would rule out the use of the privacy calculus for measuring data exchange for application benefits. Mainly, the individual would be less likely to engage in a calculus decision and more likely to just disclose information. In this case, there would be little motive to exercise a privacy calculus, thereby reducing any motivation to provide inaccurate data as part of the exchange. Essentially, despite their privacy concerns, the individuals may truthfully share their personal data regardless of the privacy calculus having little impact on driving toward a fair exchange. If the privacy paradox were in effect, despite high concerns, individuals would be less likely to offer an online equivocation in exchange for the benefits of the application.

The last consideration is whether the reverse is true in regard to privacy concerns: does providing inaccurate data increase privacy concerns rather than decreased them? The literature on deception and lying outlines that people lie for a variety of reasons: fear, self-presentation, and manipulation (Drouin et al., 2016; Levine, Kim, & Hamel, 2010). If individuals are fearful of online exposure effects such as identity theft, social shaming, or intrusive marketing, they work to avoid truthfulness. Conversely, if the fearful individuals are interested in self-presentation—putting forth a favorable image—they may be motivated to fabricate details about themselves. This manifests in some of the current behaviors reported, such as “buying likes” on social media sites to increase popularity (Dumas et al., 2017; Sass, 2017). Last, some individuals lie to manipulate others to do something, believe in something or make a decision in favor of the deceiver (Crawford, 2003).

When individuals lie, it can be stressful (Buller, & Burgoon, 1996). Keeping track in one's head of inaccurate details from one application to another is similar to tracking the hundreds of passwords individuals need to maintain security (Vance, 2010). When individuals provide false information to mobile applications, they may need to remember what information they provided to keep using the applications. Soon individuals find themselves trapped and entangled in more than one falsehood and unable to keep them all straight, which can increase anxiety and possibly increase their overall concerns (Buller, & Burgoon, 1996). Getting caught with inaccurate information online is a greater risk now because individuals possess many new opportunities to spread incorrect details. Our communication online leaves detailed record trails of our activities across dozens of applications that could be cross-referenced against reality.

The more interconnected our lives are with technology and the more we fabricate information in sharing, the more likely it is that we will be exposed personally as deceivers than actually be exposed by an application developer's losing or sharing our personal information (Garber, 2013; Hancock, Bimholtz, Bazarova, Guillory, Perlin, & Amos, 2009). Page et al. (2013) studied lying and location-sharing and found that lying increased the propensity of online privacy concerns, particularly regarding location sharing. Page et al. demonstrated that lying can backfire and increase personal privacy concerns. The question then remains: is online equivocation intended to help reduce privacy concerns, but instead increases them?

### **Conceptual Model And Propositions**

Although studies have indicated that people misrepresent their information when disclosing online, the literature has not thoroughly examined various approaches that individuals devise to misrepresent themselves and protect their personal privacy. Only a few studies have attempted to categorize online equivocation behavior, grouping actions into buckets where individuals omit data, provide inaccurate data, or are truthful (Dumas et al., 2017; Horne et al., 2007). Qualitative analysis in Essay One showed that individuals use both omission and inaccurate data in online equivocation and that online equivocation can be categorized, ranging from a simple omission to creation of an entirely new persona (see Table 2).

My online equivocation categorization complements Altman's (1975) description of how people regulate their privacy by controlling the amount of verbal output (DePaulo, 2003). Applying the same logic, it can be asserted that individuals will control their privacy by determining how much to reveal about themselves on a continuum from little effort to extensive effort. When faced with providing personal information in mobile applications where individuals do not want to divulge but are required to give a response for participating, it follows that they will resort to a method of online equivocation efficiently hiding their true selves.

Drawing on the literature of the privacy calculus theory, the conceptual model proposes that a cost-benefit decision regarding individual disclosure exists where individuals will use an online equivocation strategy to maximize their personal benefits and reduce personal costs associated with personal disclosure, thereby potentially

reducing their mobile privacy concerns. However, according to emerging research, online equivocation could have a reverse effect and actually increase mobile privacy concerns.

Overall, I have hypothesized the following:

*H1. The level of online equivocation affects the level of perceived mobile privacy concerns.*

The least costly of these strategies include omission, whereas the most costly include the development of an online persona. Individuals engage in numerous disclosure behaviors online, and the behavior that involves the least effort is to omit optional information. This recognizes that omitting required information does not enable the individual to access the mobile application. If data are required, and individuals wish to omit information, they may not be able to use the application. Omitting information about oneself requires little effort and is a practice to avoid personal information disclosure (Van Kleek et al., 2015). Accordingly, the following can be suggested:

*H1a: The practice of omission, or the leaving out of optional personal information in mobile applications, affects the perceived level of mobile privacy concerns.*

Another form of online equivocation is abbreviation. Individuals can employ other simple techniques to limit privacy exposure by abbreviating or shortening data values as a way of not providing the full information requested. Therefore, the following is expected:

*H1b: The practice of abbreviation, the limiting of personal information in mobile applications, affects the perceived level of mobile privacy concerns.*

Individuals tend to falsify some items to a greater extent than others, using numerous strategies, including the effort to hide sensitive information, create separation, and avoid harassment or discrimination (Culnan, & Milne, 2001; Fox et al., 2000; Kobsa, 2002; Van Kleek et al., 2015). In doing so, they may offer a substituted value that was true at one time but is no longer viable or is now false. Examples are old addresses, an unused phone number, or an unchecked email address. In addition, individuals may offer inaccurate data such as false phone numbers, false email addresses, alternative birth dates, or even opposite gender indicators (male for female and vice versa). In these circumstances, individuals can supply data that is essentially fake: addresses no longer accepting mail for the previous resident or email addresses that simply bounce. Using these substitution methods allows individuals to change the cost of disclosure, therefore hiding their truths. I suggest the following:

*H1c: The practice of substitution, the offering of inoperable data as a substitute for the truth in mobile applications, affects the perceived level of mobile privacy concerns.*

Another form of substitution is combined substitution. Individuals use a strategy of combining two or more inoperable data values to limit their privacy exposure. Individuals use this combined substitution as a common strategy across numerous applications in an effort to mask personal data (Drouin et al., 2016; Horne et al, 2007; Kobsa, 2002; Van Kleek et al., 2015). Therefore, the following is expected:

*H1d: The practice of combined substitution, the offering of two or more inoperable data values as a substitute for the truth in mobile applications, affects the*

*perceived level of mobile privacy concerns.*

A phenomenon seen online is the use of alternative personas, the practice of creating an alternative identity that allows individuals to present themselves differently (Drouin et al., 2016; Dumas et al., 2017; Hancock et al., 2007b; Lu, 2008, Steinel et al., 2010). Several studies have shown that this practice is often used for supporting self-presentation, allowing individuals to create a personas that represent more idealized versions of themselves. However, individuals also create these personas to hide from others, separate aspects of their personal life, and avoid detection (Drouin et al., 2016; Pak, & Zhou, 2013; Steinel et al., 2010; Van Kleek et al., 2015; Wang et al., 2016). Developing a separate persona, an online disguise, in the spectrum of equivocation strategies requires the most effort and can affect mobile privacy concerns. I suggest the following:

*H1e: The practice of developing an alternate persona, a disguised identity, in mobile applications, affects the perceived level of mobile privacy concerns.*

### ***Mobile Disclosure Context***

Disclosure is never without the influence of social context, which also extends to mobile computing. In particular, the mobile computing context can bring focused attention to certain data collection aspects that may affect individuals' view of privacy concerns and their disclosure response. Some mobile applications, such as health and fitness applications, will record not just workout plans and results but biometric data such as running distance, heart rate, and physical details. In the right context, individuals are more willing to disclose personal information in applications when their expectations for

how information is applied are met (Bansal, & Gefen, 2010; Bansal, & Zahedi, 2008; Culnan, & Armstrong, 1999; Culnan, & Bies, 1993, Stone, & Stone, 1990). The context moderates the trust model that the individual has with the application itself; if it makes sense, then it is more acceptable. Therefore, if the application provides health services, requesting health information feels more acceptable and is less likely to be a concern (Acquisti et al., 2015; Boyd, 2014; Marx, 2001; Nissenbaum 2009; Stutzman et al., 2013; Thibaut, & Kelley, 1959).

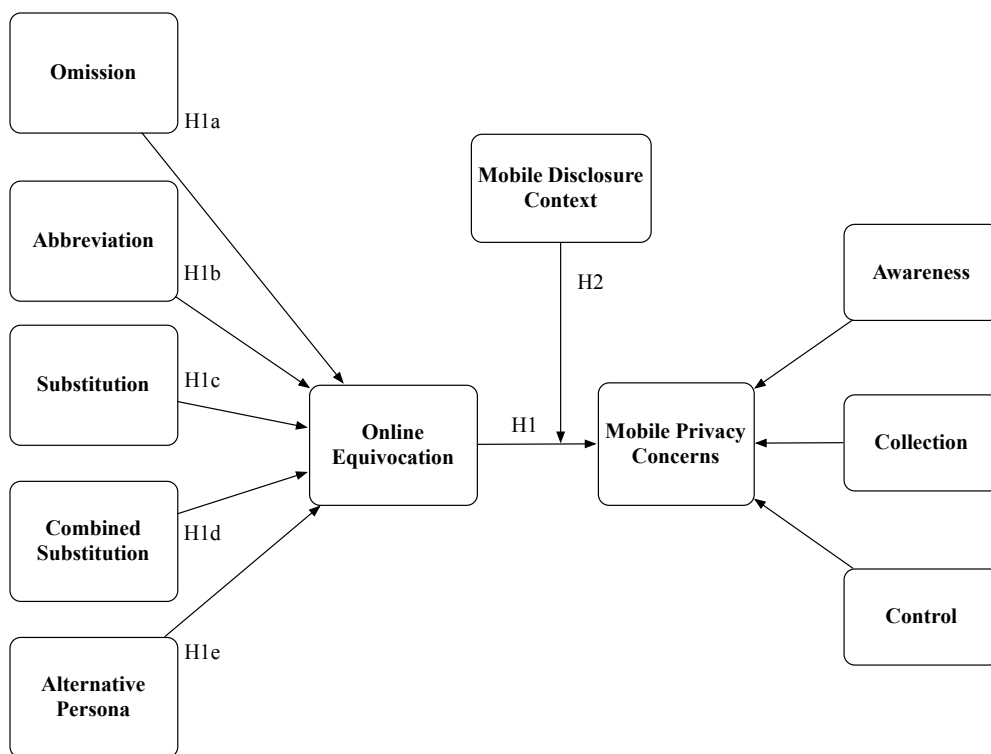
Not all data are treated the same, and individuals have different comfort levels with various types of information. Not only must the information seem appropriate to share in the context, but it may also have to meet the individual's own view of what is comfortable to share (Barkhuus, 2012; Nissenbaum, 2009; Norberg, 2007; Shklovski, 2014). Typically, information that is uniquely personally identifiable becomes more important than those aspects that are less so. When sharing health data, individuals may be less likely to share their real weight than what they had to eat that day (Ackerman, 1999). Furthermore, the more likely that information is personally identifiable the more likely they are to offer an online equivocation when in doubt (Bansal, & Zahedi, 2008; Bansal, & Gefen, 2010; Horne, 2007). Thus, I assert that how individuals value and perceive the applications and data collected may influence their disclosure behavior toward online equivocation, which in turn may influence their perceptions of privacy concerns (Fodor, & Brem, 2015; Morey et al., 2015; Teltzrow, & Kobsa, 2004; Xu et al., 2012a; Xu et al., 2012b; Zhao et al., 2012). The sensitivity of data collected can influence an individual's willingness to provide truthful information (Gu et al., 2017; Malherios et al., 2013).

Therefore, I suggest the following:

*H2: The mobile disclosure context will moderate the relationship between the level of online equivocation and the level of mobile privacy concerns.*

### *Research Framework*

The research framework examines the relationship between online equivocation and mobile privacy concerns, hypothesizing that individuals employ methods to protect their privacy by offering inaccurate information in place of accurate data, thereby reducing the risk of exposure. The model postulates that online equivocation affects mobile privacy concerns (see Figure 4). It measures online equivocation, building on the analysis completed in Essay One defining the various online equivocation strategies employed by individuals. The model measures these strategies as formative measures of online equivocation. Also, the model evaluates the effect of mobile disclosure context as a moderator on mobile privacy concerns, examining whether the mobile disclosure context moderates the overall effect.



**Figure 4. Diagram of the Conceptual Model**

## **Mehodology**

### *Measures*

The conceptual model illustrates the construct of online equivocation and mobile privacy concerns. To examine this model, I measure online equivocation by leveraging the definitions offered in Essay One. Online equivocation is defined as strategies employed by individuals to exchange truthful responses for inaccurate data. The five categories of online equivocation are omission, abbreviation, substitution, combined substitution, and alternative persona (see Table 3). To measure privacy concerns, I build upon the work of Malhotra et al. (2004), which demonstrated that privacy concerns can be examined by measuring individual perceptions and viewpoints regarding online application practices around personal information collection, control, and usage. Malhotra et al. (2004) developed an instrument called IUIPC (*Internet Users Information Privacy Concerns*), which was adapted from the *Concerns for Information Privacy* (CFIP) scale previously developed by Smith et al. (1996).

IUIPC includes three dimensions for privacy concerns: personal information collection, personal control of collected information, and personal awareness of policies around information use. Malhotra et al. (2004) demonstrated that IUIPC excelled as a predictor of privacy concerns. Since its publication, Malhotra et al.'s (2004) IUIPC instrument has been used in multiple studies; however it has been underused in subsequent mobile privacy research (Bélanger, & Crossler, 2011; Preibusch, 2013; Stewart, & Segars 2002). A few noted and more recent studies such as Xu et al. (2012a), who extended the IUIPC instrument to include factors for perceived intrusion and

perceived surveillance, have aimed to enhance Malhotra et al.'s measures. In addition, Xu et al. (2010) extended privacy awareness measures for future studies. I extend the IUIPC instrument to include both new and updated measures for mobile privacy concerns, thus building on the work of Smith et al. (1996), Malhotra et al. (2004), Xu et al. (2010), and Xu et al. (2012a). This effort is supported by the work of Bélanger and Crossler (2011), who outlined the need for a measure of privacy concerns in varying contexts and suggested that researchers build upon the previous work of privacy researchers.

I enhanced the set of measures to address the six aspects of mobile computing that can influence privacy concerns: location awareness, data sharing across applications, off-device (cloud) storage, “always on” computing behavior, unique device identifiers, and biometric data collection (Liccardi et al., 2014; Xu, 2007; Xu et al., 2012a). The final instrument extends IUIPC for the mobile computing as a contribution in this study and for future studies. Refer to Table 18 for an overview of the instrument construct and measures and Table 19 for details of the proposed additions.

**Table 18**

Construct and indicator breakdown.

Construct	Sub-Construct	Type	Description	Indicators / Description
<b>Mobile Privacy Concerns</b>		Formative 2nd Order	Sub-constructs 1st Order: Collection, Control & Awareness	Collection 1-8 Control 1-7 Awareness 1-10
	Collection	Formative 1st Order	Collection 1-8	Measures about the types of data collected online such as personal information, collected data from the device, ongoing collection, cloud based storage, unique identifier of mobile device, location and biometric data.

**Table 18**

Construct and indicator breakdown.

Construct	Sub-Construct	Type	Description	Indicators / Description
	Control	Formative 1st Order	Control 1-7	Measures on how much control over profile information, application tracking, access to other data on the device, including control over whether your data is shared with 3rd parties, ability to cancel or delete your data or account.
	Awareness	Formative 1st Order	Awareness 1-10	Knowledge and awareness of apps privacy policies, if policies are easy to understand and clear about data collected, how the data is used, if it is shared with 3rd parties, if it is combined with 3rd party data together, aware of unique id use, or location data use, or when data is shared across multiple applications, as well as awareness of biometric data collection.
<b>Online Equivocation</b>		Formative 1st Order	Behavior 1-7	Behavior of individuals to use strategies such as omission, abbreviation, substitution of their personal data (old information, unused information, fake information) or combination of multiple fake fields together up to creation of a alternative persona.

**Table 19**

Survey Items and Sources

Latent Variable	Item	Measure	Source
<b>Mobile Privacy Concerns</b>	Second order latent variable comprised of Collection, Control and Awareness.	Collection, Control and Awareness Latent Variable Scores	Steward & Segars, 2002
<b>Collection</b>	For [scenario] application, indicate your level of concern about the collection of your personal information.	Likert scale 1-5: Not at all concerned (1), Slightly concerned (2), Somewhat concerned (3), Moderately concerned (4), Extremely concerned (5)	Malhotra et al., 2004; Smith et al., 1996; Xu, 2010; Xu et al., 2012a
<b>Collection 1</b>	About Me	Collection and use of personal information about me.	Concern Likert scale 1-5 as noted above.
<b>Collection 2</b>	Other Data	Access to other data on my device.	Concern Likert scale 1-5 as noted above.

**Table 19**

## Survey Items and Sources

Latent Variable		Item	Measure	Source
<b>Collection 3</b>	Amount	Amount of personal information collected about me at sign-up.	Concern Likert scale 1-5 as noted above.	
<b>Collection 4</b>	Ongoing	Amount of personal information collected on an ongoing basis.	Concern Likert scale 1-5 as noted above.	
<b>Collection 5</b>	Cloud storage	Amount of personal information that is stored in the app's storage systems.	Concern Likert scale 1-5 as noted above.	
<b>Collection 6</b>	Unique ID	Ability to uniquely identify my mobile device.	Concern Likert scale 1-5 as noted above.	
<b>Collection 7</b>	Location	Ability to determine my location.	Concern Likert scale 1-5 as noted above.	
<b>Collection 8</b>	Biometrics	Ability to collect biometric (face, finger, voice, health) information about me.	Concern Likert scale 1-5 as noted above.	
<b>Control</b>		For [scenario] application, indicate your level of concern about the control you have over your collected personal information.	Likert scale 1-5: Not at all concerned (1), Slightly concerned (2), Somewhat concerned (3), Moderately concerned (4), Extremely concerned (5)	Malhotra et al., 2004; Smith et al., 1996; Xu, 2010; Xu et al., 2012a
<b>Control 1</b>	Control Profile	The control you have over your profile information (name, birth date, address, billing address, email).	Concern Likert scale 1-5 as noted above.	
<b>Control 2</b>	Control Tracking	The control you have over how the app tracks your app usage.	Concern Likert scale 1-5 as noted above.	
<b>Control 3</b>	Control Access to Device	The control you have over the app's access to other information on your device.	Concern Likert scale 1-5 as noted above.	
<b>Control 4</b>	Control Access to Personal Contacts	The control you have over the app's access to your personal contacts (friends and family).	Concern Likert scale 1-5 as noted above.	
<b>Control 5</b>	Control Personal Experience Data	The control you have over information used to personalize the app experience.	Concern Likert scale 1-5 as noted above.	
<b>Control 6</b>	Control Shared to 3rd Parties	The control you have over personal information shared with third parties.	Concern Likert scale 1-5 as noted above.	
<b>Control 7</b>	Control to Delete or Cancel	Ability for you to cancel or delete your account at any time.	Concern Likert scale 1-5 as noted above.	

**Table 19**

## Survey Items and Sources

Latent Variable		Item	Measure	Source
<b>Awareness</b>		For [scenario] application, indicate your level of concern about your understanding of how your personal information is managed by the application.	Likert scale 1-5: Not at all concerned (1), Slightly concerned (2), Somewhat concerned (3), Moderately concerned (4), Extremely concerned (5)	Malhotra et al., 2004; Smith et al., 1996; Xu, 2010; Xu et al., 2012a
<b>Awareness 1</b>	Accessible Policies	The app provides an accessible privacy policy.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 2</b>	Policy Easy to Understand	The app's privacy policy is easy to understand.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 3</b>	Clear about Data Collected	The app provides a clear outline of what information it collects.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 4</b>	Explains How Data Used	The app explains how it uses the information it collects.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 5</b>	Aware of 3rd party Sharing	The app describes what third parties it shares your information, what information is shared and how often.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 6</b>	Aware Combined Information with 3rd Parties	The app describes if it combines the information it collects about you with other third party information it gathers to better understand you.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 7</b>	Aware of Unique ID Use	The app describes how it uses your unique device id and/or phone number.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 8</b>	Aware Location Data Collected	The app describes how it uses your location data.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 9</b>	Aware Data is Shared with Multiple Apps	The app describes how it uses the information collected from other apps on your device such as personal photos, contacts.	Concern Likert scale 1-5 as noted above.	
<b>Awareness 10</b>	Aware of Biometric Data	The app describes how it uses biometric information it collects about you.		

**Table 19**

## Survey Items and Sources

Latent Variable		Item	Measure	Source
<b>Online Equivocation</b>		When using this [scenario] application, how likely are you to share your personal information as described.	Omission, Abbreviation, Substitution, Combined Substitution, Alternative Persona Latent Variable Scores	Van Kleek et al., 2015; Page et al., 2013; Pak & Zhou, 2011b; Son & Kim, 2008; Wang et al., 2016
<b>Behavior 1</b>	Omission	Leave out or skip personal information if it is optional.	Likert scale 1-5: Extremely unlikely (1), Unlikely (2), Neutral (3), Likely (4), Extremely Likely (5)	
<b>Behavior 2</b>	Abbreviation	Abbreviate some personal information, such as initials for a name or only part of an address.	Likely Likert scale 1-5 as noted above.	
<b>Behavior 3</b>	Substitution (old info)	Provide personal information that is accurate in the past, but is not current, such as an old address, old email, or a previous name.	Likely Likert scale 1-5 as noted above.	
<b>Behavior 4</b>	Substitution (unused info)	Provide an email address that you rarely or never check.	Likely Likert scale 1-5 as noted above.	
<b>Behavior 5</b>	Substitution (false info)	Provide some fictional personal information, such as a false name, birth date, address, phone number, gender or email address.	Likely Likert scale 1-5 as noted above.	
<b>Behavior 6</b>	Combined Substitution	Provide more than one form of old or fictional information, such as a combination of an old address and a false birth date consistently.	Likely Likert scale 1-5 as noted above.	
<b>Behavior 7</b>	Alternative Pesona	Completely make up a new false persona.	Likely Likert scale 1-5 as noted above.	
<b>Mobile Disclosure Context</b>		Each subject responded to one of seven application scenarios:		Developed for this study.
<b>MDC 1</b>		1) Social networking		
<b>MDC 2</b>		2) Photo storage & sharing		
<b>MDC 3</b>		3) Music listening & sharing		
<b>MDC 4</b>		4) Productivity tools		
<b>MDC 5</b>		5) Transportation		
<b>MDC 6</b>		6) Health & fitness		
<b>MDC 7</b>		7) Financial management		

### *Participants*

To study mobile privacy concerns and online equivocation behavior, I focused my research on subjects who participated in mobile computing using smartphones and had experience downloading mobile applications. In addition, the respondents were filtered to only reside in the geographic area of the United States. Data collection was executed through an online survey administered through an opt-in panel service called AYTM. AYTM is a large panel survey service that manages a proprietary panel of 25 million respondents. This service is similar to Amazon Mechanical Turk (MTurk) providing opt-in respondents; AYTM verifies respondents through a multi-factor authentication method to ensure no account duplication. AYTM also supports stratification on both demographics and a variety of psychometric attributes and filters respondents using pre-qualification questions.

An online survey through the AYTM service was preferred because of it offered a rapid turnaround on data collection, the ability to meet quotas and support stratification, and geographic reach across the United States (Sue, & Ritter, 2012). Opt-in online panels are considered a method of sampling, which can be used to support academic studies that cannot conduct representative surveys across large geographic areas because of timing and costs. Although the validity of online surveys and experiments using online panels has been actively debated, researchers have stated that running studies on similar online panels such as MTurk has resulted in more representative, demographically diverse responses than studies solely focused on college students (Buhrmester, Kwang, &

Grosling, 2011; Hitlin, 2016; Holden, Dennie, & Hicks, 2013). Furthermore, Buhrmester et al., (2016) showed that opt-in online panels such as MTurk met acceptable psychometric quality criteria (Buhrmester et al., 2016).

Some security and privacy researchers have regularly leveraged online panels to understand individuals' privacy preferences and measure online behavior across a broad demographic set (Redmiles, Kross, Pradhan, & Mazurek, 2017). These studies compare opt-in online panels such as MTurk to probabilistic telephone samples and have shown them to be accurate within 2.7% of true widespread sampling in the United States (Redmiles et al., 2017, p. 1) Opt-in online panels have been noted to be slightly more representative of the United States population than census-representative panels with the exception of respondents with less than a high school education or older than 50 years (Landers, & Behrend, 2015; Redmiles et al., 2017).

Studies using opt-in online panels as a method of sampling that is subject to the same methodological limits as other samples, such as having individuals recruited from common subject pools like employers and colleges. Opt-in online panels such as AYTm are not representative of any particular population because the panel service provides enough sampling capability to gather data from a large demographic and psychographic population. AYTm supported filtering to compose of sample set of respondents that met the particular demographic and psychographic population required, creating a purposive sample (Chandler, & Shapirol 2016; Trochim, Donnelly, & Arora, 2015). However, this method can exclude specific subpopulations, and the overall sample could be mistaken as representative when it is not. For instance, opt-in online panels like AYTm are more

attractive to populations that are comfortable using computers and mobile devices versus those individuals who do not (Hitlin, 2016). To a certain extent, these types of opt-in panels are exclusive to individuals who have access to online resources. This is less of an issue for this study because the desire is to build a purposive sample from a demographic selection and prequalification process targeted at subjects who have mobile computing experience. The final sample is considered a nonprobability sample that pulls from a group of individuals fitting the study's purpose (Langer, 2018; Trochim et al., 2015).

The final survey was offered to respondents in the United States over the age of 18 who met the prequalification criteria based on questions designed to ensure that the respondents had mobile computing experience using smartphones and downloading applications (Fowler, & Cosenza, 2009). As noted, AYTM provides no random selection capability; the survey is posted, and opt-in panel members who meet the criteria respond. In this sample, I was able to reach target respondents across a range of demographic attributes as well as mobile computing experience; however, the sample over-represents some subgroups with a larger percentage of generation x respondents and a higher collection of individuals with bachelor's degree (see Tables 20 and 21).

To reduce nonresponse bias in the population, I elected to gather a larger sample to support a better chance of generalizing from the respondents (Armstrong, & Overton, 1977; Sivo, Saunders, Chang, & Jiang, 2006). The anticipated effect size is 0.1, desired statistical power is 0.8, number of latent variables is two (2), number of observed variables is 31, the minimum sample size to detect effect is 947, and recommended

**Table 20**

<i>Demographics for Survey</i>		<b>Count</b>	<b>Percentages</b>	
<b>Gender</b>	Female	1423	48%	
	Male	1509	51%	
	Non Conforming	15	1%	
<b>Age</b>	Gen z	14-23*	275	9%
	Gen Y	24-41	378	13%
	Gen X	42-52	2005	68%
	Baby Boomers 2	53-63	253	9%
	Baby Boomers 1	64-72	64	2%
	Post WW 2	73-90	15	1%
<b>Education Level</b>	Less than High School	0	0%	
	High school or equivalent	251	9%	
	Some college but no degree	589	20%	
	Associate degree	277	9%	
	Bachelor degree	1266	43%	
	Graduate degree	555	19%	

sample size is 6,138 (Sloper, 2018). The final survey resulted in a total of 3,457 responses collected; of which after data cleaning, 2,947 were accepted for analysis.

**Table 21**

<i>Mobile Experience Control Variables</i>		<b>Count</b>	<b>Percentages</b>
<b>Smart Phone Experience in Years</b>	0 - Less than one year, 2018	11	0%
	1 - Since 2017	65	2%
	2 - Since 2016	177	6%
	3 - Since 2015	354	12%
	4 - Since 2014	572	19%
	5 - Since 2013	911	31%
	6 - Since 2012	1190	40%
	7 - Since 2011	1574	53%
	8 - Since 2010	2038	69%
	9 - Since 2009	2341	79%

**Table 21**

<i>Mobile Experience Control Variables</i>		<b>Count</b>	<b>Percentages</b>
	10 - Since 2008	2630	89%
	11 - Since 2007	2947	100%
<b>Application Consumption per Month on Average</b>			
	1 app per month	945	32%
	2 app per month	701	24%
	3 app per month	374	13%
	4 app per month	357	12%
	5 app per month	307	10%
	6 app per month	134	5%
	7 app per month	129	4%
<b>Total Applications on Smart Phone</b>			
	0-99	1468	50%
	100-199	641	22%
	200-299	401	14%
	300-399	267	9%
	400-499	88	3%
	500-700	82	3%

### *Procedures*

The analysis of the mobile disclosure context completed in Essay One provides a scheme for a new set of measures to affect online equivocation on mobile privacy concerns. The scheme ensures that the primary set of application types, data elements, and privacy policy sharing characteristics represent the mobile computing environment in seven key application scenarios. Scenarios are used in many business ethics studies (Mietzner, & Reger, 2005) and employed in privacy studies (Malhotra et al., 2004). In this study, we used scenarios to create differentiation by prompting subjects to respond to the theme of the scenario. Scenarios can help open the respondent's mind in the survey process and not only support the aim of data collection but also help create a storyline that can ground the subject to the survey questions.

Subjects were asked to respond to the survey instrument with one of the mobile context scenarios in mind. Enough data were collected for each of the seven scenarios to ensure adequate coverage of the variety of mobile disclosure contexts. Only one scenario was used per respondent; the scenarios varied among respondents until a quota was met for each scenario. A listing and definition of scenarios are detailed in Table 22.

Response rates are another important aspect of gaining a quality data set for analysis. It is important to encourage respondents to fill in the requested surveys, and using an opt-in panel promote response. The AYTm service provides the date and time

Table 22

*Scenario Descriptions and Respondent Counts*

<b>Scenarios</b>	<b>Description</b>	<b>Examples</b>	<b>Total Responses</b>
<b>Social Networking</b>	Applications that promote social sharing with others such as photos, calendars, commentary.	Facebook, Twitter	572
<b>Photo Storage &amp; Sharing</b>	Applications which allow individuals to store photos online in server storage not controlled by the individual (e.g. cloud storage) and share those photos with others.	SnapChat, Instagram, YouTube, GooglePhotos	389
<b>Music Listening and Sharing</b>	Applications which allow individuals to listen to music online, create personalized play lists, comment on music and share with others.	Pandora Music, iHeart Radio, Spotify Music	497
<b>Productivity Tools</b>	Applications which provide tools and online services (cloud storage) in which individuals can send electronic mail, messages, store files and manage personal calendars for themselves or shared with others.	DropBox, Google Docs, Microsoft Outlook	514
<b>Transportation</b>	Applications which provide transportation services to individuals such as private or shared taxi services and to do so expose their distinct location.	Uber, Lyft, Waze	341
<b>Health &amp; Fitness</b>	Applications which collect biometric data such as health statistics (blood pressure, heart rate), fitness activity and routines, and personal logged data.	MyFitness, Fitbit, Google Fit	329
<b>Financial Management</b>	Applications which support the management of money by providing aggregated or consolidated views of money flow and spending including personal designed budgets.	Venmo, Mint, Credit Karma	305

of each completed response to examine early against late responses to evaluate whether there is a significant difference between the entries toward the end. Some researchers have suggested that late responders are more similar to nonresponders than early responders (Draugalis, Coons, & Plaza, 2008).

Because the survey addressed individuals' behaviors around privacy and providing inaccurate data, I assume that some respondents may not want to admit to behavior they would feel was socially undesirable. Within the online questionnaire, respondents remained anonymous and were likely to worry about what the data collector might be thinking. Because the service is an opt-in service, the respondents were provided

monetary incentives to participate. The service has a clear policy protecting respondents' privacy.

To prepare the survey instrument, the survey was administered to a small subset of the intended population, testing scenarios. Subjects were asked to take the survey as well as provide feedback on the understandability of the survey instrument. The initial intent was to have subjects respond to multiple scenarios; however, pretesting results showed that subjects lost interest and were confused about for which scenario they were answering questions. Therefore, the final survey included only one scenario per subject.

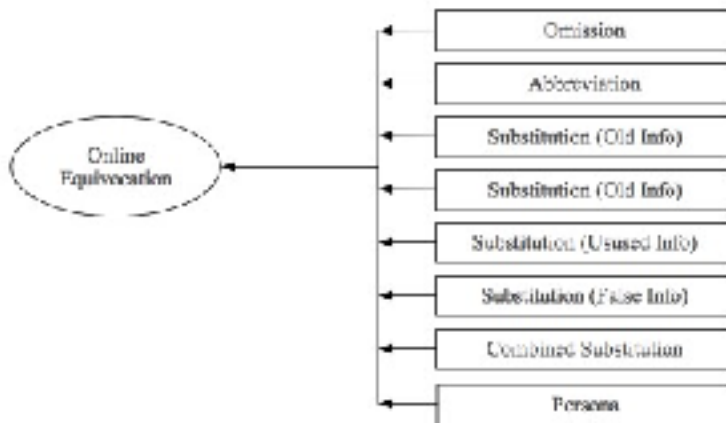
The survey instrument was also tested for face validity; 35 individuals considered experts in mobile computing read through the survey and commented on whether the questions effectively capture the topics. The collected feedback provided insights on changes to the preliminary questions regarding mobile smartphone and application use, as well as demographic questions. The majority of the face validity feedback indicated that the measures for online equivocation and mobile privacy concerns were sound.

The final survey gathered data regarding online equivocation strategies used by individuals in mobile computing and their privacy concerns. The survey allowed for anonymous responses to the sensitive questions of falsifying information. It also allowed testing of multiple scenarios that individuals encounter within mobile computing, enabling the data to reflect not just a single aspect of mobile computing but also the common ways that individuals interact with their mobile devices using a variety of applications. The survey exercised the new measures developed for mobile privacy concerns, an aspect of mobile computing that has emerged dominantly in the last decade.

## Results

The study survey was executed online in February 2018 using the AYTm online panel service and collected 3,457 responses. Data collected within the first 72 hours of the survey introduction were accepted for analysis; pretest responses and late posttest responses were removed from the data set, along with incomplete responses. IBM SPSS Statistics (SPSS) frequency statistics on the data set was used to ensure that the final data set for analysis had no missing data or was incomplete. StandardDev measures were used to check engagement (STDEV.P); rows that showed low values and had the same or similar answers across key measures were also removed. The final data set comprised 2,947 responses. The post-hoc statistical power calculation for multiple regression for this data set given the observed probably level of 0.05, seven (7) predictors and observed R-square of 0.136, and sample size of 2,947 equals an observed statistical power of 0.999 (Sloper, 2018). A statistical power close to 1.0 allows the generalization of findings to the population (Cohen, 1988, 1992).

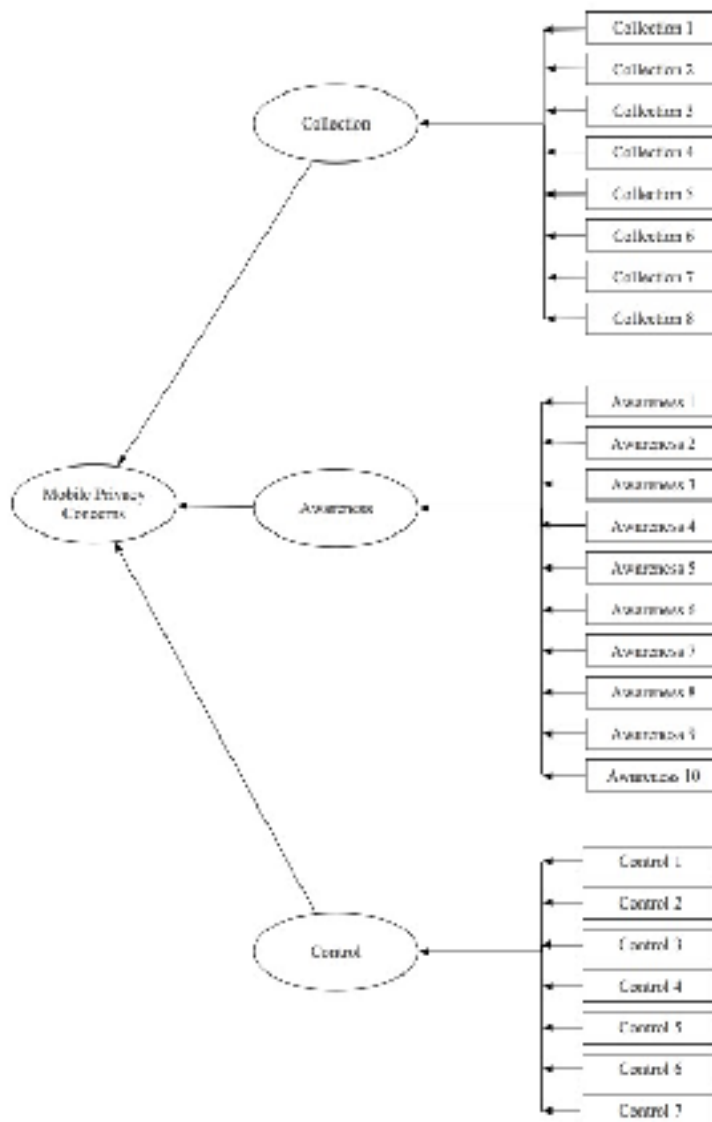
The model is formulated as a higher-order formative-formative construct using partial least square structured equation modeling (PLS-SEM; Hair, Hult, Ringle, & Sarstedt, 2016). Before building the higher-order construct, the lower-order constructs were assembled and measured for validity. The independent variable, online equivocation, and its measures are composed as outlined in Figure 5, and the PLS-SEM model figure is shown in Appendix D. The dependent variable, mobile privacy concerns,



**Figure 5. Online Equivocation (Formative Model)**

and its measures are also composed as formative and outlined in Figure 6, and the PLS-SEM model figure is given in Appendix C. Both constructs are validated by examining multicollinearity, along with the significance and relevance of the indicators as observed through outer weights. To derive the statistics required, a PLS algorithm using SmartPLS 3.2 was executed for factor analysis with 1,000 sub-samples using Mode B (Chin, 1998; Petter, Straub, & Rai, 2007). Acceptable collinearity (VIF) values of 3.3 or below show positive results for collinearity (Afthanorhan, 2014; Cenfetelli, & Basselier, 2009; Diamantopoulos, & Siguaw, 2006; Petter et al, 2007; Wan, 2014). Both the independent variable, online equivocation, and the dependent variable, mobile privacy concerns, show acceptable collinearity (VIF) statistics (see Table 23).

Both formative lower-order constructs are also tested for significance and relevance for each indicator by examining the outer weights obtained using the



**Figure 6. Mobile Privacy Concerns (Formative Model)**

PLS algorithm's bootstrap method for factor analysis with 5,000 sub-samples. The outer weights should show a *t*-statistic value of over 1.96 and a *p*-value of 0.01 or better (Hair et al., 2016; Wan, 2014). The outer weights for online equivocation demonstrate both relevance and significance (see Table 24). The outer weights for mobile privacy concerns, particularly the lower-order construct of awareness, exhibit poor results for four of the

**Table 23**

## Collinearity Results for Formative Measures

<b>Indicator</b>	<b>Collinearity VIF</b>	<b>Indicator</b>	<b>Collinearity VIF</b>
<b>Awareness 1</b>	2.871	<b>Control 1</b>	2.068
<b>Awareness 2</b>	2.736	<b>Control 2</b>	1.730
<b>Awareness 3</b>	3.150	<b>Control 3</b>	2.392
<b>Awareness 4</b>	3.176	<b>Control 4</b>	2.335
<b>Awareness 5</b>	2.870	<b>Control 5</b>	1.819
<b>Awareness 6</b>	2.666	<b>Control 6</b>	2.154
<b>Awareness 7</b>	2.525	<b>Control 7</b>	1.592
<b>Awareness 8</b>	2.497	<b>Omission</b>	1.189
<b>Awareness 9</b>	2.784	<b>Abbreviation</b>	1.509
<b>Awareness 10</b>	2.282	<b>Substitution Old Info</b>	1.721
<b>Collection 1</b>	2.574	<b>Substitution Unused Info</b>	1.463
<b>Collection 2</b>	1.956	<b>Substitution False Info</b>	2.353
<b>Collection 3</b>	2.139	<b>Combined Substitution</b>	2.559
<b>Collection 4</b>	2.510	<b>Persona</b>	1.996
<b>Collection 5</b>	2.480		
<b>Collection 6</b>	1.752		
<b>Collection 7</b>	1.694		
<b>Collection 8</b>	1.579		

**Table 24**

Outer Weights for Online Equivocation Measures

	<b>Original Sample (O)</b>	<b>Sample Mean (M)</b>	<b>Standard Deviation (STDEV)</b>	<b>T Statistics ( O/STDEV )</b>	<b>P Values</b>
<b>Omission</b>	0.099	0.098	0.006	16.906	0.000
<b>Abbreviation</b>	0.191	0.191	0.003	67.287	0.000
<b>Substitution (Old Info)</b>	0.204	0.203	0.003	66.542	0.000
<b>Substitution (Unused Info)</b>	0.188	0.188	0.003	61.665	0.000
<b>Substitution (False Info)</b>	0.233	0.233	0.003	87.471	0.000
<b>Combined Substitution</b>	0.238	0.238	0.003	84.548	0.000
<b>Persona</b>	0.216	0.216	0.003	70.910	0.000

measures: one through four (see Table 25). These measures focus on the aspects of privacy policies, in particular the availability of privacy polices, clarity, understanding, and whether the policy outlines the data collected and usage. To further explore these measures, we examine the outer loadings as well (see Table 26) and find that they are acceptable at over 0.7 (Cenfetelli, & Basselier, 2009; Hair et al., 2016; Wan, 2014). Besides the outer loading findings, it is important to retain the measures on privacy policies when examining mobile privacy concerns. A significant set of studies center around privacy polices and privacy concerns, which justifies keeping the measures in the formative causal construct. In addition, there is no overlap with the other measures (Cenfetelli, & Basselier, 2009; Smith et al., 2011).

**Table 25**

Outer Weights for Mobile Privacy Concern Measures

	<b>Original Sample (O)</b>	<b>Sample Mean (M)</b>	<b>Standard Deviation (STDEV)</b>	<b>T Statistics ( O/STDEV )</b>	<b>P Values</b>
<b>Awareness 1</b>	0.035	0.035	0.031	1.110	0.267
<b>Awareness 2</b>	-0.016	-0.016	0.030	0.524	0.600
<b>Awareness 3</b>	-0.017	-0.017	0.032	0.536	0.592
<b>Awareness 4</b>	0.058	0.057	0.034	1.695	0.090
<b>Awareness 5</b>	0.077	0.077	0.032	2.404	0.016
<b>Awareness 6</b>	0.312	0.312	0.032	9.749	0.000
<b>Awareness 7</b>	0.176	0.177	0.029	6.051	0.000
<b>Awareness 8</b>	0.169	0.169	0.030	5.689	0.000
<b>Awareness 9</b>	0.154	0.154	0.031	5.015	0.000
<b>Awareness 10</b>	0.240	0.240	0.027	8.993	0.000
<b>Collection 1</b>	0.156	0.156	0.029	5.311	0.000
<b>Collection 2</b>	0.209	0.209	0.027	7.832	0.000
<b>Collection 3</b>	0.148	0.147	0.027	5.403	0.000
<b>Collection 4</b>	0.140	0.140	0.026	5.470	0.000
<b>Collection 5</b>	0.189	0.189	0.026	7.307	0.000
<b>Collection 6</b>	0.161	0.161	0.024	6.708	0.000
<b>Collection 7</b>	0.128	0.127	0.025	5.122	0.000
<b>Collection 8</b>	0.166	0.166	0.023	7.308	0.000
<b>Control 1</b>	0.167	0.167	0.021	7.799	0.000
<b>Control 2</b>	0.218	0.218	0.020	10.760	0.000
<b>Control 3</b>	0.274	0.274	0.024	11.476	0.000
<b>Control 4</b>	0.182	0.181	0.022	8.343	0.000
<b>Control 5</b>	0.134	0.134	0.021	6.502	0.000
<b>Control 6</b>	0.218	0.217	0.022	9.970	0.000
<b>Control 7</b>	0.078	0.078	0.020	3.964	0.000

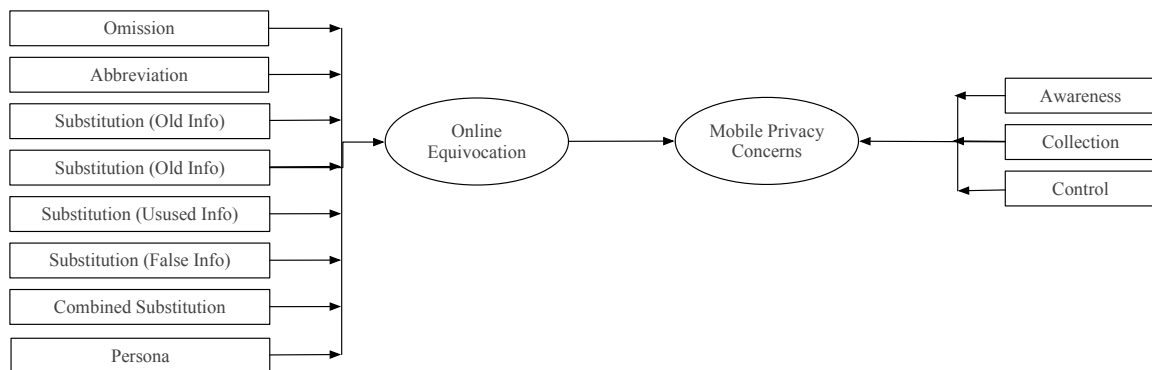
**Table 26**

Outer Loadings for Mobile Privacy Concerns Measures

	<b>Awareness</b>	<b>Collection</b>	<b>Control</b>
<b>Awareness 1</b>	0.752		
<b>Awareness 2</b>	0.724		
<b>Awareness 3</b>	0.776		
<b>Awareness 4</b>	0.808		
<b>Awareness 5</b>	0.817		
<b>Awareness 6</b>	0.881		
<b>Awareness 7</b>	0.825		
<b>Awareness 8</b>	0.822		
<b>Awareness 9</b>	0.838		
<b>Awareness 10</b>	0.835		
<b>Collection 1</b>		0.823	
<b>Collection 2</b>		0.790	
<b>Collection 3</b>		0.774	
<b>Collection 4</b>		0.818	
<b>Collection 5</b>		0.831	
<b>Collection 6</b>		0.720	
<b>Collection 7</b>		0.695	
<b>Collection 8</b>		0.698	
<b>Control 1</b>			0.785
<b>Control 2</b>			0.741
<b>Control 3</b>			0.856
<b>Control 4</b>			0.825
<b>Control 5</b>			0.714
<b>Control 6</b>			0.810
<b>Control 7</b>			0.646

To achieve a higher-order construct, I use a repeated indicators approach as outlined by Hair, Sarstedt, Ringle, and Gudergan (2017, p. 48). In the repeated indicators approach, the indicators for the lower-order constructs are reused for the higher-order construct (Hair et al., 2017). The PLS algorithm is used to generate the latent variable

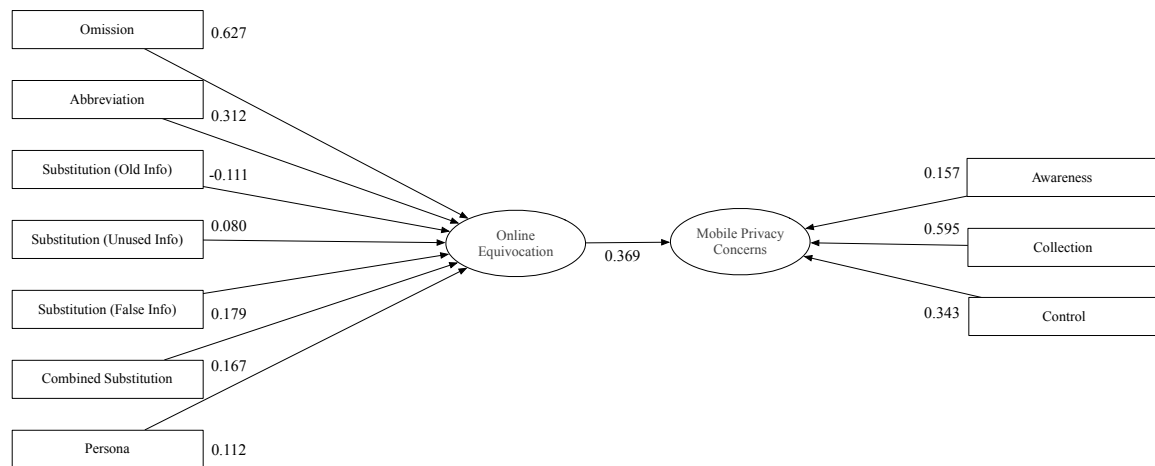
scores (weights), which are used to build the final higher-order model (Agarwal, & Karahanna, 2000; Hair et al., 2017). Using this process, I was able to transform a multidimensional model into a unidimensional model (Hair et al., 2017). The final higher order model is outlined in Figure 7.



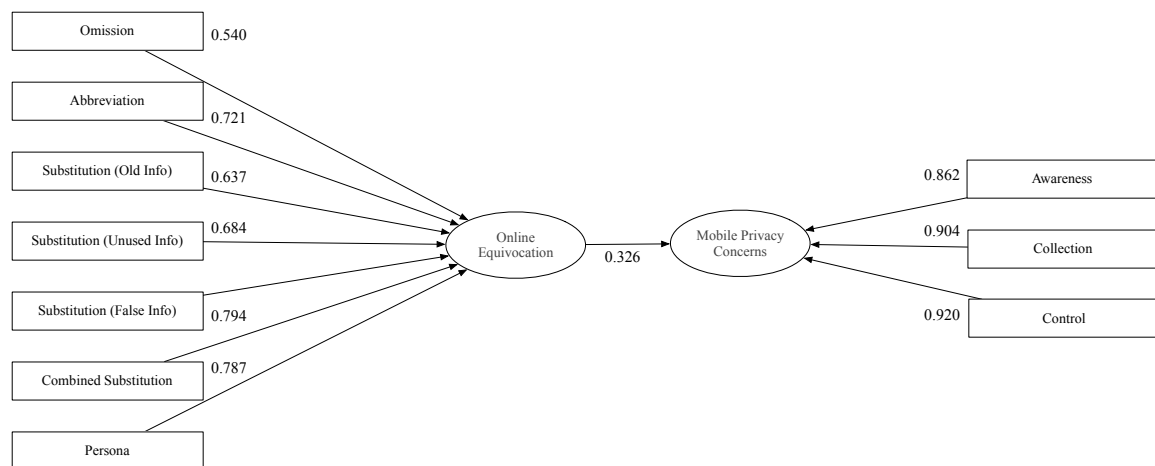
**Figure 7. High Order Unidimensional Model**

Examining the path weights for online equivocation (see Figure 9), we can see that the weights around substitution are not significant, but other factors in this formative construct are significant, which is enough to support convergent validity (Hair et al., 2016; Hair et al., 2017). One factor, the substitution of old information, has a negative sign, which likely suppresses the other variable correlations; it is not evident how it affects the overall construct of online equivocation (Cenfetelli, & Basselier, 2009). To further examine convergent validity, a redundancy analysis is executed by switching the indicators from formative to reflective. Cenfetelli and Basselier (2009) stated that if the results are similar or better, it means that the constructs likely have convergent validity (see Figures 8 and 9). Last, regarding discriminant validity, in this model, we have one

independent variable; because it is the only independent variable, it is statistically independent and supports discriminant validity (Straub, Boudreau, & Gefen, 2004).



**Figure 8. High Order Unidimensional Model (Formative Path Coefficients)**



**Figure 9. High Order Unidimensional Model (Reflective Path Coefficients)**

In addition, a test for common method bias was conducted using a method developed by Kock (2015). Kock's (2015) method evaluates the inner VIFs by running the model with all the latent variables pointing to the same latent variable, repeating for every latent variable in the model. The PLS-SEM algorithm is computed examining the

factors and the resulting inner VIFs. If the VIFs are under 3.3, there is no contamination in the common method bias. The results show no common method bias contamination in the model (see Table 27; Kock, 2015).

The final higher-order model was analyzed using PLS-SEM based on SmartPLS 3.2 (Hair et al., 2011; Ringle, Wende, & Will, 2005), a tool requiring minimum

**Table 27**

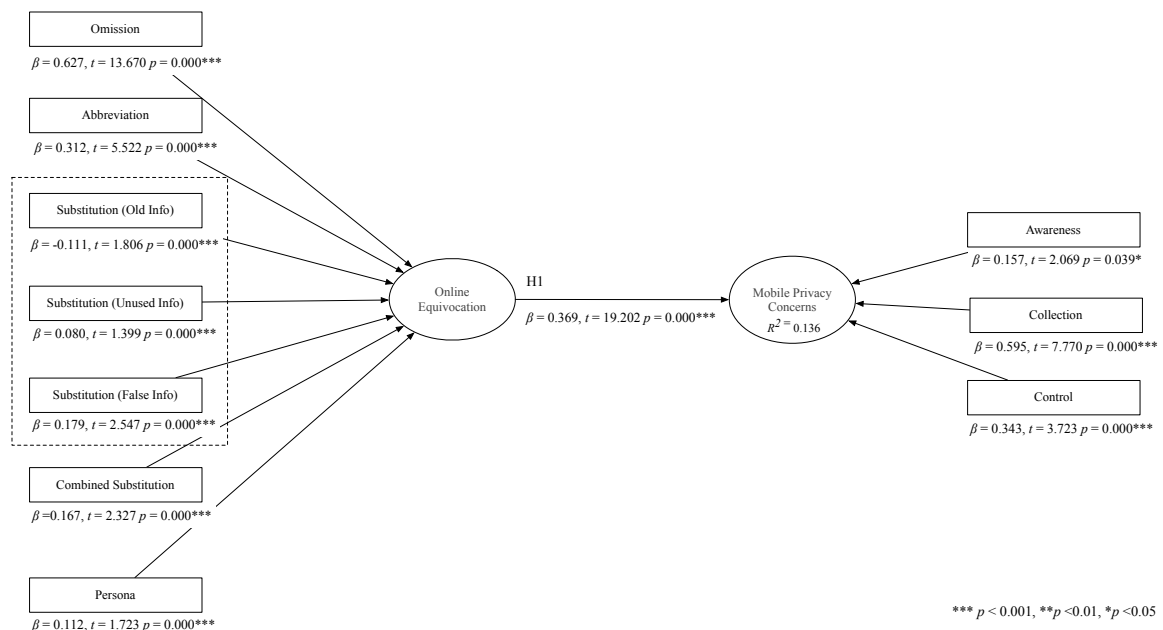
*Common Method Bias Measures. Examining collinearity of inner VIFs for values under*

	<b>O</b>	<b>A</b>	<b>SO</b>	<b>SU</b>	<b>SF</b>	<b>CS</b>	<b>AP</b>	<b>AW</b>	<b>CO</b>	<b>CR</b>
<b>O</b>		1.209	1.237	1.194	1.243	1.252	1.245	1.252	1.249	1.244
<b>A</b>	1.471		1.472	1.506	1.504	1.5	1.524	1.524	1.523	1.523
<b>SO</b>	1.703	1.665		1.697	1.713	1.53	1.722	1.723	1.723	1.724
<b>SU</b>	1.397	1.447	1.443		1.456	1.459	1.434	1.465	1.464	1.465
<b>SF</b>	2.342	2.328	2.345	2.345		2.09	2.07	2.359	2.358	2.359
<b>CS</b>	2.564	2.523	2.276	2.553	2.271		2.384	2.564	2.563	2.564
<b>AP</b>	1.987	1.999	1.997	1.956	1.754	1.859		1.999	1.997	1.999
<b>AW</b>	2.179	2.179	2.18	2.18	2.179	2.179	2.18		2.09	1.706
<b>CO</b>	2.471	2.476	2.477	2.476	2.477	2.477	2.476	2.376		1.784
<b>CR</b>	2.974	2.993	2.995	2.994	2.994	2.995	2.995	2.344	2.155	

(O) Omission; (A) Abbreviation; (SO) Substitution (Old Info); (SU) Substitution (Unused Info); (SF) Substitution (False Info); (CS) Combined Substitution; (AP) Alternative Persona; (AW) Awareness; (CO) Collection; (CR) Control.

restrictions on measure scales that is useful to model latent variables under conditions of nonnormality (Tenenhaus, Vinzi, Chatelin, & Lauro, 2005). I also chose PLS-SEM based on its ability to build higher-order constructs for formative models (Chin, Marcolin, & Newsted, 2003; Fornell, & Bookstein, 1982).

Figure 10 summarizes the hypothesis testing without the moderating effect of the mobile disclosure context. The study analyzed the collected surveys using the PLS-SEM approach. The path coefficients (betas:  $\beta$ s) are indicated on the paths between constructs along with the  $t$ -statistics and significance estimated using a PLS-SEM bootstrap technique featuring 1,000 sub-samples. The explanatory power of the model is assessed through the R-squared score (i.e., the amount of



**Figure 10. High Order Unidimensional Model (Empirical Study Results)**

variance accounted for in the model) and the latent variable paths. The final weights for the subcontracts, online equivocation, and mobile privacy concerns are interpreted as if there were  $\beta$ s in a regression (Diamantopoulos, 2011).

The empirical results show that online equivocation was associated with mobile privacy concerns for the participants ( $\beta = 0.369, t = 19.202, p = 0.000$ ; see Table 28).

Online equivocation measure statistics show omission with online equivocation ( $\beta =$

0.627,  $t = 13.670$ ,  $p = 0.000$ ) and abbreviation with online equivocation ( $\beta = 0.312$ ,  $t = 5.522$ ,  $p = 0.000$ ), as well as substitution of old information ( $\beta = -0.111$ ,  $t = 1.806$ ,  $p = 0.000$ ); substitution of unused information ( $\beta = 0.080$ ,  $t = 1.399$ ,  $p = 0.000$ ); and substitution of false information ( $\beta = 0.179$ ,  $t = 2.547$ ,  $p = 0.000$ ). Combined substitution shows ( $\beta = 0.167$ ,  $t = 2.327$ ,  $p = 0.000$ ) and creation of an alternate persona ( $\beta = 0.112$ ,  $t = 1.723$ ,  $p = 0.000$ ; see Table 29). The overall results show that omission dominates as a method of online equivocation, followed by abbreviation. The remaining measures show smaller effects with the exception of substitution, which has no effect. Mobile privacy concerns exhibit for awareness ( $\beta = 0.157$ ,  $t = 2.069$ ,  $p = 0.039$ ), collection ( $\beta = 0.595$ ,  $t = 7.770$ ,  $p = 0.000$ ), and concern ( $\beta = 0.343$ ,  $t = 3.723$ ,  $p = 0.000$ ; see Table 30).

**Table 28**

*Summary of Path Coefficients and Results. Significant results in bold.*

<b>Relationship</b>	<b><math>\beta</math></b>	<b><math>t</math></b>	<b><math>p</math></b>
Online Equivocation -> Mobile Privacy Concerns	0.369	<b>19.202</b>	<b>0.000</b>

**Table 29**

*Summary of Online Equivocation Measure Relevance and Significance*

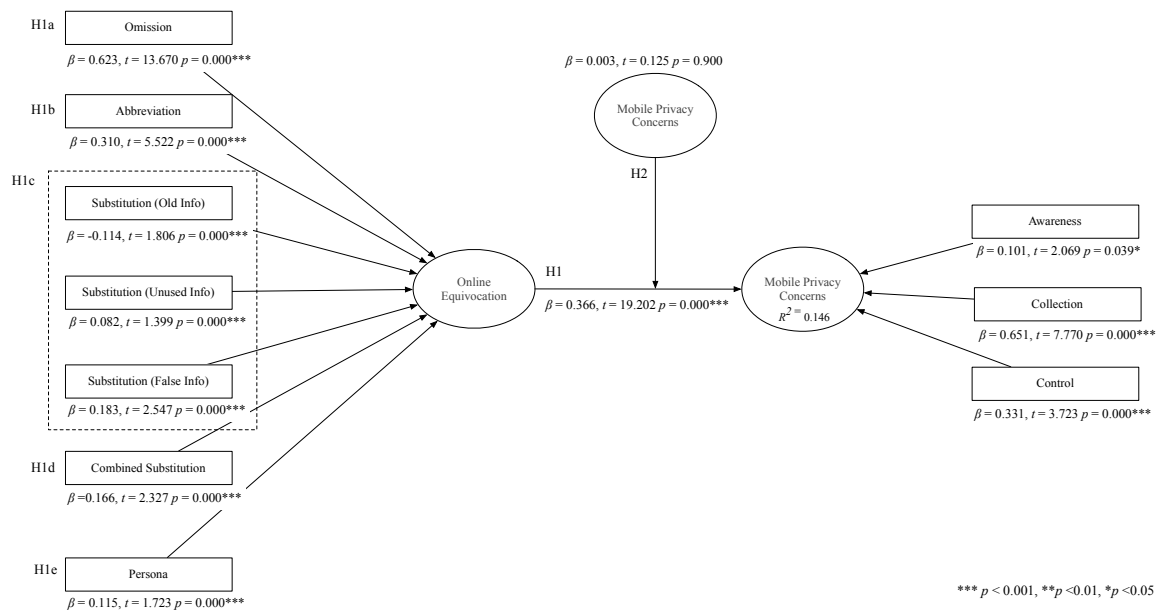
<b>Online Equivocation Measure</b>	<b><math>\beta</math></b>	<b><math>t</math></b>	<b><math>p</math></b>
Omission	0.627	<b>13.670</b>	<b>0.000</b>
Abbreviation	0.312	<b>5.522</b>	<b>0.000</b>
Substitution (Old Information)	-0.111	1.806	<b>0.000</b>
Substitution (Unused Information)	0.080	1.399	<b>0.000</b>
Substitution (False Information)	0.179	<b>2.547</b>	<b>0.000</b>
Combined Substitution (False Information)	0.167	<b>2.327</b>	<b>0.000</b>
Alternative Persona (False person)	0.112	1.723	<b>0.000</b>

**Table 30**

*Summary of Mobile Privacy Concerns Measure Relevance and Significance*

Mobile Privacy Concerns	$\beta$	$t$	$p$
Awareness	0.157	<b>2.069</b>	<b>0.039</b>
Collection	0.595	<b>7.770</b>	<b>0.000</b>
Control	0.343	<b>3.723</b>	<b>0.000</b>

Figure 11 shows the higher-order unidimensional model with the moderating effect of mobile disclosure context. To measure the moderating effect, I used the dummy variables to represent each of the seven mobile disclosure context scenarios and leveraged the higher-order model with the moderating effect capability in PLS-SEM (Chin et al., 2003; Hair et al., 2017; Henseler, & Chin, 2010; Henseler, Fassott, Dijkstra, & Wilson, 2012; Rigdon, Ringle, & Sarstedt, 2010; Toe, Tan, Ooi, & Lin, 2015). This



**Figure 11. High Order Unidimensional Model with Moderating Effect (Empirical Study Results)**

method uses a two-stage calculation method, standardized product term generation, and an automatic weighting mode (not mode b). Overall, the seven disclosure contexts had no significant effect in this model ( $\beta = 0.003$ ,  $t = 0.125$ ,  $p = 0.009$ ; see Figure 12). A separate PLS-SEM moderating effect model was run for each individual mobile disclosure context as well with no scenario showing a significant effect (see Table 31).

**Table 31**

*Path Coefficients of Mobile Disclosure Context (Scenarios) as Moderators of Mobile Privacy Concerns*

<b>Mobile Disclosure Context</b>	<b><math>\beta</math></b>	<b><math>t</math></b>	<b><math>p</math></b>
<b>Social Networking</b>	-0.009	0.440	0.660
<b>Photo &amp; video sharing</b>	-0.002	0.110	0.913
<b>Music listening</b>	0.009	0.380	0.704
<b>Productivity tools</b>	0.017	0.775	0.439
<b>Transportation</b>	-0.005	0.210	0.834
<b>Health &amp; fitness</b>	0.003	0.152	0.879
<b>Financial management</b>	-0.015	0.800	0.424

The empirical results support hypotheses H1, H1a, H1b, H1d and H1e. Substitution (H1c) is not supported in affecting mobile privacy concerns; in addition, there is no support for H2 (see Table 32).

**Table 32**

<i>Summary of Hypotheses Tested</i>		<b>Path</b>	<b>Hypothesis Support</b>
<b>H1</b>	The level of online equivocation affects the level of perceived mobile privacy concerns	Online Equivocation -> Mobile Privacy Concerns	Supported
<b>H1a</b>	The practice of omission, the leaving out of optional personal information in mobile applications, affects the perceived level of mobile privacy concerns	Omission	Supported
<b>H1b</b>	The practice of abbreviation, the limiting of personal information in mobile applications, affects the perceived level of mobile privacy concerns	Abbreviation	Supported
<b>H1c</b>	The practice of substitution, the offering of inoperable data as a substitute for truth in mobile applications, affects the perceived level of mobile privacy concerns	Substitution	Not Supported
<b>H1d</b>	The practice of combined substitution, the offering one or more inoperable data values in unison as a substitute for truth in mobile applications, affects the perceived level of mobile privacy concerns	Combined Substitution	Supported
<b>H1e</b>	The practice of developing an alternate persona, a disguised identity, in mobile applications, affects the perceived level of mobile privacy concerns	Alternative Persona	Supported
<b>H2</b>	The mobile disclosure context will moderate the relationship between the level of online equivocation and the level of mobile privacy concerns	Moderating Effect: Mobile Disclosure Context -> Mobile Privacy Concerns	Not Supported

Additional data collected allowed for examination of and insights into omission.

Subjects were asked how likely they would be to omit optional data, and the response confirmed that, if allowed, individuals leave items blank (see Table 33 and Figure 12).

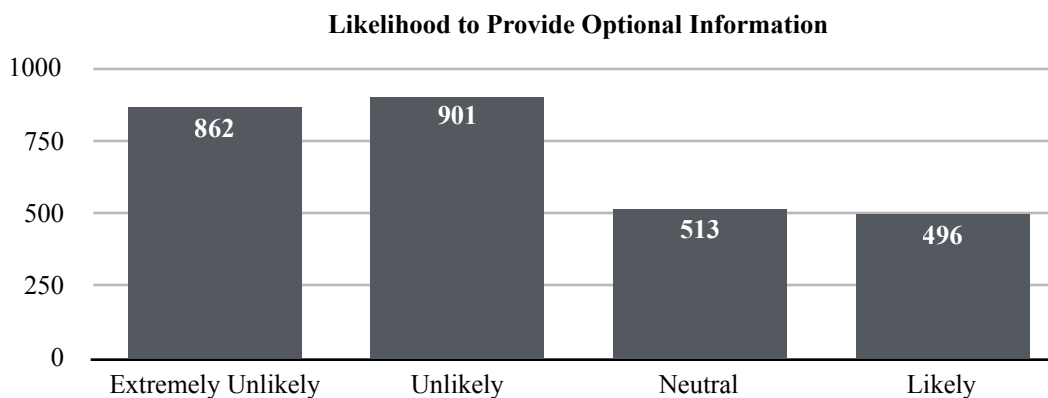
In regard to scenarios, subjects were asked to rank the seven scenarios in order of privacy concerns, from one (1), being the highest concern, to seven (7), being the least concern. As expected, individuals ranked the scenarios in the following order: (1) social networking, (2) photo sharing, (3) music listening, (4) productivity

tools, (5) transportation, (6) health and fitness, and (7) financial management. The fact that financial management posed the least privacy concerns may be a reflection of

**Table 33**

*Likelihood to Offer Optional Information. Subject to offer optional information when asked, “Most of the time, providing personal information is required to gain access to the mobile aPp. When the personal information is optional, how likely are you to provide information that is fully accurate and complete?”*

Provide Optional Information	Count	Percentage of Total
Extremely Unlikely	862	31%
Unlikely	901	33%
Neutral	513	19%
Likely	496	18%



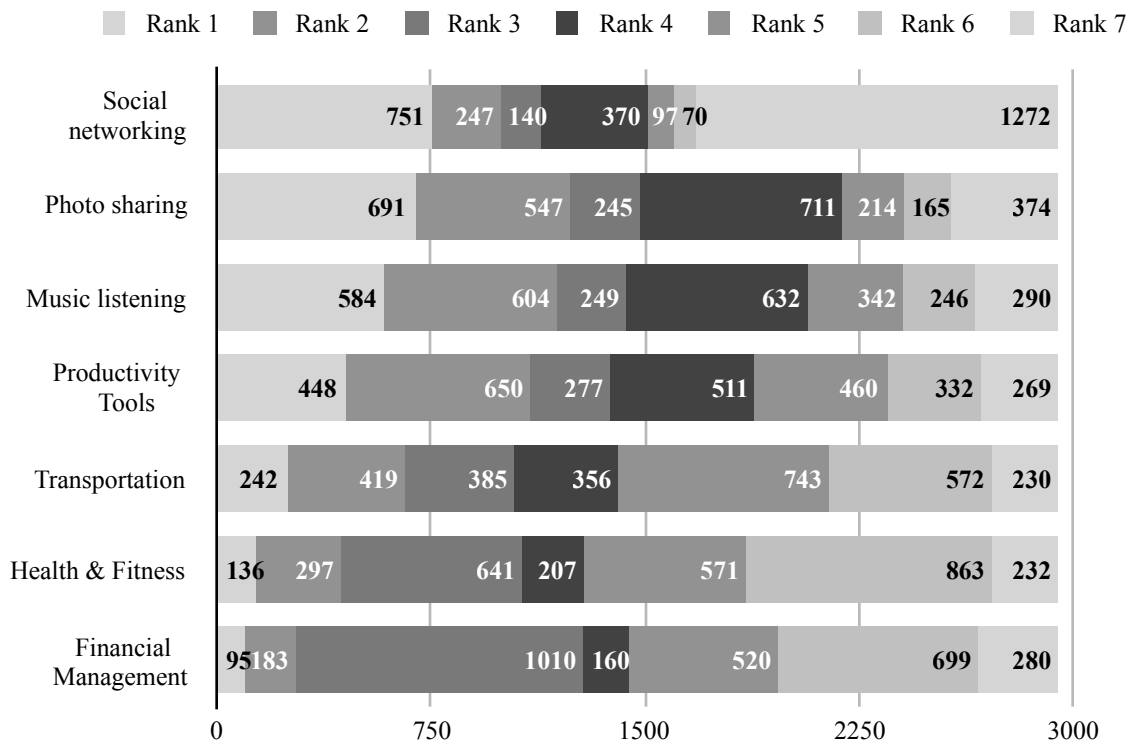
**Figure 12. Likelihood to Provide Information.**

regulatory restrictions that most individuals understand that banks and financial institutions and technology service providers must adhere to. Social networking, ranked number one for privacy concerns, also exhibited a dichotomy of being the least privacy concerned. Individuals are on the opposite side of the spectrum regarding social networking and either are very privacy concerned or the reverse (see Table 34 and Figure 13).

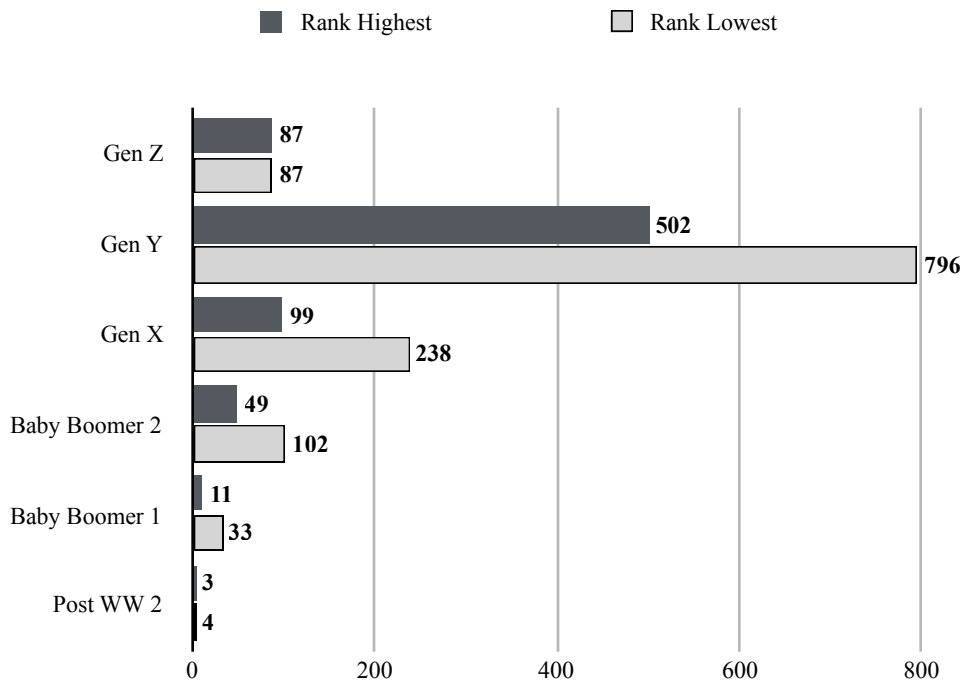
**Table 34**

*Subject Responses on Scenario Ranking.*

	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5	Rank 6	Rank 7
<b>Social networking</b>	751	247	140	370	97	70	1272
<b>Photo sharing</b>	691	547	245	711	214	165	374
<b>Music listening</b>	584	604	249	632	342	246	290
<b>Productivity Tools</b>	448	650	277	511	460	332	269
<b>Transportation</b>	242	419	385	356	743	572	230
<b>Health &amp; Fitness</b>	136	297	641	207	571	863	232
<b>Financial Management</b>	95	183	1010	160	520	699	280



**Figure 13. Stacked Bar Chart Illustration of Ranking**



**Figure 14. Social Networking Ranking from Highest to Lowest in Comparison**

A closer examination of the dichotomy of privacy concern ranking in the social networking scenario shows a tendency across age groups to be more often less concerned (see Figure 14). However, some aspects of these individuals other than age may influence their viewpoints on privacy concerns in social networking. Regardless, there is a wide variety of sentiment on which application scenarios cause individuals to feel concerned, and this small glimpse is worth examining in future research.

## Discussion

The study demonstrates that online equivocation providing in place of honest, accurate data is a phenomenon affecting individuals' privacy concerns. The intention to offer inaccurate personal information in exchange for the benefit of using mobile applications is supported, demonstrating that a privacy calculus is exercised in the disclosure decision (Culnan, & Armstrong, 1999; Dinev, & Hart, 2006; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990). This online equivocation behavior challenges the theory of the privacy paradox in that individuals may still share information but falsely. Individuals' expression of privacy concern is validated when they choose inaccurate personal disclosure over honesty (Acquisti, 2005; Barnes, 2006; Debatin et al., 2009).

The study also indicates that even though providing inaccurate information online has been shown in previous studies to be a method for lowering privacy concerns, we uncovered that it can increase mobile privacy concerns. For every increase in online equivocation, a subsequent increase in mobile privacy concerns manifests. This phenomenon deserves further study to investigate whether the rise could be a result of increased anxiety when individuals provide false information online. It could also be the result of the sheer number of possible applications that individuals engage with and tracking the various falsehoods they apply. As shown in Table 21, over 50% of respondents estimated they engaged with more than 100 applications. Last, the fact that many applications combined data from more than one source to provide the individual

with personalized services could complicate the individuals' view of their mobile privacy concerns. If one application has inaccurate data and the another does not, what is the result for the individual's application account? Does it negatively affect benefits, or could it expose them as liars?

Of the five online equivocation strategies presented, omission was the most prominent in increasing mobile privacy concerns, followed by abbreviation. The other methods, such as combined substitution and alternative persona, increased at a lesser effect. Perhaps individuals are troubled over omitting information that could be essential in using mobile applications or by using a method such as combined substitution or an alternative persona requires them to remember a complex combination of inaccurate information, which is hard to reproduce quickly. Tracking these types of detail consistently may increase individuals' anxiety and their overall privacy concern. Substitution, specifically providing old, inaccurate information, did not have an effect on mobile privacy concerns. It could be that substitution is the only online equivocation method used that either had no effect on mobile privacy concerns or reduced them. Additional research could help to expose those nuances.

Surprisingly, the effect of mobile disclosure context had no impact on individuals' mobile privacy concerns about online equivocation, which tells us that individuals were not influenced by the type of application in regard to providing inaccurate information to protect themselves. They did so even-handedly regardless of which application they were using. There were some nuances in the viewpoint on the applications themselves in regard to privacy concerns, but not enough to change behavior or the subsequent concern.

In summary, the use of online equivocation to provide inaccurate information in place of accurate data provides further support for privacy calculus theory in that individuals seek to reduce costs when sharing personal information online (Culnan, & Armstrong, 1999; Dinev, & Hart, 2006; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990). Online equivocation could offer an explanation for the privacy paradox where individuals engage in personal information sharing regardless of privacy concerns; perhaps they are sharing inaccurate data, which allows them to participate and reduce those concerns in general (Acquisti, 2005; Barnes, 2006; Debatin et al., 2009). The expression of privacy concern may remain the same, but the engagement in sharing may be masked by the fact individuals are providing inaccurate personal information. Furthermore, the uncovered insight implies that some methods of online equivocation actually increase mobile privacy concerns.

Additionally, the new instrument created for measuring mobile privacy concerns included additional factors to measure location awareness, data sharing across applications, off-device (cloud) storage, always online behavior, unique device identifiers, and collection of biometric data (Liccardi et al., 2014; Xu, 2007; Xu, 2012b). It performed well, making an overall contribution to future studies of this construct. The noted exception involves factors around privacy policies and awareness. Many studies have addressed individual awareness or unawareness of privacy policies (Capistrano, & Chen, 2015; Milne, & Culnan, 2004). What is interesting is the poor performance of these measures, specifically indicating not only that people do not read them but that people may hold policies in little regard. This aspect could lead to further investigation of

privacy policy awareness in regard to mobile privacy concerns and whether they are a measurable factor now and in the future.

## Conclusion

The objective of this study was to employ previous findings regarding online equivocation in relation to privacy concerns in mobile computing. The study demonstrated that specific methods of online equivocation affect mobile privacy concerns by increasing them. Online equivocation is used as a practice in mobile computing regardless of the type of application scenario, particularly with applications requesting data sharing in return for application use. The categorization of online equivocation was validated as a result of the analysis.

The study also introduced new measures to expand the measurement of privacy concerns for mobile computing, which maintained a high degree of validity using those new measures. This new updated instrument and measures can be leveraged by subsequent studies focused on mobile computing and privacy concerns.

The research also contributes to privacy calculus theory, demonstrating that individuals make judgements regarding disclosure and modify the value of data exchange in a cost-benefit analysis, thus maximizing their benefit and reducing their overall exposure costs. In addition, the results may pose new questions regarding the privacy paradox theory in which the paradox could be explained partially on the application of online equivocation. This aspect could be explored in future research regarding the privacy paradox.

Finally, the study contributes to a framework for examining mobile computing behavior through scenario research. Although the application scenarios proposed are

relevant for today's analysis, the process of determining scenarios and using them in mobile computing research is useful for further research.

### **Managerial Insights**

Big data has been widely acclaimed as a competitive factor in giving businesses and governments insights into people's online behaviors. The ability of business to reach new customers and develop long-standing relationships is the core of any solid business strategy. In today's online marketplace, knowing the customer is a competitive requirement. Business thought leaders expound that the only sustainable advantage for businesses in the future is successful big data strategies that cultivate customer engagement (Manyika, Chui, Brown, Bughin, Dobbs, Roxburgh, & Byers, 2001).

Business intelligence around using data in strategic ways is a key focus for most organizations to gain an advantage over competitors. Specifically, businesses want to use data to help them find new customers, understand customer needs and increase their value to customers (Experian, 2016; Liang, Saraf, Hu, & Xue, 2007; Moon, 2000). Companies that invest in big data reap big rewards from increased sales. Studies have shown that companies gain a 75% increase in sales using big data for targeted marketing, targeted social media, loyalty, and promotion optimization, as well as gaining benefits from selling the use of the transaction data with third parties (Conroy, Milano, Narula, & Singhal, 2014). Besides those benefits, big data can affect operational efficiency, customer engagement, and successful decision-making (Experian, 2013; Newman, 2017).

Today's organizations are investing in data quality, specifically around contact data as a priority with more than 88% of business reporting big data strategies focused on contact information (Experian, 2016). Contact data are core to supporting the

business's ability to communicate accurately with customers. If contact data are inaccurate, employees spend unnecessary time and resources trying to reach customers as well as incorrectly marketing to them; essentially, if the input is wrong, so will be the output (Experian, 2016; Kuran, 1995; Wirth, & Sweet, 2017).

Despite the commitment to invest in data quality, companies find their data filled with errors. It is reported that over 60% of customer records are incomplete, outdated, or contain duplicate data (Experian, 2016). When contact data are inaccurate, it wastes business investments, can damage customer relationships, and can affect brand perceptions (Experian, 2016; Lucker, Hogan, & Bischoff, 2017). Consider the example in 2017 where Gillette, working to reclaim the male market for their products that they had been losing for years to online competitors, sent a promotional Gillette razor to what they thought was a young adult male population but proved to be female. The event was widely mentioned on Twitter and other social media venues, with Gillette responding that in collecting shipping information, mishaps happen (Green, 2017; Lucker, 2017). A single demographic was needed, and Gillette had it wrong. Inaccurate contact data results in poor targeting, wrong-person, wrong-time delivery and a loss of brand connection (Lucker, 2017). Over half of consumers report that over 50% of their demographic information is wrong, including age, gender, income, and marital status. Mistakes made due to inaccurate contact data can cost organizations millions of dollars, which when estimated overall the potential poorly managed contact data across the Internet could result in a loss of billions every year (Horne et al., 2007; Strong et al., 1997).

Inaccuracy of data is caused by several factors, such as the methods used by companies to gather data, ways to manage that data internally and interweave it with other sources, and the lack of opportunity for individuals to correct simple errors. Beyond these problems, the main reason that consumers do not correctly share information or bother to fix errors is privacy concerns (Lucker, 2017; Norberg, 2007). Individuals have serious concerns over the erosion of personal privacy (Cavoukian, & Hamilton, 2002; Singer, 2015). Multiple surveys over the last few years have consistently shown that a high percentage of individuals are concerned about sharing their personal information, especially when computing on mobile devices that allow companies to use the uniqueness of a mobile device to gather details of the individual's personal behaviors (Conroy et al., 2014). These concerns transcend gender, nationality, and personality types, and companies are searching for how to manage the need for personal information to drive their programs and the lack of desire of individuals to supply it (Chahal, 2016). More than half the consumers surveyed on this topic have stated that these concerns influence their decisions on the applications they download and the data they share (Chahal, 2016). In addition, as demonstrated in this study, individuals use online equivocation to control the distribution and collection of personal information (Hiller, & Cohen, 2002; Lwin 2004). When individuals have high concerns for their personal privacy, offering inaccurate information allows them individuals to engage in the application benefits (Cavoukian, & Hamilton, 2002; Hoffman et al., 1999; Lwin, & Williams, 2003; Pavlou, Liang, & Xue, 2007). The disconcerting results are inaccurate data that create costly errors in customer databases and overall data

quality, thus propagating to other company resources and jeopardizing company business strategies and brand reputation (Experian, 2016; Horne et al., 2007; Lucker, 2017; Wirtz, & Lwin, 2009).

Oddly, despite these evident findings regarding data quality, particularly regarding about contact data and simple demographics, companies still do not perceive that consumer privacy and security are essential. A Deloitte study conducted in 2014 (Conroy et al., 2014) about consumer attitudes compared with executives' regarding data privacy and security demonstrated a significant gap in perspectives. The study showed that consumers have a perceptive understanding of the risks of data exposure and have high expectations from companies. There are three critical themes: consumers seek to gain control over their information, desire understandable policies, and require transparency regarding how information is used. In all three themes, a significant gap existed between consumer expectations and what executives felt was important. Executives fell short by large margins ranging from 12-32% regarding their perceptions compared with consumers' expectations (Conroy et al., 2014). These results make it evident that business leaders still do not understand what motivates consumers share truthful personal information.

So the question of how to obtain accurate, quality data remains. How can companies help customers feel less concerned over their privacy and make them willing to share correct contact and personal details with companies? First, executives must view privacy from the consumer's perspective to provide meaningful and understandable data collection approaches. These approaches start with providing

features that address the needs of the customer, encouraging information sharing (Awad, & Krishnan, 2006; Conroy et al., 2014). If companies take the approach that considers that consumers' personal information is valuable to them and offer a commensurate value in return for it, they will be able to build a positive relationship.

Companies also need to take the approach of transparency regarding the data they collect instead of keeping consumers in the dark and quietly collecting data with no immediate use thinking that it will be valuable someday (Morey et al., 2015). Many application developers take a formula approach to data collection design, replicating methods they see other applications implement. If customers understand what personal information is being collected and how it benefits them within policies that are clear and easy to interpret, it fosters a foundation of trust (Conroy et al., 2014). Transparency includes a concise accounting of why the personal information is being shared with selected third parties. If company strategies can avoid sharing customer information with third parties and keep it within the company itself, it will go a long way in establishing customer trust (Morey et al., 2015). As Julia Porter, *Guardian* News and Media Director stated, "If we don't explain to customers and readers why we want to use data and what we are going to do with it, there is no reason why they should share it" (Chahal, 2016, p. 1). If both the company and consumer benefit from personal information collection, their interests are aligned, and it cultivates trust (Morey et al., 2015).

Many business leaders will argue to give customers control to allow them to easily edit and delete their own information (Bahl, 2016). A friend of mine recently

mentioned that when signed up for a new, social media account, she used a false birth date because she was unsure about how the information would be used. Months later, she regretted the inaccurate decision because everyone she knows wishes her happy birthday on the wrong day and month. If she could go back and fix the one error, she as well as the social media service provider would benefit. However, at present, they both lose out.

In general, if customers do not understand how their personal information will be used and are not offered personal control, they will be less likely to share it and even more unwilling to participate at all in ensuring it is correct (Lucker, 2017). In the age of information sharing, companies strive to achieve consumers' understanding the trade of data for service, resolving the tension to share data through clarity on both sides. When companies are clear with customers on the use of their personal information and the exchange feels like a fair trade, consumer response is more likely to be honest (Morey et al., 2015).

The online world has been self-regulated for decades with only broad regulation that defined personal information in murky terms and protected general fairness in commerce both online and offline. These regulations and lack of significant legislation regarding the collection of consumer data have made it hard for consumers to argue for their rights against companies that aggressively collect personal information knowingly or unknowingly. However, a wave of change is about to ripple through the online world with the Global Data Protection Regulation (GDPR) which is expected to go into effect in May 2018. The GDPR is authored by the European Union whose progressive views

on digital development, the digital economy, and protecting citizens' rights. GDPR is about to affect most international and domestic concerns with a regulation that leans in favor of the consumer (Intersoft Consulting, 2017; IT Governance, 2018). GDPR outlines the recommendations to reduce online equivocation: transparency, fair data collection, use for legitimate reasons, control over data, the ability to fix errors, and the right to delete data. The focus of GDPR on transparency gives citizen consumers the right to expect clear and easily understandable policies about data collection and use. Furthermore, it underscores the need for companies to minimize the data they collect, ensuring that only adequate and relevant data are collected for specific purposes. The regulation protects the citizen consumers' rights to make corrections to inaccurate information within specified time frames, and consumers also have the right to demand that all the data collected about them be delivered in readable formats. In addition, for the first time, the regulation supports citizen's right to be forgotten, in that if they wish all their data to be deleted from companies systems, such companies must comply. Interestingly, the definition of *personal information* is also broadened to include categorical information such as cultural information, health information, economic information, and even feelings. Any data that can be tied back to the individual, even pseudonymous identification values, is included.

This regulation will be monumental in affecting not just the European Union and all companies doing business within it but also any company that holds data on any European citizen throughout the world (Intersoft Consulting, 2017; IT Governance, 2018). Essentially, this regulation, although put forth by the European Union, will be

applied in every country where European citizens live and use these types of services. The largest companies among us have already announced their support for this regulation and are making big changes to comply; companies like Facebook that do not allow account holders to delete an account but only deactivate it have recently announced they will be providing users control over their data and the ability to delete their accounts globally (Guynn, 2018).

As GDPR is applied worldwide, it will begin to influence other domestic regulation, hopefully for the better. The combination of companies looking for ways to increase the quality of their data and ultimately the effectiveness of their strategies aligns with the citizen sentiment and public policy that are emerging globally. This study points out the discrepancy regarding the accuracy of personal information that individuals share and underscores the trends in global government responses to citizens' concerns. The decades of self-regulation may slowly see their demise unless companies address privacy and security concerns as part of their big data strategies, including alignment with emerging regulations such as GDPR. Governments and business do not want to turn back the clock on technology adoptions, in particular those that leverage personal information. A balance between regulation and company response to consumer concerns will help in ensuring continued progress (Newman, 2017). Table 36 presents managerial recommendations to encourage consumers to provide accurate responses and to increase the overall value of business data.

**Table 36***Managerial Recommendations to Address Online Equivocation*

<b>Recommendation</b>
<b>1</b> Keep the customers viewpoint regarding sharing personal information in mind.
<b>2</b> Consistently ask for permission to collect customer data.
<b>3</b> Provide a fair exchange of valuable information for benefits.
<b>4</b> Be transparent about why the data is collected, how it is going to be used, and why that benefits the customer. This includes any sharing with third parties; being transparent about data sharing with third parties.
<b>5</b> Provide customers control over their data so they can easily correct errors, remove data or even delete their account all together.
<b>6</b> Provide a method to allow customers to request all the data that the company stores on them in easy to read format.
<b>7</b> Provide clear and easy to understand policies regarding privacy and security of customer data which is easy to access even from a mobile phone.
<b>8</b> Consider not sharing customer data with third parties, keeping customer data private as part of the ongoing customer relationship.

### **Contribution**

This study drew upon past explorations of deception and privacy concerns along with new qualitative and quantitative research to form a definition of online equivocation, which is the process of providing inaccurate data in place of accurate data online. This defines the fundamental strategies employed by individuals to offer inaccurate personal information in place of accurate responses within mobile computing. Building upon the theory of privacy calculus, I conceptualized the effect of online equivocation on mobile privacy concerns. When individuals feel privacy concerns using mobile applications, they leverage online equivocation to reduce those concerns. This finding provides added support for the theory of privacy calculus, which asserts that individuals conduct a cost-benefit analysis before disclosure that affects their disclosure behavior (Culnan, & Armstrong, 1999; Dinev, & Hart, 2006; Läufer, & Wolfe, 1977; Milne, & Gordon, 1993; Stone, & Stone, 1990). Despite the application of online equivocation to reduce privacy concerns, this study reveals that some methods of online equivocation actually increase mobile privacy concerns. This insight may lead researchers to explore other aspects of individual behavior to understand why certain online equivocation strategies cause individuals to be more concerned about their privacy. The use of online equivocation could have implications on the theory of the privacy paradox which contends that despite an individuals' privacy concerns and their intention not to disclose, they will disclose regardless (Acquisti, 2005; Barnes, 2006; Debatin et al., 2009). Individual disclosure may be false, thereby reducing privacy concerns and still allowing engagement in what seemingly is disclosure online.

The exploration not only contributes to the definition of online equivocation but also addresses previous measurement instruments used to examine privacy concerns, thus extending them to address unique aspects of mobile computing. Also, the analysis process for developing the mobile disclosure context provides a framework for future studies regarding mobile computing. Last, the scenario-based survey exhibits another method for measuring topics regarding privacy concerns in the future. Part of the analysis, an outline of potential solutions to online equivocation, encourages truthful disclosure and increases data quality, which provides a contribution to managerial practice. A framework of possible strategies can provide insights for both industries to guide the development of mobile applications and inform public policy makers regarding future regulatory and legislative strategy.

### **Future Research**

Future research may include expanding understanding of other motivations for engaging in online equivocation, including the reasons individuals may use online equivocation to self-present. This topic could include an examination of the role of the consumer's personality in the likelihood of online equivocation. Also, this study could be extended across national cultures to see whether the cultural viewpoints regarding deception still hold true in an online, mobile world.

It would also be interesting to deepen understanding of what motivates people to create new personas online and the effects of personal disclosure, relationships, and self-esteem, which may lead to new insights in this unique strategy. This may include understanding whether alternative personas are used by people to hide or avoid surveillance, harassment, or discrimination. Also, it would be compelling to describe the different types of alternative personas used online, as well as determine whether individuals have more than one persona for different purposes and why. Other research topics suggested by this study could include exploring the aspects of alternative personas in regard to self-presentation, the need for popularity, and the strategies that compliment self-presentation such as buying "likes" (Dumas et al., 2017; Sass, 2017).

In addition, examining why certain online equivocation strategies such as omission, abbreviation, combined substitution, and alternative persona increase mobile privacy concerns instead of decreasing it would be a next step beyond this finding. A longitudinal study regarding online equivocation may uncover the longer-term effects of

inaccurate data for individuals and businesses.

Because of the low validity of measures around privacy policies, it would be interesting to pursue whether privacy policies make any difference to individuals using mobile devices. Are they found, read, or used in any way in mobile computing? Or, could it be that, in mobile computing, privacy policies are rarely or never examined by application users? Perhaps privacy policies are a dimension no longer worth exploring in the mobile context.

Other aspects to consider would be expanding the mobile disclosure context. Some variation exists between how individuals view applications concerning health and fitness, financial management, and transportation over music listening or photo sharing. In the situation of online equivocation, the mobile disclosure context had no real effect, but are there other circumstances in which the mobile disclosure context could be meaningful?

Last, the privacy paradox may be affected by the phenomenon of online equivocation. Research examining whether online equivocation moderates the privacy paradox would be insightful. Do individuals use online equivocation to exchange the value of data and still engage? Or do they merely value the convenience of mobile applications with their immediate benefit over disclosure regardless of any privacy concern?

## REFERENCES CITED

- Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999, November). Privacy In E-Commerce: Examining User Scenarios And Privacy Preferences. In *Proceedings Of The 1St ACM Conference On Electronic Commerce* (Pp. 1-8). ACM.
- Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (Pp. 21-29). ACM.
- Acquisti, A., & Gross, R. (2006, June). Imagined Communities: Awareness, Information Sharing, And Privacy On The Facebook. In *International Workshop On Privacy Enhancing Technologies* (Pp. 36-58). Springer, Berlin, Heidelberg.
- Acquisti, A., & Grossklags, J. (2004). Privacy Attitudes And Privacy Behavior. In *Economics Of Information Security* (Pp. 165-178). Springer US.
- Acquisti, A., & Grossklags, J. (2005). Privacy And Rationality In Individual Decision Making. *IEEE Security & Privacy*, 3(1), 26-33.
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: a process-oriented perspective. *Communications of the ACM*, 48(10), 83-90.
- Afthanorhan, W. M. A. B. W. (2014). Hierarchical component using reflective-formative measurement model in partial least square structural equation modeling (Pls-Sem). *International Journal of Mathematics*, 2(2), 33-49.
- Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 665-694.
- Alge, B. J. (2001). Effects Of Computer Surveillance On Perceptions Of Privacy And Procedural Justice. *Journal Of Applied Psychology*, 86(4), 797.
- Almeryda, M., & Shakespeare, W. (2000). William Shakespeare's Hamlet. Faber & Faber.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., & Agarwal, Y. (2015, April). Your Location Has Been Shared 5,398 Times! A Field Study On Mobile Application Privacy Nudging. In *Proceedings Of The 33Rd Annual ACM Conference On Human Factors In Computing Systems* (Pp. 787-796). ACM.

- Aloudat, A., & Michael, K. (2011). Toward The Regulation Of Ubiquitous Mobile Government: A Case Study On Location-Based Emergency Services In Australia. *Electronic Commerce Research*, 11(1), 31-74.
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. ERIC.
- Altman, I. (1977). Privacy Regulation: Culturally Universal Or Culturally Specific? *Journal Of Social Issues*, 33(3), 66-84.
- Angwin, J., & Valentino-Devries, J. (2011, December 13). Apple's iPhones And Google's Androids Send Cellphone Location. *Wall Street Journal*. Retrieved from: <http://Wsj.Com>.
- App Annie (2017, May 1). Application Store Rankings Index. *App Annie*. Retrieved from: <https://Www.Appannie.Com/Dashboard/Home/>
- Argo, J. J., White, K., & Dahl, D. W. (2006). Social comparison theory and deception in the interpersonal exchange of consumption information. *Journal of Consumer Research*, 33(1), 99-108.
- Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of marketing research*, 396-402.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.
- Baarslag, T., Alan, A. T., Gomer, R. C., Liccardi, I., Marreiros, H., & Gerding, E. H. (2016, May). Negotiation As An Interaction Mechanism For Deciding Application Permissions. In *Proceedings Of The 2016 Chi Conference Extended Abstracts On Human Factors In Computing Systems* (Pp. 2012-2019). ACM.
- Bahl, M. (2016). Return on Trust: The New Business Performance Indicators. (Annual Journal Produced by Cognizant). Volume 9, Issue 1.
- Bansal, G., & Gefen, D. (2010). The Impact Of Personal Dispositions On Information Sensitivity, Privacy Concern And Trust In Disclosing Health Information Online. *Decision Support Systems*, 49(2), 138-150.
- Bansal, G., & Zahedi, F. (2008). The Moderating Influence Of Privacy Concern On The Efficacy Of Privacy Assurance Mechanisms For Building Trust: A Multiple-Context Investigation. *ICIS 2008 Proceedings*, 7.

- Barkhuus, L. (2012, May). The Mismeasurement Of Privacy: Using Contextual Integrity To Reconsider Privacy In HCI. *In Proceedings Of The SIG CHI Conference On Human Factors In Computing Systems* (Pp. 367-376). ACM.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9).
- Becker, G. S. (1981). Altruism in the Family and Selfishness in the Market Place. *Economica*, 48(189), 1-15.
- Beinat, E. (2001). Privacy And Location-Based Services: Stating The Policies Clearly. *GeoInformatics*, 4, 14-17.
- Bélanger, F., & Crossler, R. E. (2011). Privacy In The Digital Age: A Review Of Information Privacy Research In Information Systems. *MIS Quarterly*, 35(4), 1017-1042.
- Bentley, A., (2014, September 2). The controversial case for buying ‘false’ social media followers. *The Guardian*. Retrieved from: <https://www.theguardian.com/media/2014/sep/02/the-controversial-case-for-buying-fake-social-media-followers>
- Bentley, A. (2014, Sep 2). The Controversial Case for Buying ‘false’ Social Media Followers. *The Guardian*. Retrieved from <https://www.theguardian.com/media/2014/sep/02/the-controversial-case-for-buying-fake-social-media-followers>.
- Birchmeier, Z., Dietz-Uhler, B., & Stasser, G. (Eds.). (2011). *Strategic Uses Of Social Technology: An Interactive Perspective Of Social Psychology*. Cambridge University Press.
- Bok, S. (1999). *Lying: Moral choice in public and private life*. Vintage.
- Boyd, D. (2008). Facebook's Privacy Trainwreck: Exposure, Invasion, And Social Convergence. *Convergence*, 14(1), 13-20.
- Boyd, D. (2014). *It's Complicated: The Social Lives Of Networked Teens*. Yale University Press.
- Brahim, J. & Martiz, P. (2015). *Big & Fast Data: The Rise Of Insight-Driven Business*. (Industry Report). Capgemini.
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6, 3–5.

- Buller, D. B., & Burgoon, J. K. (1996). Interpersonal Deception Theory. *Communication Theory*, 6(3), 203-242.
- Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, 6(2), 131-158.
- Campbell, A. J. (1997). Relationship Marketing In Consumer Markets: A Comparison Of Managerial And Consumer Attitudes About Information Privacy. *Journal Of Interactive Marketing*, 11(3), 44-57.
- Campbell, J. E., & Carlson, M. (2002). Panopticon. Com: Online Surveillance And The Commodification Of Privacy. *Journal of Broadcasting & Electronic Media*, 46(4), 586-606.
- Capistrano, E. P. S., & Chen, J. V. (2015). Information privacy policies: The effects of policy characteristics and online experience. *Computer Standards & Interfaces*, 42, 24-31.
- Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *CyberPsychology & Behavior*, 9(1), 54-59.
- Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal And Ethical Issues. *Journal of Public Policy & Marketing*, 19(1), 7-19.
- Cavoukian, A., & Hamilton, T. J. (2002). *The Privacy Payoff: How successful businesses build customer trust*. McGraw-Hill Ryerson.
- Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS quarterly*, 689-707.
- Chahal, M., (2016, June 23). Marketers overestimate consumers' attitude to data. *Marketing Week*. Retrieved from: <https://www.marketingweek.com/2016/06/23/marketers-overestimate-consumers-attitude-to-data/>.
- Chandler, J., & Shapiro, D. (2016). Conducting clinical research using crowdsourced convenience samples. *Annual Review of Clinical Psychology*, 12.
- Chellappa, R. K., & Sin, R. G. (2005). Personalization Versus Privacy: An Empirical Examination Of The Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), 181-202.
- Chen, K., & Rea Jr, A. I. (2004). Protecting Personal Information Online: A Survey Of User Privacy Concerns And Control Techniques. *Journal of Computer Information Systems*, 44(4), 85-92.

- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, 295(2), 295-336.
- Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research*, 14(2), 189-217.
- Cohen, J. (1988) *Statistical Power Analysis For The Behavioral Sciences*. Mahwah, NJ: Lawrence Erlbaum.
- Cohen, J. (1992). A power primer. *Psychological bulletin*, 112(1), 155.
- Cohen, S. (1985). *Visions of social control: Crime, punishment and classification* (Pp. 127-143). Cambridge: Polity Press.
- Conroy, P. & Narula, A., (2014, November 13). Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry. *Deloitte Insights*. Retrieved from <https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html>
- Conroy, P., Milano, F., & Narula & Singhal, R. (2014). *Building consumer trust: Protecting personal data in the consumer product industry*. (Industry Report) Deloitte University Press, 13, 1-28.
- Cooney, M., (2016, May 11). Smartphone tracking apps raise security privacy and legality questions. *Network World*. Retrieved from: <https://www.networkworld.com/article/3068627/security/smartphone-tracking-apps-raise-security-privacy-and-legality-questions.html>
- Crawford, V. P. (2003). Lying for strategic advantage: Rational and boundedly rational misrepresentation of intentions. *American Economic Review*, 93(1), 133-149.
- Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 341-363.
- Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, And Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104-115.
- Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic And Justice Considerations. *Journal Of Social Issues*, 59(2), 323-342.

- Davies, S. G. (1997, January). Re-Engineering The Right To Privacy: How Privacy Has Been Transformed From A Right To A Commodity. *In Technology And Privacy* (Pp. 143- 165). MIT Press.
- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook And Online Privacy: Attitudes, Behaviors, And Unintended Consequences. *Journal Of Computer-Mediated Communication*, 15(1), 83-108.
- DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., & Epstein, J. A. (1996). Lying In Everyday Life. *Journal Of Personality And Social Psychology*, 70(5), 979.
- DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues To Deception. *Psychological Bulletin*, 129(1), 74.
- Diamantopoulos, A. (2011). Incorporating formative measures into covariance-based structural equation models. *Mis Quarterly*, 335-358.
- Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, 17(4), 263-282.
- Dinev, T., & Hart, P. (2003, August). Privacy Concerns And Internet Use—A Model Of Trade-Off Factors. *In Academy Of Management Proceedings* (Vol. 2003, No. 1, Pp. D1-D6). Academy Of Management.
- Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model For E-Commerce Transactions. *Information Systems Research*, 17(1), 61-80.
- Donaldson, T. (1989). *The Ethics Of International Business*. New York: Oxford University Press.
- Donaldson, T., & Dunfee, T. W. (1994). Toward A Unified Conception Of Business Ethics: Integrative Social Contracts Theory. *Academy Of Management Review*, 19(2), 252- 284.
- Draugalis, J. R., Coons, S. J., & Plaza, C. M. (2008). Best Practices For Survey Research Reports: A Synopsis For Authors And Reviewers. *American Journal Of Pharmaceutical Education*, 72(1), 11.
- Drouin, M., Miller, D., Wehle, S. M., & Hernandez, E. (2016). Why do people lie online? “Because everyone lies on the internet”. *Computers in Human Behavior*, 64, 134-142.

- Dumas, T. M., Maxwell-Smith, M., Davis, J. P., & Giulietti, P. A. (2017). Lying Or Longing For Likes? Narcissism, Peer Belonging, Loneliness And Normative Versus Deceptive Like-Seeking On Instagram In Emerging Adulthood. *Computers in Human Behavior*, 71, 1-10.
- Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social Contracts And Marketing Ethics. *The Journal of Marketing*, 14-32.
- Dvoskin, E. (2013 October 14). Study: Digital Marketing Industry Worth \$62 Billion [Blog]. *Wall Street Journal*. Retrieved from <http://blogs.wsj.com/digits/2013/10/14/study-digital-marketing-industry-worth-62-billion>
- Dwyer, C. (2007, January). Digital Relationships In The" Myspace" Generation: Results From A Qualitative Study. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (Pp. 19-19). IEEE.
- Earp, J. B., & Baumer, D. (2003). Innovative Web Use To Learn About Consumer Behavior And Online Privacy. *Communications Of The ACM*, 46(4), 81-83.
- Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living In A Big Data World: Predicting Mobile Commerce Activity Through Privacy Concerns. *Computers in Human Behavior*, 58, 214-220.
- Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice Architecture And Smartphone Privacy: There's a Price For That. In *The Economics Of Information Security And Privacy* (Pp. 211-236). Springer Berlin Heidelberg.
- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N. (2014). Taintdroid: An Information-Flow Tracking System For Realtime Privacy Monitoring On Smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2), 5.
- Experian (2013). Data Quality, The Effect of Dirty Data on Business. Experian Information Solutions, Inc.
- Experian (2016). *The impact of bad contact data quality*. (White paper). Retrieved from <https://www.edq.com/resources/data-management-whitepapers/the-impact-of-bad-contact-data-quality2/> 2016

- Federal Trade Commission. (2009). *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*. Washington DC: FTC. Retrieved from: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.
- Felt, A. P., Egelman, S., & Wagner, D. (2012a, October). I've Got 99 Problems, But Vibration Ain't One: A Survey Of Smartphone Users' Concerns. *In Proceedings Of The Second ACM Workshop On Security And Privacy In Smartphones And Mobile Devices* (Pp. 33-44). ACM.
- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012b, July). Android Permissions: User Attention, Comprehension, And Behavior. *In Proceedings Of The Eighth Symposium On Usable Privacy And Security* (p. 3). ACM.
- Fodor, M., & Brem, A. (2015). Do Privacy Concerns Matter For Millennials? Results From An Empirical Analysis Of Location-Based Services Adoption In Germany. *Computers in Human Behavior*, 53, 344-353.
- Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing research*, 440-452.
- Fowler Jr, F. J., & Cosenza, C. (2009). *Design And Evaluation Of Survey Questions*. The SAGE Handbook Of Applied Social Research Methods, 375-412.
- Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C. (2000). Trust And Privacy Online: Why Americans Want To Rewrite The Rules. *The Pew Internet & American Life Project*, 1-29. Retrieved from: <http://www.pewinternet.org>
- Foxman, E. R., & Kilcoyne, P. (1993). Information Technology, Marketing Practice, And Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing*, 106-119.
- Frattaroli, J. (2006). Experimental disclosure and its moderators: a meta-analysis. *Psychological bulletin*, 132(6), 823.
- Garber, M., (2013). How to Catch a Liar on the Internet. *The Atlantic*. Retrieved from: <https://www.theatlantic.com/magazine/archive/2013/09/the-way-we-lie-now/309431/>.

- Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle With Care: How Online Social Network Providers' Privacy Policies Impact Users' Information Sharing Behavior. *The Journal Of Strategic Information Systems*, 24(1), 33-43.
- Ghazinour, K., Razavi, A. H., & Barker, K. (2014). A model for privacy compromisation value. *Procedia Computer Science*, 37, 143-152.
- Gilliland, S. W. (1993). The Perceived Fairness Of Selection Systems: An Organizational Justice Perspective. *Academy Of Management Review*, 18(4), 694-734.
- Glazer, R. (1991). Marketing In An Information-Intensive Environment: Strategic Implications Of Knowledge As An Asset. *The Journal Of Marketing*, 1-19.
- Granovetter, M. (1995). *Getting A Job: A Study Of Contacts And Careers*. University Of Chicago Press.
- Granryd, M. (2016). You're Probably Reading This On Your Mobile. *World Economic Forum*. Retrieved from <https://www.weforum.org/agenda/2016/01/what-role-will-mobile-play-in-future-of-internet>
- Green, D., (2017, July 17). Gillette has been accidentally sending "Welcome to Manhood" packages to women. *Business Insider*. Retrieved from <http://www.businessinsider.com/gillette-accidentally-sends-razors-to-women-2017-7>
- Greengard, S. (2015). *The Internet Of Things*. MIT Press.
- Greenwald, G. (2014). *No Place To Hide: Edward Snowden, The NSA, And The Us Surveillance State*. Macmillan.
- Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, 94, 19-28.
- Guynn, J., (2018, January 29). Facebook to launch privacy center ahead of EU regulations. *USA Today*. Retrieve from: <https://www.usatoday.com/story/tech/2018/01/29/facebook-launch-privacy-center-ahead-eu-regulations/1071430001/>.
- H.E.W. (1973). *Secretary's Advisory Committee On Automated Personal Data Systems. Records, Computers, And The Rights Of Citizens*. (Report). U.S. Department Of Health, Education, And Welfare.

- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.
- Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*. SAGE Publications.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, 19(2), 139-152.
- Hancock, J. T. (2009). Digital Deception: The Practice of Lying in the Digital Age. Deception: Methods. *Contexts and Consequences*, 109-120.
- Hancock, J. T., Curry, L. E., Goorha, S., & Woodworth, M. (2007b). On Lying And Being Lied To: A Linguistic Analysis Of Deception In Computer-Mediated Communication. *Discourse Processes*, 45(1), 1-23.
- Hancock, J. T., Thom-Santelli, J., & Ritchie, T. (2004, April). Deception And Design: The Impact Of Communication Technology On Lying Behavior. *In Proceedings of the SIGCHI conference on Human factors in computing systems* (Pp. 129-134). ACM.
- Hancock, J. T., Toma, C., & Ellison, N. (2007a, April). The truth about lying in online dating profiles. *In Proceedings of the SIGCHI conference on Human factors in computing systems* (Pp. 449-452). ACM.
- Hancock, J., Birnholtz, J., Bazarova, N., Guillory, J., Perlin, J., & Amos, B. (2009, April). Butler lies: awareness, deception and design. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Pp. 517-526). ACM.
- Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal Of Management Information Systems*, 24(2), 13-42.
- Henseler, J., and Chin, W. W. 2010. A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling. *Structural Equation Modeling: A Multidisciplinary Journal*, 17(1): 82-109.
- Henseler, J., Fassott, G., Dijkstra, T., and Wilson, B. 2012. Analysing Quadratic Effects of Formative Constructs by Means of Variance-Based Structural Equation Modelling. *European Journal of Information Systems*, 21(1): 99-112.
- Hiller, J., & Cohen, R. (2002). *Internet law and policy*. Prentice Hall.

- Hitlin, P., (2015). What is Mechanical Turk?. *Pew Research Center*. Retrieved from: <http://www.pewinternet.org/2016/07/11/what-is-mechanical-turk/>.
- Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information Privacy In The Marketspace: Implications For The Commercial Uses Of Anonymity On The Web. *The Information Society*, 15(2), 129-139.
- Holden, C. J., Dennie, T., & Hicks, A. D. (2013). Assessing the reliability of the M5-120 on Amazon's Mechanical Turk. *Computers in Human Behavior*, 29(4), 1749-1754.
- Horne, D. R., Norberg, P. A., & Cemal Ekin, A. (2007). Exploring consumer lying in information-based exchanges. *Journal of Consumer Marketing*, 24(2), 90-99.
- Houston, F. S., & Gassenheimer, J. B. (1987). Marketing and exchange. *The Journal of Marketing*, 3-18.
- Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The Value Of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 19-33.
- IBM (2016). Why big data is the new natural resource. *Washington Post*. Retrieved from <http://www.washingtonpost.com/sf/brand-connect/wp/ibmpowersystems/why-big-data-is-the-new-natural-resource/>
- Intersoft Consulting, (2018). General Data Protection Regulation (GDPR). Intersoft Consulting. Retrieved from: <https://www.intersoft-consulting.de/en/gdpr/>.
- IT Governance (2018). The EU General Data Protection Regulation (GDPR). *It Governance*. Retrieved from: <https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation>.
- Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research Note—Privacy Concerns And Privacy-Protective Behavior In Synchronous Online Social Interactions. *Information Systems Research*, 24(3), 579-595.
- Jobs, S. (Writer) & K Discovery (Producer). (2007, January). *iPhone: Steve Jobs Announcing The First iPhone In 2007*. YouTube. Retrieved from: [https://www.youtube.com/watch?v=wGoM\\_wVrwng](https://www.youtube.com/watch?v=wGoM_wVrwng)
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully Ignorant: The Effects Of General Privacy Concerns, General Institutional Trust, And Affect In The Privacy Calculus. *Information Systems Journal*, 25(6), 607-635.

- Keith, M. J., Lowry, P. B., Babb, J., & Furner, C. (2017). Limited Information And Quick Decisions: Consumer Privacy Calculus For Mobile Applications. *Transactions On Human Computer Interaction*, 8(3), 88-130.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies*, 71(12), 1163-1173.
- Kelley, P. (2012, July). Privacy as part of the app selection process. In In Proceedings of the Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM). Washington DC, USA: Symposium On Usable Privacy and Security (SOUPS).
- Kelley, T., & Bertenthal, B. I. (2015). Tracking Risky Behavior On The Web: Distinguishing Between What Users 'Say' And 'Do'. In *HAISA* (Pp. 204-214).
- Kobsa, A. (2002). Personalized hypermedia and international privacy. *Communications of the ACM*, 45(5), 64-67.
- Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (IJeC)*, 11(4), 1-10.
- Konečný, Š. (2009). Virtual environment and lying: perspective of czech adolescents and young adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2).
- Kuran, T. (1995). The inevitability of future revolutionary surprises. *American Journal of Sociology*, 100(6), 1528-1551.
- Landers, R. N., & Behrend, T. S. (2015). An inconvenient truth: Arbitrary distinctions between organizational, Mechanical Turk, and other convenience samples. *Industrial and Organizational Psychology*, 8(2), 142-164.
- Langer, G. (2018). Probability Versus Non-Probability Methods. In *The Palgrave Handbook of Survey Research* (Pp. 351-362). Palgrave Macmillan, Cham.
- Laudon, K. C. (1986). *Dossier Society: Value Choices In The Design Of National Information Systems*. Columbia University Press.
- Läufer, R. S., & Wolfe, M. (1977). Privacy As A Concept And A Social Issue: A Multidimensional Developmental Theory. *Journal Of Social Issues*, 33(3), 22-42.

- Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. *Pew internet & American life project*.
- Levenson, H., (2017). 5 apps That Have Completely Nailed Mobile Personalization. *Appsee*. Retrieved from: <https://blog.appsee.com/5-mobile-apps-that-have-completely-nailed-mobile-personalization>.
- Levine, T. R., Kim, R. K., & Hamel, L. M. (2010). People lie for a reason: Three experiments documenting the principle of veracity. *Communication Research Reports*, 27(4), 271-285.
- Liang, H., Saraf, N., Hu, Q., Xue, Y., (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. *MIS Quarterly* 31, 59–87.
- Liccardi, I., Pato, J., & Weitzner, D. J. (2014). Improving User Choice Through Better Mobile Applications Transparency And Permissions Analysis. *Journal Of Privacy And Confidentiality*, 5(2), 1.
- Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation And Purpose: Understanding Users' Mental Models Of Mobile Application Privacy Through Crowdsourcing. *In Proceedings Of The 2012 ACM Conference On Ubiquitous Computing* (Pp. 501-510). ACM.
- Ling, R. S. (2008). *New tech, new ties*. Cambridge, MA: MIT press.
- Liu, C., Marchewka, J. T., & Ku, C. (2004). American And Taiwanese Perceptions Concerning Privacy, Trust, And Behavioral Intentions In Electronic Commerce. *Journal Of Global Information Management (JGIM)*, 12(1), 18-40.
- Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014, January). Privacy As A Tradeoff: Introducing The Notion Of Privacy Calculus For Context-Aware Mobile Applications. *In System Sciences (HICSS), 2014 47th Hawaii International Conference on* (Pp. 1063-1072). IEEE.
- Lu, H. Y. (2008). Sensation-seeking, Internet dependency, and online interpersonal deception. *CyberPsychology & Behavior*, 11(2), 227-231.
- Lucker, J., Hogan, S.K., Bischoff, T. (2017). Predictably Inaccurate. The prevalence and perils of bad big data. *Deloitte Review*. Retrieved from <https://www2.deloitte.com/insights/us/en/deloitte-review/issue-21/analytics-bad-data-quality.html>

- Lwin, M. O., & Williams, J. D. (2003). A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters*, 14(4), 257-272.
- Mai, B., Menon, N. M., & Sarkar, S. (2010). No Free Lunch: Price Premium For Privacy Seal-Bearing Vendors. *Journal Of Management Information Systems*, 27(2), 189- 212.
- Malheiros, M., Preibusch, S., & Sasse, M. A. (2013, June). "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. *In International Conference on Trust and Trustworthy Computing* (Pp. 250-266). Springer, Berlin, Heidelberg.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (Iuipc): The Construct, The Scale, And A Causal Model. *Information Systems Research*, 15(4), 336-355.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Byers, A. H., (2001, May). Big data: The next frontier for innovation, Competition and productivity. *McKinsey*. Retrieved from: [https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI\\_big\\_data\\_exec\\_summary.ashx](https://www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx).
- Margulis, S. T. (1977). Conceptions Of Privacy: Current Status And Next Steps. *Journal of Social Issues*, 33(3), 5-21.
- Margulis, S. T. (2003). Privacy As A Social Issue And Behavioral Concept. *Journal of Social Issues*, 59(2), 243-261.
- Marx, G. (2001). *Identity and anonymity: Some conceptual distinctions and issues for research*. Princeton University Press.
- McNamara, A., Verma, A., Stallings, J., & Staddon, J. (2016, October). Predicting Mobile App Privacy Preferences with Psychographics. *In Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (Pp. 47-58). ACM.
- Mietzner, D., & Reger, G. (2005). Advantages and disadvantages of scenario approaches for strategic foresight. *International Journal of Technology Intelligence and Planning*, 1(2), 220-239.

- Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management And National Regulation. *Organization Science*, 11(1), 35-57.
- Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing*, 19(1), 1-6.
- Milne, G. R., & Boza, M. E. (1999). Trust And Concern In Consumers' Perceptions Of Marketing Information Management Practices. *Journal Of Interactive Marketing*, 13(1), 5-24.
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15-29.
- Milne, G. R., & Gordon, M. E. (1993). Direct Mail Privacy-Efficiency Trade-Offs Within An Implied Social Contract Framework. *Journal of Public Policy & Marketing*, 206-215.
- Miyazaki, A. D., & Fernandez, A. (2000). Internet Privacy And Security: An Examination Of Online Retailer Disclosures. *Journal Of Public Policy & Marketing*, 19(1), 54-61.
- Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323-339.
- Morey, T, Forbath, T., & Schoop, A. (2015). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*. Retrieved from: <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>
- Nafus, D., & Tracey, K. (2002). 13 Mobile Phone Consumption And Concepts Of Personhood. *Perpetual Contact*, 206.
- Newman, D., (2017, April 4). Improving Customer Experience Through Customer Data. *Forbes*. Retrieved from: <https://www.forbes.com/sites/danielnewman/2017/04/04/improving-customer-experience-through-customer-data/#76da96a84e64>
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal Of Consumer Affairs*, 41(1), 100-126.

- Nowak, G. J., & Phelps, J. (1992). Understanding Privacy Concerns. An Assessment Of Consumers' Information-Related Knowledge And Beliefs. *Journal of Interactive Marketing*, 6(4), 28-39.
- O'Sullivan, B. (2000). What You Don't Know Won't Hurt Me. *Human Communication Research*, 26(3), 403-431.
- Oksman, V., & Rautiainen, P. (2003). Perhaps It Is A Body Part": How The Mobile Phone Became An Organic Part Of The Everyday Lives Of Finnish Children And Teenagers. *Machines That Become Us: The Social Context Of Personal Communication Technology*, 161-70.
- Olmstead, K. (2014, April 29). Mobile Applications Collect Information About Users, With Wide Range Of Permissions. *Pew Research Center*. Retrieved from <http://www.pewresearch.org/fact-tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/>.
- P.P.S.C., Privacy Protection Study Commission, (1977). *Personal Privacy In An Information Society*. (Privacy Protection Study Commission.) Washington, D.C.: U.S. Government Printing Office. Retrieved From: <http://epic.org/privacy/ppsc1977report/>.
- Page, X., Knijnenburg, B. P., & Kobsa, A. (2013, February). What A Tangled Web We Weave: Lying Backfires In Location-Sharing Social Media. *In Proceedings Of The 2013 Conference On Computer Supported Cooperative Work* (Pp. 273-284). ACM.
- Pak, J., & Zhou, L. (2014). Social Structural Behavior Of Deception In Computer-Mediated Communication. *Decision Support Systems*, 63, 95-103.
- Pappas, N. (2016). Marketing strategies, perceived risks, and consumer trust in online buying behaviour. *Journal of Retailing and Consumer Services*, 29, 92-103.
- Patil, S., & Kobsa, A. (2005, November). Uncovering Privacy Attitudes And Practices In Instant Messaging. *In Proceedings Of The 2005 International ACM, Sig Group Conference On Supporting Group Work* (Pp. 109-112). ACM.
- Pavlou, P.A., Liang, H.G., Xue, Y.J., 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS Quarterly* 31, 105-136.

- Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 65, 409-419.
- Perez, Sarah (2017, May 4). Report: Smartphone Owners Are Using 9 Apps Per Day; 30 Per Month. *Techcrunch*. Retrieved from: <https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/>.
- Petronio, S. (2012). *Boundaries Of Privacy: Dialectics Of Disclosure*. Suny Press.
- Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS quarterly*, 623-656.
- Pew Research Center (2018 February 5). Mobile Fact Sheet. *The Pew Internet & American Life Project*, 1-29. Retrieved from: <http://www.pewinternet.org/fact-sheet/mobile/>
- 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.
- Posner, R. A. (1981). The Economics Of Privacy. *The American Economic Review*, 71(2), 405-409.
- Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133-1143.
- Raine, L., & Madden, M. (2015). American Views On Government Surveillance Programs. *Pew Research Center: Internet, Science & Tech*, 16.
- Rajput, M. (2017, April). Top Trending Mobile App Categories In 2017. *Mind Inventory*. Retrieved from: <https://www.mindinventory.com/blog/top-trending-mobile-app-categories-in-2017/>.
- Redmiles, E. M., Kross, S., Pradhan, A., & Mazurek, M. L. (2017). *How well do my results generalize? Comparing security and privacy survey results from MTurk and web panels to the US*.
- Rigdon, E. E., Ringle, C. M., and Sarstedt, M. 2010. Structural Modeling of Heterogeneous Data with Partial Least Squares, in *Review of Marketing Research*, N. K. Malhotra (ed.), Sharpe: Armonk, 255-296.
- Ringle, C. M., Wende, S., & Will, S. (2005). *SmartPLS 2.0 (M3) Beta*, Hamburg 2005.

- Sass, E. (2017, March 3). Ordinary Social Media Users Are Buying ‘Likes’ Too. *Mediapost*. Retrieved from: <https://www.mediapost.com/publications/article/296359/ordinary-social-media-users-are-buying-likes-too.html>
- Saunders, K. M., & Zucker, B. (1999). Counteracting Identity Fraud In The Information Age: The Identity Theft And Assumption Deterrence Act. *International Review of Law, Computers & Technology*, 13(2), 183-192.
- Scholl, F., & Hollander, J. (2003). The changing privacy and security landscape. *Business Communications Review*, 33(5), 54-57.
- Schroder, W.J. (2017). Generations X, Y, Z and the Others. [socialmarketing.org](http://socialmarketing.org). Retrieved from <http://socialmarketing.org/archives/generations-xy-z-and-the-others/>
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions Of Privacy Concern Among Online Consumers. *Journal Of Public Policy & Marketing*, 19(1), 62-73.
- Shin, D. H. (2010). The Effects Of Trust, Security And Privacy In Social Networking: A Security-Based Approach To Understand The Pattern Of Adoption. *Interacting With Computers*, 22(5), 428-438.
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness And Creepiness In Application Space: Perceptions Of Privacy And Mobile Application Use. In *Proceedings Of The 32Nd Annual ACM Conference On Human Factors In Computing Systems* (Pp. 2347-2356). ACM.
- Singer, E., Mathiowetz, N. A., & Couper, M. P. (1993). The Impact Of Privacy And Confidentiality Concerns On Survey Participation The Case Of The 1990 Us Census. *Public Opinion Quarterly*, 57(4), 465-482.
- Singer, N., (2015). Sharing Data, but not Happily. *The New York Times*. Retrieved from: <https://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html>
- Sivo, S. A., Saunders, C., Chang, Q., & Jiang, J. J. (2006). How low should you go? Low response rates and the validity of inference in IS questionnaire research. *Journal of the Association for Information Systems*, 7(6), 17.
- Sloper, D., (2018). Statistics Calculators: Sample Size, Statistical Power. Retrieved from: <https://www.danielsoper.com/statcalc/default.aspx>
- Slovic, Paul. (1995). “The Construction of Preference,” *American Psychologist*, 50(5), 364–371.

- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989-1016.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, 167-196.
- Solove, D. J. (2008). The end of privacy?. *Scientific American*, 299(3), 100-106.
- Son, J. Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy And A Nomological Model. *MIS Quarterly*, 503-529.
- Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. *In Proceedings of the 3rd ACM conference on Electronic Commerce* (Pp. 38-47). ACM.
- Statista (2017, March). Number Of Apps Available In Leading App Stores As Of March 2017. *Statista*. Retrieved from: <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>.
- Steinel, W., Utz, S., & Koning, L. (2010). The good, the bad and the ugly thing to do when sharing information: Revealing, concealing and lying depend on social motivation, distribution and importance of information. *Organizational Behavior and Human Decision Processes*, 113(2), 85-96.
- Steinfeld, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, 29(6), 434-445.
- Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination Of The Concern For Information Privacy Instrument. *Information Systems Research*, 13(1), 36-49.
- Stone, E. F. (1978). *Research methods in organizational behavior*. Goodyear Publishing Company.
- Stone, E. F., & Stone, D. L. (1990). Privacy In Organizations: Theoretical Issues, Research Findings, And Protection Mechanisms. *Research In Personnel And Human Resources Management*, 8(3), 349-411.
- Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems*, 13(1), 63.

- Strong, D. M., Lee, Y. W., & Wang, R. Y. (1997). Data quality in context. *Communications of the ACM*, 40(5), 103-110.
- Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent Listeners: The Evolution Of Privacy And Disclosure On Facebook. *Journal Of Privacy And Confidentiality*, 4(2), 2.
- Sue, V. M., & Ritter, L. A. (2011). *Conducting Online Surveys*. Sage Publications.
- Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278-292.
- Teltzrow, M., & Kobsa, A. (2004). Impacts of user privacy preferences on personalized systems. In *Designing personalized user experiences in eCommerce* (Pp. 315-332). Springer Netherlands.
- Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, 48(1), 159-205.
- Thibaut, J. W., & Kelley, H. H. (1959). *The social psychology of groups*. Wiley. New York.
- Thibaut, J. W., & Walker, L. (1975). *Procedural Justice: A Psychological Analysis*. L. Erlbaum Associates.
- Thurm, S., & Kane, Y. I. (2010). Your apps are watching you. *The Wall Street Journal*, 17(1).
- Tian, K., & Keep, B. (2002). *Customer Fraud And Business Responses: Let The Marketer Beware*. Greenwood Publishing Group.
- Toe, A. C., Tan, G. W. H., Ooi, K. B., & Lin, B. (2015). Why consumers adopt mobile payment? A partial least squares structural equation modeling (PLS-SEM) approach. *International Journal of Mobile Communications*, 13(5), 478-497.
- Toma, C. L., & Hancock, J. T. (2013). Self-affirmation underlies Facebook use. *Personality and Social Psychology Bulletin*, 39(3), 321-331.
- Trochim, W. (2006). Non-probability sampling: Purposive sampling. *Ithaca, NY*.
- Trochim, W., Donnelly, J. P., & Arora, K. (2015). *Research methods: The essential knowledge base*. Nelson Education.
- Tsikerdekis, M., & Zeadally, S. (2014). Online Deception In Social Media. *Communications of the ACM*, 57(9), 72-80.

- Turkle, S. (2008). *10 Always-On/Always-On-You: The Tethered Self. Handbook of mobile communication studies*, 121.
- Tyler, T. R. (1994). Psychological Models Of The Justice Motive: Antecedents Of Distributive And Procedural Justice. *Journal Of Personality And Social Psychology*, 67(5), 850.
- Van Kleek, M., Murray-Rust, D., Guy, A., Smith, D. A., O'Hara, K., & Shadbolt, N. R. (2015, June). Self curation, social partitioning, escaping from prejudice and harassment: the many dimensions of lying online. *In Proceedings of the ACM Web Science Conference* (p. 10). ACM.
- Vance, A. (2010). If your password is 123456, just make it hackme. *The New York Times*, 20, A1-A1.
- Vroom, V. H. (1964). *Work and motivation*. Oxford, England: Wiley.
- Wan, M.A. (2014). Hierarchical Component Using Reflective-Formative Measurement Model Partial Least Square Structural Equation Modeling (PLS-SEM), *International Journal of Mathematics and Statistics Invention (IJMSI)*, 2(2): 55-71.
- Wang, L., Yan, J., Lin, J., & Cui, W. (2017). Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking. *International Journal of Information Management*, 37(1), 1428-1440.
- Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, 12(4), 5-33.
- Wang, R. Y., Lee, Y. W., Pipino, L. L., & Strong, D. M. (1998). Manage your information as a product. *Sloan Management Review*, 39(4), 95.
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531-542.
- Ward, C., & Berno, T. (2011). Beyond social exchange theory: Attitudes toward tourists. *Annals of Tourism Research*, 38(4), 1556-1569.
- Westin, A. (2001). Opinion Surveys: What Consumers Have To Say About Information Privacy. (Prepared Witness Testimony) The House Committee on Energy and Commerce.
- Westin, A. F. (1968). Privacy And Freedom. *Washington And Lee Law Review*, 25(1), 166.

- Westin, A. F. (2003). Social And Political Dimensions Of Privacy. *Journal of Social Issues*, 59(2), 431-453.
- Wheeless, L. R., & Grotz, J. (1976). Conceptualization And Measurement Of Reported Self-Disclosure. *Human Communication Research*, 2(4), 338-346.
- Wirth K., & Sweet, K. (2017). *One-to-One Personalization in the Age of Machine Learning: Harnessing Data to Power Great Customer Experiences*. BookBaby.
- Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research*, 12(2), 190-207.
- Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering Personal Information On The Internet: Effects Of Reputation, Privacy Notices, And Rewards On Online Consumer Behavior. *Marketing Letters*, 17(1), 61-74.
- Xu, H. (2007). The Effects Of Self-Construal And Perceived Control On Privacy Concerns. *Icis 2007 Proceedings*, 125.
- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, 6.
- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012a). Measuring Mobile Users' Concerns For Information Privacy. *Thirty Third International Conference on Information Systems, Orlando 2012*. IS Security and Privacy.
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The Role Of Push-Pull Technology In Privacy Calculus: The Case Of Location-Based Services. *Journal of Management Information Systems*, 26(3), 135-174.
- Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012b). Research Note—Effects Of Individual Self-Protection, Industry Self-Regulation, And Government Regulation On Privacy Concerns: A Study Of Location-Based Services. *Information Systems Research*, 23(4), 1342-1363.
- Xu, J., Tang, X., Hu, H., & Du, J. (2010). Privacy-conscious location-based queries in mobile environments. *IEEE Transactions on Parallel and Distributed Systems*, 21(3), 313-326.
- Yahoo, (2011). Mobile Internet — Delivering on the Promise of Mobile Advertising. *Yahoo*. Retrieved from <https://www.statista.com/statistics/188352/mobile-internet-users-in-the-us-from-2009-to-2014>

- Yang, Z., & Jun, M. (2002). Consumer perception of e-service quality: from internet purchaser and non-purchaser perspectives. *Journal of Business Strategies*, 19(1), 19.
- Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology & Behavior*, 11(6), 763-765.
- Zhang, X., Ying, K., Aafer, Y., Qiu, Z., & Du, W. (2016, February). Life after App Uninstallation: Are the Data Still Alive? Data Residue Attacks on Android. *In NDSS*.
- Zhang, Y., Chen, Z., Xue, H., & Wei, T. (2015, May). Fingerprints On Mobile Devices: Abusing And Leaking. *In Black Hat Conference*.
- Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure Intention Of Location-Related Information In Location-Based Social Network Services. *International Journal of Electronic Commerce*, 16(4), 53-90.
- Zhou, T. (2011a). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, 111(2), 212-226.
- Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011b, June). Taming information-stealing smartphone applications (on android). In *International conference on Trust and trustworthy computing* (Pp. 93-107). Springer, Berlin, Heidelberg.
- Zimbler, M., & Feldman, R. S. (2011). Liar, Liar, Hard Drive On Fire: How Media Context Affects Lying Behavior. *Journal of Applied Social Psychology*, 41(10), 2492-2507.
- Zwick, D., & Dholakia, N. (2004). Whose Identity Is It Anyway? Consumer Representation In The Age Of Database Marketing. *Journal of Macromarketing*, 24(1), 31-43.

**APPENDICES**

## APPENDIX A: MOBILE PRIVACY CONCERN STUDIES 2007-2017

<i>Mobile Privacy Concern Studies 2007-2017</i>		
<b>Author</b>	<b>Title</b>	<b>Key Findings</b>
<b>Eastin et al., 2016</b>	<i>Living in a big data world: Predicting mobile commerce activity through privacy concerns.</i>	Perceived control and unauthorized access to personal information have a significant negative influence on m-commerce activity. Extend of data collection, awareness of collection and the collection of location more passive dimensions on behavior.
<b>Felt et al., 2012a</b>	<i>I've Got 99 Problems, But Vibration Ain't One: A Survey of Smartphone Users' Concerns</i>	Ranking of perceived risk with data sharing with application developer and location being the top most concern. Type of data shared influenced viewpoints on risk.
<b>Fodor &amp; Brem, 2015</b>	<i>Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany</i>	Privacy concerns negatively influence the adoption of location based service applications.
<b>Gu et al., 2017</b>	<i>Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective</i>	Permission justification and perceived app popularity decreases privacy concerns. Negative experiences moderates the effect reducing the effect.
<b>Keith et al., 2017</b>	<i>Limited Information and Quick Decisions: Consumer Privacy Calculus for Mobile Apps</i>	Consumer adoption of applications based on network size increases benefits and reduces risk. Privacy assurance (not sharing with 3rd parties) increases adoption. Network size reduces concerns on location based services.
<b>Keith et al., 2013</b>	<i>Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior .</i>	Weak relationship between disclosure intention and actual disclosure moderated by consumer practice of disclosing false data.
<b>Liu et al., 2014</b>	<i>Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications</i>	Personalization and control of mobile content influence disclosure, reducing affect of privacy concerns.
<b>McNamara et al., 2016</b>	<i>Predicting Mobile Application Privacy Preferences with Psychographics</i>	Psychographics combined with the attributes of the application context are predictive of user privacy preferences. Users who are independent decision makers are more conservative about personal information.

<i>Mobile Privacy Concern Studies 2007-2017</i>		
<b>Author</b>	<b>Title</b>	<b>Key Findings</b>
<b>Pentina et al., 2016</b>	<i>Exploring privacy paradox in information-sensitive mobile application adoption: A cross-cultural comparison.</i>	Privacy concerns do not influence adoption of private-information sensitive apps. Extraversion and agreeableness are positively related to user perceptions of benefits obtained by apps
<b>Shklovski et. al., 2014</b>	<i>Leakiness and creepiness in application space</i>	Concerns about tracking, desire to be more in control. Data leakage considered privacy violation and increased concerns.
<b>Sun et al., 2015</b>	<i>Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences</i>	Support for privacy calculus model to different benefits and examines gender differences showing that females value hedonic benefits, males value utilitarian benefits.
<b>Wang et al., 2016</b>	<i>Intention to disclose personal information via mobile apps: A privacy calculus perspective.</i>	Self presentation and personalized services positively influence benefits and intention to disclose. Perceived severity and control negatively affect disclosure intention.
<b>Xu et al., 2012a</b>	<i>Measuring Mobile User's Concerns for Information Privacy</i>	Instrument development, consumers concerns for privacy is aggravated in the mobile environment; cannot hide identity unique ID number, location tracking.
<b>Zhang et al., 2015</b>	<i>Mobile Commerce and Consumer Privacy Concerns.</i>	Education level and age are significant demographic differences in mobile commerce privacy concerns. Higher the education or younger in age are less likely to be concerned about privacy in mobile commerce.
<b>Zhao et al., 2012</b>	<i>Disclosure Intention of Location-Related Information in Location-Based Social Network Services</i>	Users perceived benefits on information disclosure affected location-sharing behavior even when privacy concerns were present.
<b>Zhou, 2011a</b>	<i>The impact of privacy concern on user adoption of location-based services.</i>	Risk and Trust affect usage intention which are influenced by privacy concerns with larger affect of collection, secondary use on risk, where as errors affected trust.
<b>Zhou, 2011b</b>	<i>Taming information-stealing smartphone applications (on android).</i>	Smartphones are used in everyday life, studies show that users personal information is a risk by applications. Increasing control can help empower users.

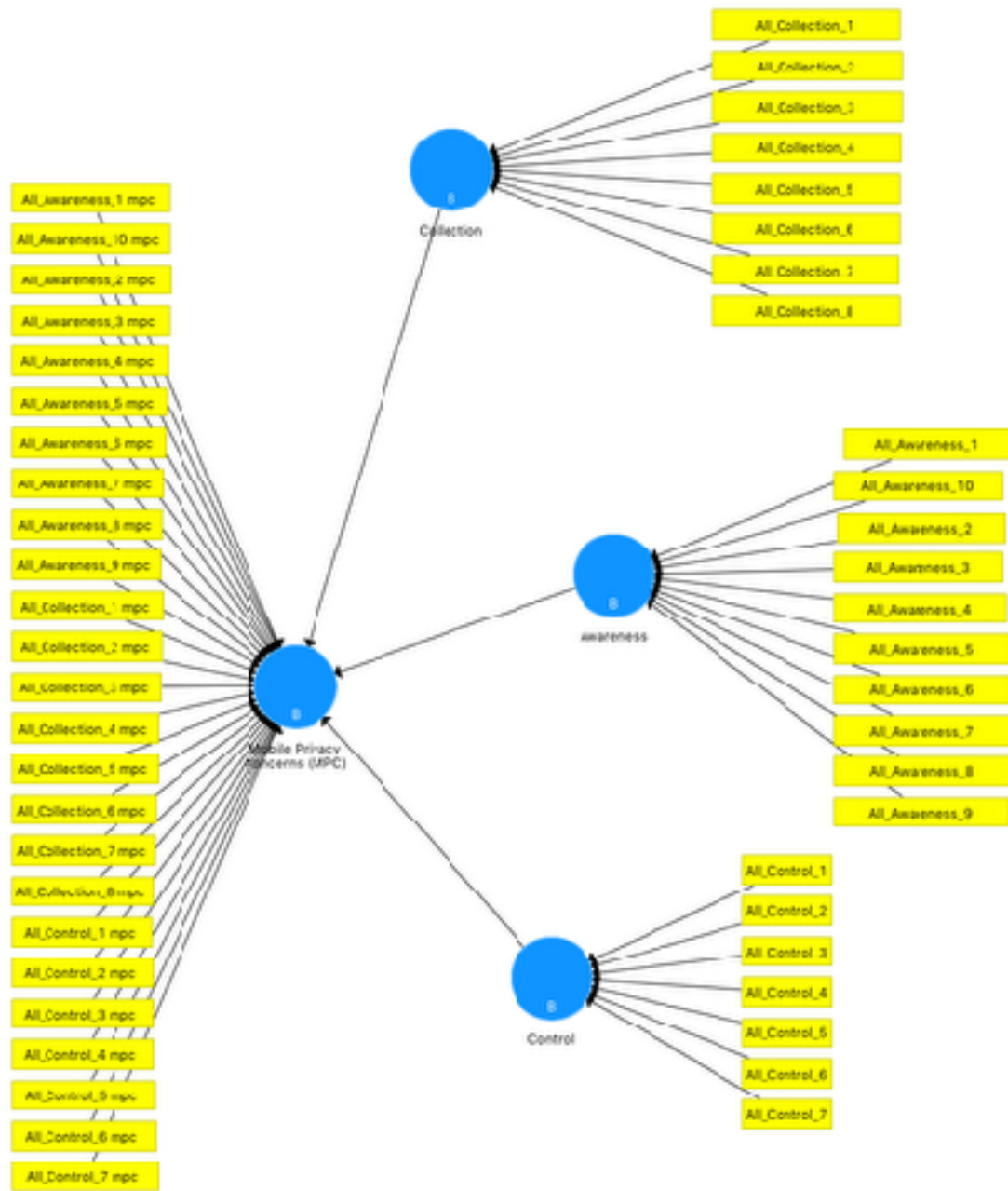
## APPENDIX B: ONLINE DECEPTION STUDIES

<i>Online Deception Studies</i>		
<b>Author</b>	<b>Title</b>	<b>Key Findings</b>
<b>Caspi &amp; Gorsky, 2006</b>	<i>Online Deception: Prevalence, Motivation, and Emotion</i>	One third of users reported engaging in online deception. Frequent online users deceive online more than infrequent users, young users more than old, competent users more than non-competent. Motivations to deceive related to privacy concerns and enjoyment.
<b>Drouin et al., 2016</b>	<i>Why do people lie online? "Because everyone lies on the internet"</i>	Lying behavior for self and others vary across online contexts. Type of lies vary across context. Perceptions of others lying is related self online deception.
<b>Dumas et al., 2017</b>	<i>Lying or longing for likes? Narcissism, peer belonging, loneliness and normative versus deceptive like-seeking on Instagram in emerging adulthood</i>	Participants engaged in variety of validation behaviors from normal to deceptive such as buying likes or fabricating photos. Users with stronger narcissism and weaker sense of belonging are more likely to be deceptive.
<b>Hancock et al., 2017</b>	<i>The Truth about Lying in Online Dating Profiles</i>	Deception was observed in 81% of participant's profiles showing a pervasiveness of deception in online dating.
<b>Horne et al, 2007</b>	<i>Exploring consumer lying in information-based exchanges</i>	Individuals tend to falsify some items more than they do others, when information is not personally identifying there is a high level of deception. Users can be grouped based on their disclosure strategies (lying, omitting, truthful). Users perform a cost/benefit calculus which influences lying.
<b>Kobsa, 2002</b>	<i>Personalized Hypermedia and International Privacy</i>	Users very concerned about threats to their privacy using Internet, they are concerned about divulging personal information online, extremely concerned about being tracked online. User report leaving sites that required registration of information (41%), entering false registration information (40-24% and having refrained from shopping and bought less 32% - 24%.
<b>Konený, 2009</b>	<i>Virtual Environment and Lying: Perspective of Czech Adolescents and Young Adults</i>	Users misrepresent information about themselves. young age groups tendency to lie more often.
<b>Konený, 2009</b>	<i>Virtual Environment and Lying: Perspective of Czech Adolescents and Young Adults</i>	Users misrepresent information about themselves. young age groups tendency to lie more often.
<b>Lu, 2008</b>	<i>Sensation-Seeking, Internet Dependency, and Online Interpersonal Deception</i>	Sensation-seekers and high Internet users are more likely to engage in online deception.
<b>Lu, 2008</b>	<i>Sensation-Seeking, Internet Dependency, and Online Interpersonal Deception</i>	Sensation-seekers and high Internet users are more likely to engage in online deception.

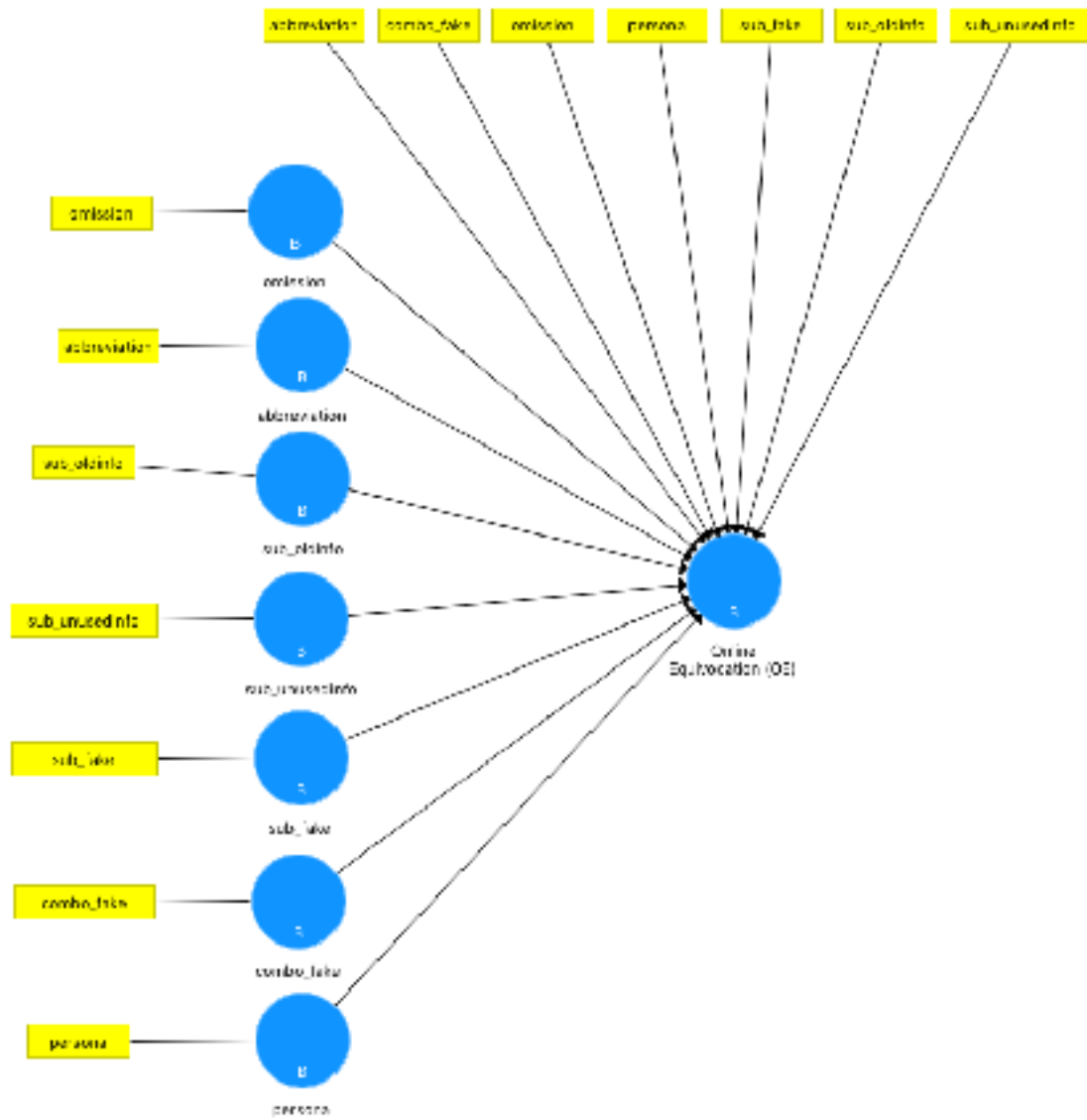
<i>Online Deception Studies</i>		
<b>Author</b>	<b>Title</b>	<b>Key Findings</b>
<b>Lwin &amp; Williams, 2003</b>	<i>A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online</i>	Users positive attitudes towards deception is more likely to support behavior to deceive. Users perceived ability to fabricate successfully positively affects their behavior to fabricate. The more likely a user has a perceived moral obligation the less likely they will fabricate.
<b>Lwin &amp; Williams, 2003</b>	<i>A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online</i>	Users positive attitudes towards deception is more likely to support behavior to deceive. Users perceived ability to fabricate successfully positively affects their behavior to fabricate. The more likely a user has a perceived moral obligation the less likely they will fabricate.
<b>Malherios et al., 2013</b>	<i>“Fairly truthful”: The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure</i>	Fairness significant effect on disclosure and truthfulness.
<b>Malherios et al., 2013</b>	<i>“Fairly truthful”: The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure</i>	Fairness significant effect on disclosure and truthfulness.
<b>Page et al., 2013</b>	<i>What a Tangled Web We Weave: Lying Backfires in Location-Sharing Social Media</i>	Individuals who have a high propensity to lie also have increased privacy concerns and are more likely to lie regarding location sharing.
<b>Page et al., 2013</b>	<i>What a Tangled Web We Weave: Lying Backfires in Location-Sharing Social Media</i>	Individuals who have a high propensity to lie also have increased privacy concerns and are more likely to lie regarding location sharing.
<b>Pak &amp; Zhou, 2013</b>	<i>Social structural behavior of deception in computer-mediated communication</i>	Deception is a strategic activity where the deceiver juggles between the dual goals of promoting agenda or avoiding detection.
<b>Pak &amp; Zhou, 2013</b>	<i>Social structural behavior of deception in computer-mediated communication</i>	Deception is a strategic activity where the deceiver juggles between the dual goals of promoting agenda or avoiding detection.
<b>Son &amp; Kim, 2008</b>	<i>Internet Users’ Informational Privacy-Protective Responses: A Taxonomy and a Nomological Model</i>	Privacy concerns are a major source of responses. Privacy concerns did not have a strong impact on users intention to falsify personal information.
<b>Steinel et al., 2010</b>	<i>The good, the bad and the ugly thing to do when sharing information: Revealing, concealing and lying depend on social motivation, distribution and importance of information</i>	Information sharing depends on pro-social, pro-self motivation of what people consider important to reveal, withhold or falsify in their private/public information. Pro-self motivated individuals (selfish) are more likely to conceal or lie about their private/public information.

<i>Online Deception Studies</i>		
<b>Author</b>	<b>Title</b>	<b>Key Findings</b>
<b>Tsikerdekis &amp; Zeadally, 2014</b>	<i>Online Deception in Social Media</i>	Psychological and physical distance influence occurrence and amount of deception. Context, type of social media and capabilities influence deception (difficulty).
<b>Van Kleek et al., 2015</b>	<i>Self Curation, Social Partitioning, Escaping from Prejudice and Harassment: the Many Dimensions of Lying Online</i>	Individuals have many reasons for fabricating, omitting or alternating the truth online including creative expression, hiding sensitive information, privacy, separation (work/friends), role-playing and avoiding harassment or discrimination
<b>Wang et al., 2016</b>	<i>Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking.</i>	Application reputation and experience reduces privacy concerns. Application compatibility and experience increases perception of social rewards. More weight is placed on social rewards than monetary rewards. Social rewards positively influence disclosure honesty.
<b>Zimbler &amp; Feldman, 2011</b>	<i>Liar, Liar, Hard Drive on Fire: How Media Context Affects Lying Behavior</i>	Most lying occurs in email vs. instant messaging or face-to-face. Normal to distort reality online. Propose that individuals grow psychologically and physically further from the person when they are online and more likely to lie. View of permanence in the communication affects the degree of deception.

**APPENDIX C: MOBILE PRIVACY CONCERNS PLS-SEM FORMATIVE MODEL (REPEATED INDICATORS APPROACH)**



**APPENDIX D: ONLINE EQUIVOCATION PLS-SEM FORMATIVE MODEL  
(REPEATED INDICATORS APPROACH)**



## **APPENDIX E: IRB SUBMISSION**

### **1) Abstract of the study**

As fast as individuals engage in new ways to share online, their concerns over privacy are increasing almost as fast. Online engagement is not just “to share or not to share,” it is more a continuum of disclosure. To remain engaged online and to avoid privacy exposure, individuals will sometimes use a process called online equivocation. Misrepresented information can misinform firms and lead to incorrect decisions. This study seeks to examine the way in which the disclosure context affects individual behavior, in particular how individuals use online equivocation as a method to lower privacy concerns or protect their personal privacy. The expected result is a categorization of the various online equivocation strategies by users within mobile applications (apps), which can be used to inform firms regarding data collection approaches to encourage truthful digital representation.

### **2) Protocol Title**

Usage of Mobile Applications

### **3) Investigators**

**Susan Mudambi**, Department of Marketing and Supply Chain Management,  
Executive DBA

**Irene Graff**, Executive DBA Doctoral Student

### **4) Objectives**

To understand the mobile contexts in which individuals make data sharing

(disclosure) decisions

To learn when individuals feel concerned about their privacy in these mobile context

To examine the mobile context and the online equivocation of personal information

## **5) Rationale and Significance**

Firms make broad generalizations about what data individuals will share in mobile applications. They also depend on this data to tailor services, support business processes and decision-making. The study proposes that the mobile context in which individuals share data will influence their sharing behavior. In some contexts, individuals may feel concerned about their privacy and are likely provide misrepresented (false) information to avoid negative effects of exposure. It is a business advantage to understand those factors and provide application processes that encourage truthful disclosure.

## **6) Resources and Setting**

Beyond the required CITI training, the investigator has ensured that persons assisting with the study are adequately informed about the protocol and their study-related duties and functions by meeting with each researcher to discuss and review role specific tasks and expectations.

The research will take place in an online environment. Participants will be recruited through AYTМ panel system. AYTМ is opt-in community of people who take surveys for compensation (similar to Amazon MTurk), however AYTМ offers a few more capabilities—they double check panelists to ensure uniqueness, no duplication, no robots; they are rewarded for honesty; they protect their panel privacy; they don't rent their community; they avoid professional survey takers; and they have global reach in 26

countries and can reach to 60+ more if necessary. To supplement the research, MTurk may also be used. Participation in the study requires completing a short online questionnaire. For example, subjects will read a short scenario describing a mobile application. Then the subjects will answer a series of questions about their attitudes toward the information sharing activities involved with the application. There is no specific location where the research must be performed.

## **7) Prior Approvals**

No other non-IRB approvals are necessary in order to perform the research.

## **8) Study Design**

### **a) Recruitment Methods**

Each study aims to recruit approximately 3,500 respondents. Subjects will be obtained by online or computer generated survey. Subject collection will stem from the AYTM panel of 25 million across the United States. A second phase study using same instrument will be expanded to up to four additional markets—China, Russia, India, Brazil or Indonesia through the same AYTM panel service. The AYTM panel service pays the respondents for completing the survey based on their panel agreement with them. To supplement the research, MTurk may also be used.

### **b) Inclusion and Exclusion Criteria**

The study will only include participants who are at least 18 years old.

### **c) Study Timelines**

We estimate the entire survey will require about 15-20 minutes to complete.

Participation is open to anyone that meets the estimated threshold, but participants are

limited to finish only one survey.

We will launch the project immediately upon the approval of the protocol. We will initiate the data collection within a few days from the approval of the protocol. Initial data collection is expected to be completed in the Summer of 2017. Data collection is expected to continue through 2018.

**d) Study Procedures and Data Analysis**

Subjects will complete the questionnaire through the online AYTM system. The task involves several steps:

1. Subjects will read a short scenario describing a mobile application, and then the subjects will answer a series of questions about their attitudes toward data sharing. AYTM provides general demographic information as participants of the panel which are categorized, no personal private identification is shared.
2. The entire procedure will take about 15-20 minutes to complete.
3. Their information will be anonymously recorded (by a unique identifier) in a secure database managed by AYTM.

**e) Withdrawal of Subjects**

Subjects may withdraw from the study simply by ending the task early. No contact with the investigator is required. There are no circumstances where a subject will be removed from the study without his or her consent.

**f) Privacy & Confidentiality**

The study will not use or disclose subjects' personal health information (PHI). The data will be stored on a password-protected computer. Regardless, there will be no personally-identifiable information in the data set. The study results will be presented in aggregate form in working and completed research papers. The results will not be able to be traced back to individual responses. *We will make sure the subjects are aware that we will anonymize the data so that individual responses cannot be linked back to their name. We will explain this on the online consent form on the instrument. In addition, AYTМ panelists are ensured their privacy by AYTМ and their procedures.*

**9) Risks to Subjects**

There are no risks to subjects in this study.

**10) Multi-Site Human Research**

This research does not involve multi-site studies.

**11) Potential Benefits to Subjects**

There is no direct benefit to individual subjects, other than the payment or course credit they will receive for completing the task.

**12) Costs to Subjects**

None

### **13) Informed Consent**

The investigators will follow Investigator Guidance: Informed Consent (HRP-802). Informed consent (see attachment A) will be presented the beginning of the session. The informed consent will be obtained via qualification through AYTm interface prior to starting any survey. AYTm allows survey control to ensure that the consent must be captured before any survey instrument can be administered. This is a completely voluntary study as it is not a part of any course or job. We do not see any possibility of coercion or undue influence.

It will be made clear during the consent process (before they sign the consent form) that participation is optional and they can leave at any time.

The study will be explained during the consent process (before they acknowledge their consent through the online form). Participants will be told that they will be reading a described scenario and answering questions about the data sharing in this scenario.

### **14) Vulnerable Populations**

The study does not seek to obtain respondents with any specific defining characteristics and will not include individuals who are not yet adults (infants, children, teenagers), pregnant women, prisoners, or adults unable to consent.

## APPENDIX F: QUESTIONNAIRE #1

We invite you to take part in this research study. If you use a smart phone or mobile device, we value your opinions about how applications collect, store and utilize your personal data.

What you should know about this research study:

- You volunteer to be in the study
- The alternative to participating is to not participate, and you can decline at any time
- The total estimated duration of the study is about 10 minutes
- Efforts are made to keep your responses anonymous
- A limited number of research team members will have access to collected data for analysis

This research has been reviewed and approved by the Temple University Institutional Review Board. Please contact the research team with any questions, concerns or complaints about this research by emailing [susan.mudambi@temple.edu](mailto:susan.mudambi@temple.edu). You may also contact the Review Board at (215) 707-3390 or email them at [irb@temple.edu](mailto:irb@temple.edu) for any questions about your rights, to obtain information, or to offer input.

By agreeing to complete this questionnaire, you are not waiving any of the legal rights that you otherwise would have as a participant in a research study.

Click on the arrow in the right-hand corner to continue through each screen as you take the survey.

“Have you ever misrepresented your information online to protect your personal privacy?  
Please tell us what types of things you do to protect privacy.”

---

---

---

---

---

## APPENDIX G: QUESTIONNAIRE #2

We invite you to take part in this research study. If you use a smart phone or mobile device, we value your opinions about how applications collect, store and utilize your personal data.

What you should know about this research study:

- You volunteer to be in the study
- The alternative to participating is to not participate, and you can decline at any time
- The total estimated duration of the study is about 10 minutes
- Efforts are made to keep your responses anonymous
- A limited number of research team members will have access to collected data for analysis

This research has been reviewed and approved by the Temple University Institutional Review Board. Please contact the research team with any questions, concerns or complaints about this research by emailing [susan.mudambi@temple.edu](mailto:susan.mudambi@temple.edu). You may also contact the Review Board at (215), 707-3390 or email them at [irb@temple.edu](mailto:irb@temple.edu) for any questions about your rights, to obtain information, or to offer input.

By agreeing to complete this questionnaire, you are not waiving any of the legal rights that you otherwise would have as a participant in a research study.

Click on the arrow in the right-hand corner to continue through each screen as you take the survey.

I am 18 years of age or older, have read the consent guidelines on the previous screen and agree to take part in this research study.

- Yes, I consent (1)
- No, I do not consent (2)

Downloading mobile applications (apps) onto smart phones and other mobile devices has become very common and popular since their first introduction about 10 years ago. However, many people have concerns about their privacy and about how well their personal information is protected.

To help us better understand this phenomena, please think back to your past behavior when adding mobile applications, and answer the following questions below.

Do you have a smart phone?

- Yes (1)
- No (2)

Use the slider to mark the approximate year you first got a smart phone.

**[Slider here 2007-2018]**

Over the years since you first got a smart phone, approximately how many mobile apps have you added?

**[Slider 0-700 apps]**

On average, how many times a month have you added a new mobile app to a smart phone or mobile device.

**[Slider 1-7 apps]**

Although mobile apps are popular, many people have concerns about their privacy and personal information. To try to protect their privacy, some people provide personal information that is not fully complete, reliable or honest when they add a new mobile app.

To help us understand this behavior, look back and reflect on the mobile apps you have added and answer the following questions.

When signing up for a mobile app, describe how often you have done the following. Never (1); Seldom (2); Sometimes (3); Often (4); Usually (5); Almost Always (6); and Always (7)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Left out or skipped personal information if it was optional. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Abbreviated some personal information, such as initials for a name or only given part of an address. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provided personal information that was accurate in the past, but is not current, such as an old address, old email, or a previous name. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provided an email address that you rarely or never check. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provided some fictional personal information, such as a false name, birth date, address, phone number, gender or email address. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provided more than one form of old or fictional information, such as a combination of an old address and a false birth date. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Completely made up a new false persona. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fully cooperated with all requests for personal information. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Some people are so concerned about their privacy that they provide false or misleading personal information in order to download an app. How do you think that providing false or misleading information makes them feel? Describe these feelings in your own words (minimum of 50 characters).

---



---



---



---



---

**Tell us generally a little more about you.**

What is your gender?

- Female (1)
- Male (2)
- Non Conforming (3)

How old are you?

What is the highest level of school you have completed, or the highest degree you have received?

- Less than high school (1)
- High school or equivalent (2)
- Some college but no degree (3)
- Associate degree (4)
- Bachelor degree (5)
- Graduate degree (6)

## APPENDIX H: SURVEY

We invite you to take part in a research study about electronic applications on mobile devices. We value your opinion on the methods employed by applications to collect, store and utilize your personal data when shared.

What you should know about this research study:

- You volunteer to be in the study
- The alternative to participating is to not participate, you can decline at any time
- The total estimated duration of the study is about 10 minutes
- Efforts are made to keep your responses anonymous
- A limited number of research team members will have access to collected data for analysis.

This research has been reviewed and approved by the Temple University Institutional Review Board. Please contact the research team with any questions, concerns or complaints about this research by emailing [susan.mudambi@temple.edu](mailto:susan.mudambi@temple.edu). You may also contact the Review Board at (215), 707-3390 or email them at [irb@temple.edu](mailto:irb@temple.edu) for any questions about your rights, to obtain information, or to offer input.

By agreeing to complete this questionnaire, you're not waiving any of the legal rights that you otherwise would have as a participant in a research study.

Click on the arrow in the right-hand corner to continue through each screen as you take the survey.

I am 18 years of age or older, have read the consent on the previous screen and agree to take part in this research study.

- Yes, I consent (1)
- No, I do not consent (2)

Downloading mobile applications (apps) onto smart phones and other mobile devices has become very common and popular since their first introduction about 10 years ago. However, many people have concerns about their privacy and about how well their personal information is protected.

To help us better understand this phenomena, please think back to your past behavior when adding mobile applications, and answer the questions in the next couple of screens.

Do you have a smart phone?

- Yes (1)
- No (2)

**[Slider 0-700 apps]**

On average, how many times a month have you added a new mobile app to a smart phone or mobile device.

**[Slider 1-7 apps]**

Have you downloaded and used any of the application types below?

**Check all that apply.**

- Social networking (1)
- Photo storage & sharing (2)
- Music listening & sharing (3)
- Productivity tools (email apps, message apps, file storage & sharing, calendar etc.) (4)
- Transportation (e.g. car service, train tickets) (5)
- Fitness & health tracking (6)
- Financial management (7)

### **Ranking**

Of the apps presented below rank them in the order of how concerned you are about your privacy using them. Drag and drop the apps in the order of concern, 1 being the highest concern to 7 being the lowest concern.

1=Highest Concern about Privacy

7=Lowest Concern about Privacy

- \_\_\_\_\_ Social networking (1)
- \_\_\_\_\_ Photo storage & sharing (2)
- \_\_\_\_\_ Music listening & sharing (3)
- \_\_\_\_\_ Productivity tools (email, message, calendar and file storage apps) (4)
- \_\_\_\_\_ Transportation (car service, train ticket apps) (5)
- \_\_\_\_\_ Fitness & health tracking (6)
- \_\_\_\_\_ Financial management (7)

Scenario Imagine you have recently downloaded a [Scenario].

To establish an account, this app collects personal information such as your name, phone number, address, billing address, birth date, gender.

It also collects information about your usage habits and your community sharing behavior. It collects the type of device you use and the mobile carrier type.

Lastly, the app offers purchase opportunities for additional services and products by the app developer and third parties. If you elect to purchase through the app, the developer will collect your payment information.

***Respond to the questions in the next couple of screens based on using this type of aPp.***

Click on the arrow in the right-hand corner to continue.

Collection For a [Scenario] app, indicate your level of concern about the **COLLECTION** of your personal information. Not at all concerned (1); Slightly concerned (2); Somewhat concerned (3); Moderately concerned (4); Extremely concerned (5).

	(1)	(2)	(3)	(4)	(5)
Collection and use of personal information about me. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Access to other data on my device. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Amount of personal information collected about me at sign-up. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Amount of personal information collected on an ongoing basis. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Amount of personal information that is stored in the app's storage systems. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability to uniquely identify my mobile device. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability to determine my location. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability to collect biometric (face, finger, voice, health) information about me. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Control For a [Scenario] app, indicate your level of concern about the **CONTROL** you have over your collected personal information. Not at all concerned (1); Slightly concerned (2); Somewhat concerned (3); Moderately concerned (4); Extremely concerned (5).

	(1)	(2)	(3)	(4)	(5)
The control you have over your profile information (name, birth date, address, billing address, email). (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The control you have over how the app tracks your app usage. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The control you have over the app's access to other information on your device. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The control you have over the app's access to your personal contacts (friends and family). (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The control you have over information used to personalize the app experience. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The control you have over personal information shared with third parties. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ability for you to cancel or delete your account at any time. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Awareness For a [Scenario] app, indicate your level of concern about your **UNDERSTANDING** of how your personal information is managed by the aPp. Not at all concerned (1); Slightly concerned (2); Somewhat concerned (3); Moderately concerned (4); Extremely concerned (5).

	(1)	(2)	(3)	(4)	(5)
The app provides an accessible privacy policy. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app's privacy policy is easy to understand. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app provides a clear outline of what information it collects. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app explains how it uses the information it collects. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes what third parties it shares your information, what information is shared and how often. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes if it combines the information it collects about you with other third party information it gathers to better understand you. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes how it uses your unique device id and/or phone number. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes how it uses your location data. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes how it uses the information collected from other apps on your device such as personal photos, contacts. (9)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The app describes how it uses biometric information it collects about you. (10)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

More instructions Thank you for providing your viewpoints on [Scenario] app regarding collection, control and awareness of your personal data.

In this study it is also important for us to understand your sharing behavior in the [Scenario] app based on your viewpoints.

Consider your typical personal information sharing behavior in the next question, click on the arrow in the right-hand corner to continue.

Behavior When using this [Scenario] app, how likely are you to share your personal information as described. Extremely unlikely (1); Unlikely (2); Neutral (3); Likely (4); Extremely Likely (5).

	(1)	(2)	(3)	(4)	(5)
Leave out or skip personal information if it is optional. (1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Abbreviate some personal information, such as initials for a name or only part of an address. (2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide personal information that is accurate in the past, but is not current, such as an old address, old email, or a previous name. (3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide an email address that you rarely or never check. (4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide some fictional personal information, such as a false name, birth date, address, phone number, gender or email address. (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide more than one form of old or fictional information, such as a combination of an old address and a false birth date consistently. (6)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Completely make up a new false persona. (7)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fully cooperate with all requests for personal information. (8)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Most of the time, providing personal information is required to gain access to the mobile aPp. When the personal information is **OPTIONAL**, how likely are you to provide information that is fully accurate and complete?

- Extremely unlikely (1)
- Unlikely (2)
- Neutral (3)
- Likely (4)
- Extremely likely (5)

**Tell us generally a little more about you.**

What is your gender?

- Female (1)
- Male (2)
- Non Conforming (3)

How old are you?

What is the highest level of school you have completed, or the highest degree you have received?

- Less than high school (1)
- High school or equivalent (2)
- Some college but no degree (3)
- Associate degree (4)
- Bachelor degree (5)
- Graduate degree (6)