8-11-2017

A Privacy Calculus Model for Personal Mobile Devices

Gregory J. Bott

A privacy calculus model for personal mobile devices

By

Gregory J. Bott

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Business Information Systems
in the Department of Management Information Systems

Mississippi State, Mississippi

August 2017

A privacy calculus model for personal mobile devices

By

Gregory J. Bott

Approved:

Merrill Warkentin
(Director of Dissertation)

Robert F. Otondo
(Minor Professor)

Kent Marett
(Committee Member)

Robert E. Crossler
(Committee Member)

Joel E. Collier
(Committee Member)

Nicole Ponder
(Graduate Coordinator)

Sharon L. Oswald
Dean
College of Business

Name: Gregory J. Bott

Date of Degree: August 11, 2017

Institution: Mississippi State University

Major Field: Business Information Systems

Director of Dissertation: Dr. Merrill Warkentin

Title of Study: A privacy calculus model for personal mobile devices

Pages in Study 186

Candidate for Degree of Doctor of Philosophy

Personal mobile devices (PMDs) initiated a multi-dimensional paradigmatic shift in personal computing and personal information collection fueled by the indispensability of the Internet and the increasing functionality of the devices. From 2005 to 2016, the perceived necessity of conducting transactions on the Internet moved from optional to indispensable. The context of these transactions changes from traditional desktop and laptop computers, to the inclusion of smartphones and tablets (PMDs). However, the traditional privacy calculus published by (Dinev and Hart 2006) was conceived before this technological and contextual change, and several core assumptions of that model must be re-examined and possibly adapted or changed to account for this shift.

This paradigm shift impacts the decision process individuals use to disclose personal information using PMDs. By nature of their size, portability, and constant proximity to the user, PMDs collect, contain, and distribute unprecedented amounts of personal information. Even though the context within which people are sharing information has changed significantly, privacy calculus research applied to PMDs has not moved far from the seminal work by Dinev and Hart (2006). The traditional privacy calculus risk-benefit model is limited in the PMD context because users are unaware of

how much personal information is being shared, how often it is shared, or to whom it is shared. Furthermore, the traditional model explains and predicts *intent* to disclose rather than *actual* disclosure. However, disclosure intentions are a poor predictor of actual information disclosure. Because of perceived indispensability of the information and the inability to assess potential risk, the deliberate comparison of risks to benefits prior to disclosure—a core assumption of the traditional privacy calculus—may not be the most effective basis of a model to predict and explain disclosure. The present research develops a Personal Mobile Device Privacy Calculus model designed to predict and explain disclosure behavior within the specific context of actual disclosure of personal information using PMDs.

DEDICATION

This dissertation is dedicated to my mother and father, Tony and Dixie Bott. When others treated a university education as a primarily a method to find a better job, you stressed the importance of being truly educated and well-rounded. I did not understand at the time, but have been very grateful since. You have never stopped learning and always believed in me.

ACKNOWLEDGEMENTS

First, I want to express deep appreciation and gratitude to Robert Crossler, my initial chair, mentor, and friend. He was integral to the development and completion of this work and my development as a researcher. He often provided feedback, correction, ideas, and wise counsel.

To Merrill Warkentin, who encouraged me to begin the program and helped build the foundation for all of us to become researchers. Early in the program taught us how to think like researchers and to understand the value, method, and purpose of research. He demonstrated consistent and contagious passion for excellence in research and teaching.

To my committee members, Joel Collier, Kent Marett, and Bob Otondo, who were always available and helped me avoid pitfalls, achieve greater clarity, and ultimately complete this work. Each of them spent significant time with me and with this work and without them this would never have happened.

Finally, to my fellow Ph.D. students, Martin Ndicu, Dustin Ormond, and especially Philip Menard. Phil was more than once the sounding board that enabled me to retain my sanity during this process and offered encouragement, insightful ideas and a solid example of how to complete the process. I am glad to have been your office mate.

I must also mention Joe Sullivan. His dedication and care for our cohort as well as his deep understanding of statistics was inspirational.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AA = Alcoholics Anonymous

AMOS = Analysis of Momentary Structures

AVE = Average Variance Extracted

BTS = Bott Technology Solutions

CEO = Chief Executive Officer

CFA = Confirmatory Factor Analysis

CFI = Comparative Fit Index

CFIP = Concern for Information Privacy

CMB = Common Method Bias

CNN = Cable News Network

DF = Degrees of Freedom

DNA = Deoxyribonucleic Acid

EA = Excessive Access

EFA = Exploratory Factor Analysis

FBI = Federal Bureau of Investigation

FERPA = Family Educational Rights and Privacy Act

GPS = Global Positioning System

HIPAA = Health Insurance Portability and Accountability Act

HIT = Human Intelligence Task

IBM = International Business Machines

IFI = Incremental Fit Index

InfoSec = Information Security

iOS = i Operating System

IoT = Internet of Things

IPA = Information Privacy Apathy

IPC = Internet Privacy Concerns

IS = Information Systems

IT = Information Technology

IUIPC = Internet Users Information Privacy Concern

JSON = JavaScript Object Notation

LED = Light Emitting Diode

LW = Local Weather

MMS = Multimedia Messaging Service

MTurk = Amazon Mechanical Turk

NFI = Normed Fit Index

NFL = National Football League

NOAA = National Oceanic and Atmospheric Administration

PC = Personal Computer; Privacy Concerns

PI = Personal Internet Interest

PMD = Personal Mobile Device

PPIT = Willingness to Provide Personal Information to Transact on the Internet

PR = Privacy Risk

RMSEA = Root Mean Square Error of Approximation

SD = Standard Deviation

SEM = Structural Equation Modeling

SMS = Short Messaging Service

SNS = Social Networking Sites

SPSS = Statistical Package for the Social Science

SQL = Structured Query Language

T = Trust

TLI = Tucker-Lewis Index

TPB = Theory of Planned Behavior

TRA = Theory of Reasoned Action

TWC = The Weather Channel

ULMC = Unmeasured Latent Method Construct

US = United States of America

USB = Universal Serial Bus

WMP = Weather by MacroPinch

WU = Weather Underground

CHAPTER I

OVERVIEW

Introduction

As consumers have grown increasingly dependent on personal mobile devices (PMDs), mobile devices, in turn, have embedded deeper and deeper into consumers' lives. PMDs include smartphones such as Apple's iPhone and Samsung's Galaxy series phones based on the iOS and Android operating systems, respectively. Deep embeddedness of the device into the lives of users provides greater functionality and benefit to the user. However, greater functionality and embeddedness come at a cost. App developers and organizations are collecting more and more personal information threatening personal information privacy. Information privacy in the context of the present research is "the right to select what personal information about me is known to what people" (Westin 1967, p. 5). Selecting what information is known, and to whom, is increasingly difficult given the deep integration of PMDs into user's lives.

With more than two million apps in the Google Play store (Statista 2016), PMD users have an overwhelming number of ways to integrate their lives with their PMD. Most apps collect significant amounts of personal information (Federal Trade Commission 2013a; Kane and Thurm 2010). The convergence of the growing user embeddedness into mobile devices and organizations' seemingly insatiable desire for that information results in a constant stream of personal and private information outside of the

PMD—often without prior knowledge or permission from the user (Andriatsimandefitra et al. 2012; Balebako et al. 2013; Enck et al. 2014; Perlroth and Bilton 2012).

Not all organizations nor all apps are seeking to invade users' privacy, and some apps collect much more personal information than others. Social media apps like Snapchat and Facebook and health apps collect a significant amount of personal information (Weissman 2015). While researching his thesis in 2010, Max Schrems, an Australian law student, sent a request to Facebook asking them to send all the data associated with his personal account. Facebook sent only the data for his personal account and it contained 1,200 pages of data in 57 categories (Solon 2012).

Social apps like GroupMe and Facebook Messenger are designed to assist and encourage users to share personal information. They collect a wide range of personal information for use in their respective communities and for marketing and monetization purposes (Jaeger 2014). Health apps monitor sleep habits, blood sugar levels, eating habits, heart rate, stress, and the number of steps walked each day. These wellness apps often share the data they collect with third parties and may do so without worry of regulatory risk (Weissman 2015). With more than 100,000 health apps alone, there are health apps that track individual activity and nutrition, ovulation cycles for couples wanting to have a baby, and apps for individuals struggling with a chemical addiction (Addonizio 2016). There are dozens of Alcoholic Anonymous (AA) apps and Narcotics Anonymous apps available to users to access program materials, find meetings, and read inspirational messages to help maintain sobriety.

Businesses and organizations want access to personal information to better market to existing customers and to identify new customers. Depending on the functions provided by the app, certain permissions are both appropriate and necessary for proper functionality. However, businesses take advantage of consumer need and naiveté and often request and obtain access to information well beyond their functional need (Vijayan 2013). Consumers are largely unaware of the full capability of apps to access their personal information (Balebako et al. 2013). Many mobile apps are free of monetary cost. However, both free and paid apps often collect vast amounts of information about the user without the user's knowledge (Chia et al. 2012). This phenomenon has been explained, in part, by viewing personal information as a tradable commodity (Acquisti 2002; Phelps et al. 2000).

Users sometimes trade data to obtain greater personalization of apps (Xu et al. 2011). In many cases, access to data is necessary for apps to function properly, but often data collection is opportunistic and an invasion of privacy. Customers enjoy the personalization benefits of apps derived from access to personal information, but they also desire control over their personal information. Control over personal information is very important to Americans. According to a 2015 study by Pew, more than 90% of adults indicated being in control of who has access to information about them is important with 74% indicating "very important." Similarly, 90% state that controlling *what* information is collected about them is important with 65% indicating it is "very important" (Madden and Rainie 2015).

Granting certain Android permissions results in loss of control over personal information. For example, apps on an Android-based device may request the permission group, Device and App History, which if granted, enables the requesting app to collect the running apps, access your web browsing history, and other potentially intrusive actions (Chia et al. 2012; Degirmenci et al. 2013; Sarma et al. 2012). If a user has installed an app related to AA, it is likely that he or she would strongly object to companies compiling de facto membership lists of AA by mining mobile devices for the presence of, and activity in, the AA apps. Having this permission enables organizations to do just that. A 2014 study demonstrated that from the apps list alone, personality traits such as religion, marital status, spoken languages, countries of interest, and whether or not the user has small children could be predicted with 90% accuracy (Seneviratne et al. 2014).

Although the personal mobile device is a computer, it is unlike desktop and laptop computers with regard to information privacy control. Consider that this same ability to mine apps for personality traits has been possible on a traditional desktop or laptop computer for the past thirty years or longer, but to the author's knowledge, to the present day, it has never been attempted on a significant commercial scale. Personal computing has experienced a major change with the adoption of the PMD, and that change involves loss of control over information.

The intersection of our time in history, the advancement of mobile technology, the ascension of the Internet to indispensable status, and rapid diffusion of mobile devices laid a foundation for a paradigmatic shift in how the privacy calculus is applied to mobile devices. Current privacy calculus research stems from the seminal work of Laufer and Wolfe (1977) and extends the offline direct mail privacy calculus of Culnan and Armstrong (1999). Within e-commerce, Dinev and Hart (2006) assert that the user makes a rational choice weighing risks of disclosing personal information against the perceived benefits of participating in the transaction. A similar choice to transact is made considering vendor familiarity and trust (Van Slyke et al. 2006), and choice to disclose location to utilize location-based services (Xu et al. 2009). The majority of extant privacy calculus literature, including the articles above, assumes the existence of a rational choice (Wilson and Valacich 2012). One stream of research explores less rational choice-making regarding the privacy calculus (Acquisti and Grossklags 2005; Keith et al. 2013). Rationality is challenged because users often lack sufficient information with which to make a rational decision (Li et al. 2010; Wilson and Valacich 2012), or they discount risks hyperbolically—e.g., a high discount rate over a short period of time and a relatively low discount rate over a long period of time (Acquisti and Grossklags 2003). The important consistency across the research is the assumed existence of a genuine choice, whether rational or irrational. One explanation is that many users do not perceive a choice and in fact may not have one. For example, a user desiring to use Facebook on her Android smartphone has two choices: accept the more than sixty permissions demanded by the app or don't use Facebook. Later versions of the Android operating system mitigate this all-or-nothing approach by enabling users to grant or deny permission selectively. However, users lack sufficient understanding of the reasons or need for the requested permissions (Neisse et al. 2016), so even in the selective context, users give up a significant amount of personal information. In some cases, apps will not function without certain permissions. Hence, the choice is not a genuine one.

Individuals clearly value privacy. However, prior research claims that although users state strong intentions to protect private information, they nevertheless disclose data contrary to their intentions (Barnes 2006; Norberg et al. 2007; Spiekermann et al. 2001). This is referred to as the privacy paradox. Various explanations have been offered to explain why, after stating intentions to protect data, individuals willingly disclose personal information. Foundational to the explanation of user behavior within a PMD is the paradigm above shift in personal computing after the introduction of the iPhone in 2007.

Paradigm Shift

In 2006, when Dinev and Hart (2006) presented their e-commerce privacy calculus, transacting on the Internet was far from commonplace (U.S. Department of Commerce 2016). A consumer had a genuine choice between participating in an e-commerce transaction or obtaining the same outcome from a traditional brick and mortar store. Additionally, consumers understood exactly what information was being disclosed and how. Unlike PMDs, which distribute dozens of information attributes in the background with and without the user's knowledge, on a desktop or laptop computer, Internet information disclosure consists of a user providing information using their browser with a web-based form. The possibility of giving up access to the names, addresses, phone numbers and emails for every contact to purchase a software package for a desktop or laptop computer was inconceivable. Because neither laptops nor desktops typically have access to GPS, obtaining a precise location wasn't feasible. Giving up precise location and access to one's contacts is often an option or mandatory during the purchase of an app (Almuhimedi et al. 2015; Jones and Heinrichs 2012; Sheng et al. 2008; Xu et al. 2009). Consequently, the privacy calculus model presents a risk-benefit model of decision making (Dinev and Hart 2006). The user clearly understood *what* information was being disclosed and the potential benefit for doing so. Until the iPhone was released in June 2007, mobile devices were merely feature-rich cordless (though cellular) phones. Though a laptop computer has many of the same capabilities as a smartphone and typically greater processing power and storage, the laptop is not “with” the user. Unlike laptops, mobile devices are almost always powered on and within reach of the user. As personal as a computer or laptop can be, it does not reach the companion-like status of a personal mobile device.

PMDs are much more personal than any previous computing or communication device, not only because they are with the user, but also because of the information users entrust within it. Users typically store all calendar information for their business or personal lives as well as contact information for their peers or colleagues, one or more social networking apps, a large number of photos, and various apps for music, entertainment, and potentially apps that are required for their job. PMDs are often used for text messages, multimedia messages (MMS), social media communication, email, storing phone call history as well as various forms of instant messaging (WhatsApp, Facebook Messenger, Snapchat, etc.) or collaboration technology (Skype, GroupMe, Google Hangouts). PMDs combine sensing capabilities with data storage, Internet access, and programmability—all of which are essential ingredients of a powerful data collection tool (Raento et al. 2009). A typical high-end phone has an accelerometer used to monitor direction and acceleration, a gyroscope to provide a more precise orientation, a magnetometer to detect magnetic fields, a proximity sensor, a light sensor, thermometer, barometer, pedometer, heart rate monitor, fingerprint sensor, microphone, and multiple cameras (Mylonas et al. 2013). Newer phones even have the ability to detect harmful radiation and can see in three dimensions (Nicas 2015; Yu 2014).

Mobile devices have evolved into a unique context of their own. No other device prior to the smartphone has combined personal technology and personal information so tightly or in such quantity. A smartphone is more than a computer mashed together with a mobile phone. The capabilities and indispensability of a users' mobile device are far greater than the combination of a computer and landline phone. The indispensability of a PMD is reflected in the 2014 Mobile Behavior Report which states 85% of "respondents said mobile devices are a central part of everyday life" (Salesforce.com 2014, p. 33). Nearly 90% said mobile devices allowed them to stay up-to-date with loved ones and current with social events. The "mobile device signifies connectivity to all that's going on in their world" (Salesforce.com 2014, p. 6). PMDs are critical for teens to connect and participate with their peer group. Two quotes from teenagers from a CNN Special Report further illustrate the point: "I would rather not eat for a week than get my phone taken away. It's really bad. I literally feel like I'm going to die." "When I get my phone taken away, I feel kind of naked (Hadad 2015, p. 1)". The traditional privacy calculus which was born out of direct mail and desktop computer access to e-commerce websites fails to account for the indispensability of the PMD and ignores the significant change in demographics by the arrival of Millennials, which, within the context of this study will be synonymous with Digital Natives.

Those born in or after 1982 are commonly called the Millennials (Howe and Strauss 2009). Though the term 'digital natives' is not necessarily synonymous with Millennials, within the United States, the overwhelming majority of this generation would be termed digital natives, and these terms will be used interchangeably in this study. A *digital native* is a child who grew up after the widespread adoption of digital technology. Digital natives grew up with computers, the Internet, and cell phones and have the same level of comfort and familiarity that the previous generation has with the television.

Those born before 1982 who adopt digital technology are classified as *digital immigrants* (Prensky 2001). Digital immigrants experienced the emergence and proliferation of digital technology. They remember a time before computers existed. To a digital immigrant, new technology, by definition, was foreign and unfamiliar. A digital native views a computer like a telephone, radio, or television to those who grew up never knowing a time without them. They are an assumed part of life. These two life experiences (native and immigrant) are markedly different and may lead “today’s students to *think and process information fundamentally differently* from their predecessors” (Prensky 2001, p. 1).

One fundamental difference is how Millennials (digital natives) approach personal information disclosure. To participate in, and be accepted by their community, participation in social media via interesting updates and real life experiences is the norm (Yadin 2012). For Millennials, there is no significant distinction between a virtual (online) friend and a real friend (Yadin 2012). They live in a culture where choosing to abstain from online updates could lead to an isolation problem (Schütz and Friedewald 2011). It is not surprising then that Millennials’ perspective on information privacy is also fundamentally different. In 2010, while addressing the audience at the Crunchie awards in San Francisco, Mark Zuckerberg, CEO of Facebook, said privacy is no longer a social norm. He reflected on his experience starting Facebook as a student at his dorm at Harvard where people asked why they would want to put any information on the

Internet at all. With hundreds of billions of users actively using Facebook in the present, clearly, that perspective has changed. "That social norm [privacy] is just something that has evolved over time," says Zuckerberg (Bradbury 2015, p. 33). It should come as no surprise that the privacy calculus developed for digital immigrants before the introduction of the smartphone, and at a time when e-commerce was purely optional, may need to evolve as well.

Privacy Calculus

Current privacy calculus research has not strayed far from the core conceptual framework first proposed by Culnan and Armstrong (1999) and extended by Dinev and Hart (2006) with most privacy calculus research depicting the user entering into a rational, risk-benefit decision process prior to disclosing personal information (Chellappa and Shivendu 2007; Culnan and Armstrong 1999; Dinev et al. 2006; Dinev and Hart 2006; Kehr et al. 2015; Li et al. 2010; Xu et al. 2009). No research to date has addressed the paradigm shift caused by the introduction of PMDs. Within the context of a PMD, the privacy calculus assumes that a user weighs the benefits of a particular app against the risks associated with installing it. Then, based on a decision process (calculus), the user makes a deliberate and rational decision to disclose personal information in exchange for the app, or additional features for the same premium version of an app. While acknowledging the aforementioned paradigm shift, this study was developed to test a new privacy calculus model designed specifically for the present-day user in the context of a PMD.

Privacy Paradox

The paradigmatic shift of mobile devices has profound implications for paradoxical privacy intentions and behavior. Our research model may also help explain the discrepancy between the level of concern expressed by users compared to the level of protection activity engaged in by users. Users often state a preference for protecting privacy but act in ways that are not consistent with desires to protect their privacy (Acquisti and Grossklags 2005; Norberg et al. 2007). This research will add to our understanding of how or if the privacy paradox applies to information disclosure within the mobile device context. Furthermore, this study measures *actual* personal information disclosure rather than a willingness to disclose, or intent to disclose. A large portion of privacy paradox research only captures intent. It has been suggested that the lack of studies measuring actual information disclosure is one reason for the lack of understanding of the privacy paradox (Bélanger and Crossler 2011; Keith et al. 2013; Wilson and Valacich 2012).

Contribution

Existing privacy calculus research assumes the user engages in a rational risk-benefit assessment. More recent research allows for less rationality and greater influence of situational variables. However, no research to date has considered that the foundation on which the traditional privacy calculus rests has significantly changed. Many of the assumptions simply do not apply to the present indispensability of the Internet, the extremely personal nature of the PMD, and the culture blindly accepting broad disclosure. This confluence of forces compels us to take a fresh look at how privacy decisions are made within the PMD context and to put forth a theory-based model. This research proposes such a model based on prior mobile disclosure and privacy calculus research. The primary contribution of this study is the development of a mobile privacy calculus that takes into account the current disposition to the Internet, the device, and the predisposition to disclose as well as states of resignation and information privacy apathy (IPA). Using this calculus, researchers can better predict and understand user behavior regarding disclosure of personal information on a PMD.

The research question for this study is generalizable within the context of a PMD such as a smartphone, tablet, or a wearable device.

- In what decision process do users engage prior to disclosing personal information on a PMD?

Organization of the Study

The remainder of this paper is structured as follows. Chapter 2 provides an in-depth review of the literature related to information privacy, information privacy concerns, the privacy calculus, the privacy paradox, resignation and information privacy apathy. Chapter 2 also presents the research model, corresponding hypotheses and the reasoning for each hypothesis. Chapter 3 discusses the research method and data analysis to be performed.

CHAPTER II

LITERATURE REVIEW, RESEARCH MODEL, AND HYPOTHESES

Introduction

Chapter two presents the theoretical foundation upon which the research model and mobile privacy calculus are built. The over-arching theory on which this research is based is the privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). Users' behavior follows a "calculus of behavior" impacted by factors that increase or decrease the likelihood of disclosure of personal information. Ultimately this study focuses on how mobile users address issues of information privacy disclosure using their PMD.

Information Privacy

Few concepts have been ascribed with as many meanings or debated so intently across as many disciplines as privacy. No single, agreed-upon definition of privacy exists, though many refer to the succinct definition, "the right to be left alone" as provided by Samuel Warren and Louis Brandeis in their 1890 treatise, "The Right to Privacy" (Warren and Brandeis 1890). Personal privacy comprises solitude, personal space, the right to anonymity, the secrecy of our thoughts, and numerous social norms and mores governing everyday life. Though privacy is viewed as a universal need, the form privacy takes varies greatly from culture to culture (Westin 1967).

Information privacy is a subset of personal privacy. The present study is focused specifically on information privacy within the United States. Though the concept of information privacy pre-dates computers, it is in the context of computers and the Internet that I examine information privacy. More precisely, I am concerned with information privacy on personal mobile devices (PMDs). In this context, I define information privacy as the “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, p. 5). The determination of, or the control of, information flow is the key component of this definition. Control includes both secrecy and confidentiality of data as well as sharing and disclosure. Within the context of PMDs, individuals lack the ability to control the extent of information flow or to whom the information is communicated. This lack of perceived control over one’s personal information leads to greater information privacy concerns (Dinev and Hart 2006).

Information Privacy Concern

Thomas Jefferson voiced privacy concerns with unauthorized and unintended individuals reading posts he sent via the US Mail (Solove 2003). With the arrival of the printing press, camera, telegraph, telephone, each new technological advance has further eroded our ability to control information about ourselves. Today information about individuals is copied, shared, re-shared, and if it was shared on social media, the information is perpetually owned by another entity, such as Facebook. The ease and fluidity of information distribution, reproduction, and alteration pose a grave threat to privacy.

Though the conceptualization and operationalization of privacy concerns has evolved over time, the core definition of information privacy concerns has remained constant. Information privacy concerns are beliefs about which organizations and other entities have access to previously disclosed personal information and how that information might be used (Culnan and Armstrong 1999; Dinev and Hart 2006; Stone et al. 1983; Westin 1967). The greater the uncertainty of who is using the information or how that information is used, the greater the privacy concern (Dinev and Hart 2006).

Smith et al. (1996) created a multi-dimensional scale to measure concern for information privacy (CFIP). CFIP focuses on organizations' collection and use of personal information. The context of the study was offline, consisting of one-way communication, and focused on traditional direct marketing. CFIP comprises four dimensions: collection, unauthorized secondary use, improper access, and errors (Smith et al. 1996). Privacy concerns begin at the point of collection. Concerns increase when collection is irrelevant, perceived as invasive, or information is requested outside of an established relationship. Individuals in the United States rightly perceive that large amounts of personal information about them are being collected from their PMD (Shklovski et al. 2014). Smith et al. (1996) noted that users tended to resent this type of collection. In their study, they divided unauthorized secondary use into internal and external. An example of unauthorized internal secondary use is collecting data ostensibly to be used for the one purpose but actually used for another. Examples of external use are direct marking (Culnan 1993), or otherwise renting or selling customer information to third-parties. Improper access encompasses the concept that collected information should only be accessed by individuals that have a "need to know." Federal laws such as those governing student records (FERPA) and personal health information (HIPAA) codify this concept. Errors contained in personal data can be highly problematic, and Smith et al. (1996) note that companies should place greater concern on the accuracy of individuals' information.

Malhotra, Kim, and Agarwal (2004) developed the Internet Users' Information Privacy Concerns (IUIPC) measurement scale. Based on Smith et al. (1996), they characterize the notion of IUIPC in three dimensions: collection, control, and awareness of privacy practices. Collection is defined as "the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of the benefits received (Malhotra et al. 2004, p. 338)." As stated earlier, control is central to privacy concerns. If an individual perceives he has control over his personal information via opt-out mechanisms, approval/disapproval, modification, or by exiting the transaction or relationship, his privacy concerns will be lower. Control over personal information is paramount given the risks of disclosure. An individual's privacy concerns "center on whether the individual has control" of disclosure of personal information (Malhotra et al. 2004, p. 339). Privacy awareness is the degree to which a consumer is concerned about his or her awareness of organization information privacy practices. A privacy-aware user will seek privacy.

For both Android and Apple PMDs, a core requirement and nearly unavoidable first step are to register your unique Apple ID or Google account on the respective device (Apple 2016; Google 2016). Though it may be possible to operate said devices without providing a specific user account, the practical use of the device is severely diminished absent a valid Apple ID or Google account. Furthermore, it is doubtful that the typical

PMD user would know how to bypass this step (Purdy 2012). Thus, data collection begins moments after a PMD is powered on. It is demanded by the provider and necessary for full functionality. For Android users prior to the version 6.x release (code-named Marshmallow) of the operating system, the ante is much higher. Many popular, “essential” apps such as Facebook and Snapchat, request dozens of permissions, however, prior to the Marshmallow release, users had an all-or-nothing choice—either accept all 62 permissions requested by Facebook (Chia et al. 2012) or do not use Facebook on your PMD (Elenkov 2014). For iPhone users and Android users post version 5.9, a selective approach to disclosure is possible. For some permissions, users are given the option to grant or deny access, though a significant number of permissions (including the unique ID of the device and listing all apps) are granted without the ability to block them. Thus, for the PMD user, collection is a foregone conclusion.

Despite mandatory collection and the all-or-nothing permissions approach, hundreds of millions of users download apps disclosing huge amounts of information (Federal Trade Commission 2013a). This is another symptom of the aforementioned paradigm shift. The extended privacy calculus research was published prior to the release of the iPhone. Outside a PMD, if a user perceived that a particular website collected information beyond what was necessary for the transaction, they could simply choose a different website or arrange an alternative (brick and mortar) option to obtain the good or service they desired. Within the context of the PMD, the moment you set up your phone and downloaded an app, your data has already been and is being, collected. The data collection landscape has drastically changed after the release of the iPhone in 2007.

It is important to note the scope of the paradigm shift with respect to data collection. Within the PMD context, data collection is either assumed and generally accepted, or users are unaware of data collection (Balebako et al. 2013; Kane and Thurm 2010). Within the traditional personal computer context, data collection is NOT the norm nor is it generally accepted. The privacy backlash handed to Microsoft Corporation over its collection of telemetry information provides an example. It wasn't until the release of Windows 10 that Microsoft joined the other tech giants in aggressive data collection. Geoffrey Fowler of *The Wall Street Journal* compares Windows 10 to spyware though he admits that it does nothing different than Facebook or Google (Fowler 2015). Fowler states Windows 10 is the most aggressive data collector of any previous operating system but fails to recognize that data collection on the PC is minor compared to both the scope and depth of data collection on a PMD. Because users carry PMDs on their person nearly all the time, PMDs contain much more personal information than a PC and yet no alternatives exist for the user to avoid data collection on the PMD. On the PC, Microsoft offers numerous methods to limit or stop data collection within its operating systems, data collection on smartphones cannot be stopped. Both Apple iOS devices and Android devices post version 5.9 allow the user to lessen data collection, but not stop it. Thus, I argue that basic level of data collection is assumed and perceived as inevitable to the user.

Similarly, errors as an information privacy concern are notably absent from current literature (Degirmenci et al. 2013; Lutz and Strathoff 2014; Miltgen and Peyrat-Guillard 2014; Xu et al. 2012). Perhaps this is due to advances in technology, the automated nature of data collection, or simply the sheer amount of data collected resulting in cross-checked and verifiable data. Malhotra et al. (2004) omitted concern for erroneously collected information from IUIPC. In similar manner, I assert that users have no significant concern over erroneously collected data in the context of PMDs.

Although users remain concerned about collection of personal data, erroneous data about themselves, improper access of the personal data, and secondary use of the data, they have no ability even to imagine how or who might be using their data and in what ways. The typical user is wholly unaware of the enormity of the data collection constantly occurring on their mobile device. Many have never considered that information about them leaves their phone at all (Balebako et al. 2013). Perhaps this is because of the extreme difficulty of ascertaining even the most basic feedback about what information is being shared outside of the PMD. Where previous privacy concern research measured the willingness of users to explicitly and deliberately provide their personal information to fill out a form to complete a transaction, information in the PMD context is collected behind the scenes. Personal information is siphoned from the PMD without ever notifying the user. Because of this lack of visibility, lack of understanding, and inability to trace or even form a viable guess as to where this information goes, traditional privacy concerns are excluded from our research model and replaced with what the user can *actually* observe, namely, excessive access. This is in line with research in the mobile context that found that a consumer's general privacy concern did not have any effect on actual personal information disclosure (Keith et al. 2013; Xu et al. 2009). Instead of drawing upon a general privacy concerns or other abstract privacy concerns, users may leverage observable information in the form of the app brand, or developer familiarity, combined with excessive access to drive the privacy calculus for mobile devices. These factors are discussed later in this chapter as Familiarity, Excessive Access, and Distrust. These three factors combined with Perceived Need, Resignation and Information Privacy Apathy form the Personal Mobile Device Privacy Calculus.

Privacy Calculus

Since the advent of computers, information privacy concerns have steadily grown into a crucial issue for consumers (Federal Trade Commission 2012, 2013b; Westin 2001). A key to understanding privacy as a social issue is the concept of a "calculus of behavior" (Laufer and Wolfe 1977). It is an assessment of, and trade-off between, perceived risks and expected benefits. Perceived risk is regulated and impacted by control belief. Individuals choose to disclose information or to participate in certain activities based on the belief they have control or at least have some ability to manage information, both now and in the future to minimize potential consequences.

The privacy calculus theory is often called upon to explain and predict the disclosure behavior of individuals. Based on a social contract between the customer and the organization, Culnan and Armstrong (1999) argue for organizations to demonstrate "procedural fairness" by adopting and communicating fair information practices. Furthermore, they posited that prior to the disclosure of personal information required to transact for product and services, consumers enter into a privacy calculus (Culnan and Armstrong 1999).

The privacy calculus applies not only to tangible goods and services but also to Internet transactions (Dinev and Hart 2006; Malhotra et al. 2004). Dinev and Hart (2006) proposed an extension to Culnan and Armstrong's (1999) privacy calculus to explain an individual's willingness to disclose personal information to transact on the Internet (See

Figure 1). Both Internet Privacy Concerns (IPC) and Internet Trust (T) mediate the relationship between Perceived Internet privacy risk (PR) and intent to disclose (PPIT). PR refers to the user's perceived risk associated with the opportunistic collection of personal information disclosed. Subsequent studies have identified factors altering perception of risks and benefits, e.g. online shopping communication (Spiekermann et al. 2001), familiarity (or lack of familiarity) with the vendor (Van Slyke et al. 2006), emotions, awareness of privacy statements, and sensitivity of information (Li et al. 2011), high monetary rewards (Malhotra et al. 2004; Xu et al. 2011), situation-specific considerations (Keith et al. 2013; Wilson and Valacich 2012) such as cognitive absorption (Alashoor and Baskerville 2015).

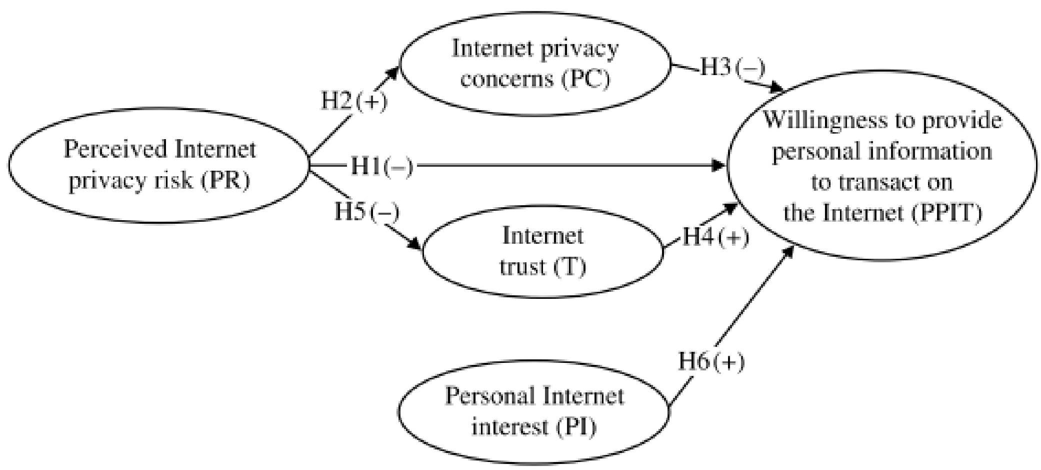


Figure 1 Hypothesized Relationships of the Extended Privacy Calculus Model

However, the overwhelming majority of studies have utilized behavioral *intent,* rather than *actual* behavior (Bélanger and Crossler 2011). The dependent variable of the extended privacy calculus model (see Figure 1) is *intent* to transact ("Willingness to provide personal information to transact on the Internet [PPIT]") rather than performing an actual transaction. Within the framework of the Theories of Reasoned Action (TRA) (Ajzen and Fishbein 1980) and the Theory of Planned Behavior (TPB) (Ajzen 1985) IS research results have repeatedly demonstrated the high correlation between behavioral intentions and actions. Despite this consistency in other areas of IS research, intentions to disclose do not accurately predict actual disclosure behavior (Bélanger and Crossler 2011; Keith et al. 2013; Smith et al. 2011).

The Dinev and Hart (2006) extended privacy calculus model assumes congruency with expectancy theory, which states users will make choices that minimize negative outcomes and maximize positive ones (van Eerde and Thierry 1996; Vroom 1964). An important aspect of expectancy theory for the context of this research is the core assumption of the privacy calculus that users perform a rational assessment of costs and benefits of the behavior prior to disclosure.

The choice to disclose is motivated by a perception of benefit and absence of perceived risk or consequences. If disclosing information results in a direct benefit to an individual, and that benefit is greater than the perceived risks or potential consequences, the traditional privacy calculus indicates an individual will likely disclose information (Culnan and Armstrong 1999; Dinev et al. 2006; Dinev and Hart 2006). Individuals may choose to withhold information if they consider that at some point, even in the distant future, their ability to manage or control information is not certain (Featherman et al. 2006).

However, individuals are more likely to disclose information and to view the collection of information as less privacy-invasive when the following are true:

- Information requested seems relevant to the context in which it is being collected
- Information is collected from a vendor or organization with whom a previous relationship exists
- The individual perceives some level of control or management of that information
- The individual believes information will be used to draw relevant and accurate inferences about them (Stone and Stone 1990).

To make a rational, even a subjectively rational choice, users must be able to critically assess the risks as well as the benefits associated with disclosure. Much privacy calculus research has rational user behavior as a core tenet (Dinev and Hart 2006; Malhotra et al. 2004; Xu et al. 2009); however, users are limited in their understanding of risk and prone to time-distortions involving risk assessment (Acquisti and Grossklags 2003; Laibson 1997). Users are limited in their understanding of privacy disclosure implications because of information asymmetry. Beyond messages mandated by the Android operating system and arcane privacy policies, mobile app developers do not disclose how information is used (Enck et al. 2014). Without such information, users are unable to make rational or informed decisions based on who is using information, and how that information will be used. Absent contrary information and bolstered by the future discounting of risk, users are more likely to disclose personal information for relatively small perceived benefits (Tsai et al. 2011). Although providing users easier access to privacy policies and stating how information will be used increases rational behavior in users, disclosure behavior is not a purely rational decision-making process.

Almost forty years ago, Laufer and Wolfe (1977) warned that with the advent of the digitalization of data, large amounts of personal information would be aggregated and used in ways unknown to the user: “The presence of computerized data banks’ use of Social Security numbers as personal identifiers for all sorts of transactions mean that at some point a mass of information about an individual can be compiled by unknown persons for unknown purposes” (Laufer and Wolfe 1977, p. 37) Perhaps one of the first tangible effects felt by the consumer as a result of this unexpected aggregation of personal information (or “secondary use”) was direct marketing (“junk mail”). Participants in the 1993 study by Culnan regarding direct marketing indicated a desire for control over who received their information and what would be done with it. Subjects that felt they had greater control had a more positive attitude towards organizations that collected their information. Consistent with the privacy calculus theory, participants perceiving a benefit for disclosing were more likely to share personal information.

Given the extant research surrounding the alleged privacy paradox, measuring intent to disclose, rather than actual disclosure, could prove problematic (Smith et al. 2011) and result in mismatched results between intentions to disclose and actual disclosure (Bélanger and Crossler 2011). Chapter 3 discusses capturing actual disclosure to avoid possible effects from the so-called privacy paradox.

Privacy Paradox

Austin Hill, security and privacy entrepreneur humorously summarizes the privacy paradox, “If you ask a room full of 100 people whether they care about online privacy, 80 people raise their hands. If you asked the same room full of people if they are willing to donate a DNA sample in exchange for a free big Mac, 80 people would raise their hands (Marsan 2000).” Hill refers to the discrepancies between users’ *stated* privacy concerns and their *actual* disclosure behavior. This discrepancy has been termed the privacy paradox (Acquisti and Gross 2006; Norberg et al. 2007). Despite much privacy paradox research, results are inconclusive. Several solutions or explanations for the privacy paradox have been offered. Perhaps most salient is the use of intent to disclose rather than actual disclosure to detect paradoxical behavior. Keith et al. (2013) find support for the privacy paradox only in that "[personal] information disclosure intentions poorly explain actual information disclosure even though it is a statistically significant indicator" (Keith et al. 2013, p. 1164). In the same study, they found results opposite of the privacy paradox. Subjects that intended to disclose did not disclose. Results from their study contradict expected paradoxical privacy behavior.

Other studies challenge the deliberate and rational decision-maker assumption present within the privacy calculus literature. Users have limited information about how information is disclosed, to whom it is disclosed, with what frequency, and how that information might be used (Acquisti 2002). Even if users possessed this information, they lack the expertise to comprehend the full implications and consequences of disclosing personal information (Acquisti and Grossklags 2003). Immediate gratification and self-control problems may be better predictors for users that intend, but fail, to protect information (Acquisti 2004). Users may be enlarging near-term benefits and disproportionately discounting future risks (hyperbolic discounting) (Acquisti and Grossklags 2003). Furthermore, users are generally reticent to apply privacy protective measures (Warkentin et al. 2011), lack symmetry of information, and they also lack the technical expertise to understand how and by whom information can be collected (Acquisti and Grossklags 2005). The present study recognizes that users lack both symmetries of information and collection expertise and proposes a variance model (see

Figure 2) to explain and predict the outcome of disclosure (or lack of disclosure) based on a decision calculus.

Research Model and Hypotheses

The present study has a well-defined context (PMDs and the Google Play store), consistent disclosure mechanisms (same set of apps presented to each user), measures *actual* disclosure rather than intent, and presents a real-world scenario with real risk. The apps presented for review are apps available in the Google Play store rather than obviously contrived, obscure apps developed only for research. Three of the apps, AccuWeather, The Weather Channel, and Yahoo! Weather have been downloaded millions of times from the Google Play store. The other two apps are more obscure, but still publicly available with thousands of user reviews. To demonstrate the applicability of our research model (see Figure 2) I utilize real-world apps to avoid the potentially skewed data that may result from user's perception they are using a "pretend" app developed only for research and is consequently free of significant or actual risk.

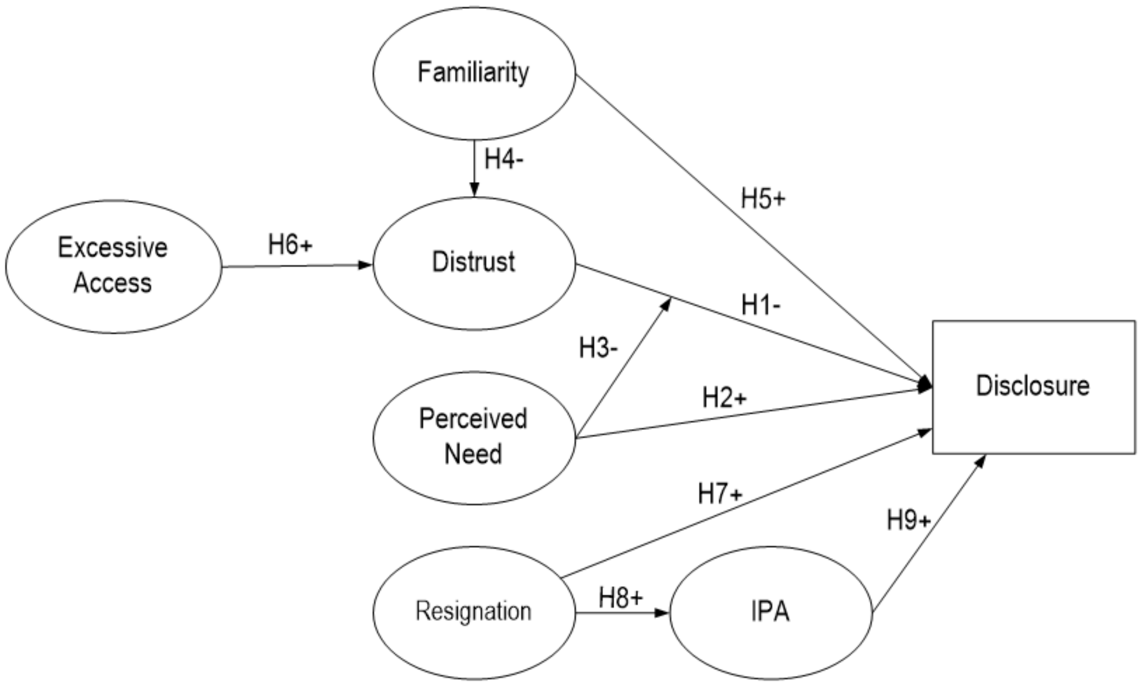


Figure 2 Research Model

Trust and Distrust

Trust is not modeled as a construct of interest. An explanation for the absence of trust in the model may be useful. Trust is “the confidence a person has in his or her favorable expectations of what other people will do, based, in many cases, on previous interactions” (Gefen 2000, p. 726). It is a “solution for specific problems of risk (Luhmann 2000, p. 94).” Trust in the context of this study is engendered by the Google Play store infrastructure. Specifically, as with other familiar and respected online stores (e.g., Apple’s Marketplace) and brick and mortar stores, users assume a baseline level of safety and quality (Harbach et al. 2014).

The PMD app install process is another facet of the paradigm shift. Though users also install applications on personal computers (PCs), the experience is markedly different. PC Users install relatively fewer applications and typically obtain them from reputable vendors. PMD users, however, download a significantly greater number of apps and often do so from unknown sources (Gates et al. 2014). PC applications are available in disjointed marketplaces--applications may be obtained directly from the creator (e.g., Microsoft Store, Intuit.com, etc.), from a retail outlet (Wal-Mart, Best Buy), an obscure website, or may be bundled with a PC. Though multiple options exist for the PMD user, the vast majority of apps are downloaded from within a marketplace (Gerlich et al. 2015). If the method by which users obtained apps has experienced a paradigmatic shift, there are major implications for the disclosure decision process (calculus).

Apps in Apple's Marketplace are vetted prior to distribution and removed from the approval process if they violate Apple policy (Felt et al. 2011). Google aggressively filters harmful apps using a technology dubbed "Bouncer" (Weichselbaum et al. 2014). Furthermore, products not meeting such minimum standards would result in a highly visible backlash from customers negatively impacting downloads and potentially prompting removal of the offending product. Certainly the possibility remains that a rogue, malicious app lurks in the store, but nevertheless a general acceptance and trust pervades the user experience (Kurkovsky and Syta 2010). Because accountability is assumed within the primary marketplaces (Apple Marketplace and Google Play store), distrust may prove to be the more compelling predictor of disclosure and non-disclosure.

Distrust is not simply the absence of trust. Nor is distrust necessarily on the same continuum with trust—they often occupy different, distinct roles (Cho 2006) and can be viewed as a two-process model (Komiak and Benbasat 2008). A gradual erosion of trust does not equate to a gradual increase in distrust. Rather the presence of distrust obliterates trust altogether (Gefen et al. 2008). After significantly reducing or eliminating trust, the conceptual presence of distrust forces the app user to much more carefully consider the consequences of disclosure.

Prior research indicates both trust and distrust are predictors of risk. However, distrust is more effective predicting high-risk perceptions (McKnight et al. 2004). Because the user already trusts the marketplace and either has already accepted data collection or is ignorant of it, this study assumes that a user's primary concern is high-risk perceptions. Consequently, although trust is a key construct in the traditional privacy calculus, this study uses distrust to predict risk. Because users have a baseline trust of the marketplace, they routinely install apps from unfamiliar developers. However, it is the presence of distrust that causes a user to forego installation of an app (Anderson 2015). Consequently, this study measures distrust and hypothesizes that:

H1: Distrust will be negatively associated with the user's disclosure of personal information.

Resignation

A user is in a state of resignation when he or she believes an undesirable outcome is inevitable, and nothing they do will affect or change it (Turow et al. 2015). In that sense, resignation is very similar to learned helplessness. In psychology, an individual in a condition of learned helplessness feels powerless to alter his outcome. This condition often arises from a traumatic event or a series of events resulting in persistent failure (Maier and Seligman 1976; Peterson et al. 1995; Seligman and Maier 1967).

Martin Seligman and Steve Maier (1967) demonstrated learned helplessness using dogs in an experiment at the University of Pennsylvania. Three groups of dogs were harnessed and placed on a metal surface that transmitted an uncomfortable level of electric shock. The first group was given the ability to terminate the shocks by pressing a lever, but pressing the lever provided for dogs in the second group did nothing to affect the length of the shock. The third group of dogs was a control group and was harnessed and released without being shocked. Because pressing the lever had no termination effect for the second group, and because the shocks seemingly occurred at random, the second group eventually learned shocks were unavoidable (Seligman and Maier, 1967). Seligman and Maier then placed the dogs into shuttle boxes. Each box was partitioned by a short divider over which the dogs could easily jump. The floor of one partition of the shuttle box delivered an electric shock while the floor of the other partition did not. Subjects in the first group, when shocked, jumped out of the first partition into the second to avoid the shock. Subjects in the second group, when shocked, made no attempt to jump over the divider though they could have easily done so. Their inactivity supports the proposition that animals can learn helplessness--that they can learn they have no ability to affect the outcome of their situation. Consequently, they make no further attempts to do so (Maier and Seligman 1976).

Similar experiments have been applied to cats (Thomas and Dewald, 1977) and rats (Maier and Testa, 1975) with similar results. The study was also applied to college students, though with a loud sound rather than electric shock. Students were divided into two groups with one group having a working device to terminate a loud sound, and the other group's device had no effect on the sound. The results with the college students closely aligned with the results Selig and Maier found using the dogs and shuttle box (Peterson et al. 1995).

I propose that individuals may suffer from a similar privacy learned helplessness that I term *resignation*. Either as a result of multiple privacy invasions (Yoo et al. 2012) or as a result of the perception that one's personal information is already irretrievably "out there," one may develop a stance of futility toward protecting personal information (Keith et al. 2013; Warkentin et al. 2006). I see parallels between the qualitative results from (Yoo et al. 2012) and subjects that are in a state of resignation and perceive (have "learned") that no action on their part to protect their personal information will have any positive effect on their outcome. Specifically, one subject stated, "But after similar incidents, I became quite insensitive to personal information hacking even though I still worried about potential danger." (Yoo et al. 2012, p. 7)

According to a 2015 Annenberg survey and contrary to much of the privacy calculus literature, most Americans do not willingly trade information for benefits. The study points to resignation as the explanation rather than to a privacy economics decision or digital commerce ignorance. Furthermore, the Annenberg 2015 study found that "people who know more about ways marketers can use their personal information are *more* likely rather than less likely to accept discounts in exchange for data when presented with a real-life scenario" (Turow et al. 2015, p. 3). One explanation for this finding is a deeper understanding of the broad capabilities of information collection and dissemination increases a PMD user's level of resignation.

Attempting to control access (or understand who has access) to one's personal information contained within a PMD could very easily be met with persistent failure. Individuals with a greater understanding of how information is collected, used, and potentially distributed are more likely to perceive failure, and more likely to exhibit greater levels of resignation. Consequently, I hypothesize the following:

H7: Resignation will be positively associated with the user disclosure of personal information.

H8: Resignation will be positively associated with information privacy apathy.

Perceived Need

Perceived need is defined as the requirement of something because it is essential or very important. Need refers to the "disparity between an individual's present state and a goal (or desired) state" (Mishra and Lalumière 2010). A user's perceived need for an app or service motivates installation of that app, and a high perceived need will override other protective factors (Li et al. 2010). Perceived need has been shown as a reason users divulged their location (Xu et al. 2009, p. 147) as an "overriding interest"—which may be more aptly termed a "strong want"—and bypass the rational risk-benefit assessment of the privacy calculus (Dinev and Hart 2006). User's perceived need by a third party (the government) is used to explain greater acceptance of surveillance (Dinev et al. 2008).

Despite the identification of perceived need in prior research, the perceived need of PMDs is unique and a key component in the paradigm shift discussed in Chapter 1. Unlike legacy cellular telephones or desktop or laptop computers, PMDs are essential artifacts of personal, everyday life. Dan Siewiorek describes the role of PMDs as a "constant companion, helper, coach, and guardian (Siewiorek 2012)." The traditional cellular telephone, desktop computer, and laptop computer never attained such a role. PMDs are distinguished from laptop and desktop computer by their unique functionality as provided by the myriad of apps available. Consequently, the PMD has reached indispensable status for most, and borders on addiction for some. Users place a high practical and monetary value on PMDs, keep them close at all times, habitually or compulsively checking them throughout the day and often exhibit high anxiety at their loss or malfunction (Lee et al. 2014). This level of PMD criticality results in a perception of need not experienced in prior technological contexts and demands a fresh look at the corresponding implications regarding privacy decision-making around personal information disclosure and risk-taking.

Humans and animals are generally risk-averse, preferring more predictable, stable outcomes. For example, a bird needing 1,000 calories to survive the night, but lacking 400 calories is in a situation of mortal high need. If the bird is given a choice of two patches: a low-risk patch guaranteed to provide 100-150 of the 400 calories needed for survival and a high-risk patch that may yield anywhere from 50-500 calories, the bird will shift from risk-aversive behaviors to risk-prone behaviors. This pattern of risk behavior is called the energy-budget rule and applies to humans as well as animals (Kacelnik and Bateson 1996; Mishra and Lalumière 2010). PMD users place a high need on their smartphone. Nearly 50% of smartphone users indicate that the PMD is something "they couldn't live without" (Smith 2015, p. 7). I assert that just like the calorie-deficit birds, PMD users that perceive a high need for an app will shift from risk-averse behaviors to risk-prone behaviors.

The majority of privacy calculus research assumes individuals follow a pattern of maximizing desirable outcomes. However, a significant body of research indicates users act contrary even to stated desires of maximizing actual outcomes (Barnes 2006; Norberg et al. 2007; Wilson and Valacich 2012). According to the energy-budget rule, individuals will not seek an optimal outcome, but instead will seek to avoid outcomes that fail to meet their needs. Rather than methodically evaluate each option for an optimal solution, as assumed by the traditional privacy calculus, users tend to select apps based on "good enough" reasoning. These individuals are employing "satisficing" decision-making (Simon 1996). Like the foraging birds, PMD users perceiving a high need for an app will shift from risk-averse disclosure behaviors to risk-prone behaviors. Therefore, I hypothesize the following:

H2: A user's perceived need will be positively associated with the user's disclosure of personal information.

H3: A user's perceived need will negatively moderate the relationship between distrust and disclosure of personal information.

Familiarity

As users gain experience with how an entity (e.g., organization, brand, developer) collects and protects personal information, perceptions of risk may be determined by the familiarity of the entity more than information privacy concerns. Depending on whether historical experience with an entity is positive or negative, familiarity may increase either trust or distrust (Luhmann 1979). Prior research indicates that experience with IT technology innovation influences intent to use. Intent to use technology differed between those without experience and those who, by experience, were familiar with the technology (Karahanna et al. 1999). Ecommerce customers differ in willingness to transact based on experience (familiarity) with the vendor (Gefen et al. 2003; Kim and Park 2005). In a study comparing willingness to transact with a more familiar online web merchant with a less familiar one, familiarity had a larger impact on willingness to transact than trust (Van Slyke et al. 2006).

In the context of this research, I define familiarity with apps as recognizability based on prior experience with the app itself. It is knowledge of the who, what, how, and when of the present (Luhmann 1979). Familiarity results in decreased uncertainty of why, how, and what is happening in the present (Luhmann 1979). Gefen et al. (2003) notes in the context of ecommerce that unfamiliar websites, or experience with a website that is overly difficult to use, may imply the e-vendor is acting opportunistically or deceptively (Gefen et al. 2003). Familiarity with the present process linked to similar prior experiences where the user was not exploited reduces these concerns (Gulati and Sytch 2008). Consequently, because unfamiliarity increases distrust and familiarity reduces concerns over exploitation, I hypothesize the following:

H4: A user's familiarity with an app will be negatively associated with distrust.

H5: A user's familiarity with an app will be positively associated with the user's disclosure of personal information.

Excessive Access

The installation process employed by the Google Play store includes a mandatory permissions window that must be accepted prior to installing an app. The Android operating system requires express permissions from the user prior to allowing access to certain types of information and capabilities of the PMD. Applications may request zero to dozens of permissions. Applications may request only the permissions required to provide the promised features of the app or the might request permissions in excess of what is required. The process assumes users pay attention to such notices and can associate the permissions with risks and make a rational decision. However, many users are unable or unwilling to correlate risks with the level of permissions granted to a PMD

(Chia et al. 2012; Felt et al. 2012). Users desiring to select only necessary permissions for apps may struggle because permissions descriptions such as “full Internet access” and “read phone state and identity” are difficult to translate into how those capabilities might be used to harm or benefit the user (Cranor et al. 2006). Felt et al. (2012) indicated that only 20% of users indicated awareness of permissions when installing an app. This is further complicated by some permissions that are only visible by tapping “See more.”

Users choose apps to install based on their features and benefits. Users desire the capabilities, entertainment value, social connection, or utility that an app provides (Sawers 2015). And although users are not necessarily familiar with the permission structure of Android apps (Sarma et al. 2012), users confronted with app permissions are able to perceive a mismatch between the permissions requested in the function of the app. According to 2015 Pew Research Center study on mobile apps and privacy, 60% of smartphone users chose not to download an app after they discovered how much personal information was required by the app (Anderson 2015). Even if their assessment is inaccurate, an app requesting either a large number of permissions or permissions not relevant for its function, is considered excessive access.

A clear majority of users involved in an ecommerce transaction believe that information disclosed to complete an ecommerce transaction will be used for marketing purposes (Acquisti and Grossklags 2005). PMD users are frequently exposed to mobile advertising, especially on apps distributed free of charge. Coupled with the assumption that their information is valuable to third-party organizations as well as their ability to forego apps based on overly intrusive information requests, I theorize that apps requesting excessive access to PMD functionality and information will result in greater distrust.

> *H6: The user's perception of excessive access of device permissions will be positively associated with distrust.*

Information Privacy Apathy

Apathy implies indifference. In the context of information contained on a user's mobile device, information privacy apathy (IPA) is indifference towards the disclosure of that personal information. Scant literature exists because IPA is a relatively new concept in information privacy literature (Yoo et al. 2012). Depending upon the context of a particular situation, individuals may demonstrate a range of privacy behavior from extreme concern to apathy (Acquisti et al. 2015). It differs from resignation in that an apathetic user may have the ability to protect his information (affect an outcome), but simply not care to do it. Furthermore, users resigned to the futility of protecting personal information may still place a high value on their personal information and exhibit frustration and resentment in a disclosure situation whereas an apathetic user does not place high value on his personal information.

IPA may arise from lack of value or importance attached to privacy in general, or to information contained in the PMD in particular (Boss et al. 2009). Information privacy apathy may stem from, or be magnified by, resignation. The notion that a user's information is already in the hands of countless third-party organizations and any action taken now to protect information already disseminated is too little, too late (Sharma and Crossler 2014). Users who perceive that their information has already been distributed place a lower value on that information, and display a higher inclination to disclose personal information (Yoo et al. 2012). Faced with legal and logistical complexity and difficulties, companies may also succumb to privacy apathy (Schreider 2003).

Furthermore, individuals that heavily utilize social media and other privacy-invasive apps may have already accepted Scott McNealy's notion that consumer privacy is actually just pretend, a "red herring" (Sprenger 1999, para. 1) Per McNealy, "You have no privacy anyway. Get over it" (Sprenger 1999, para. 3). Perspectives such as these lead to a lack of motivation to act. Consequently, I theorize a lack of motivation to protect one's information (a higher level of information privacy apathy) is associated with higher levels of disclosure.

H9: A user's level of information privacy apathy will be positively associated with the user's disclosure of personal information.

CHAPTER III

RESEARCH METHOD

Introduction

Chapter three describes the design and research method employed in this study. First, the sample population is presented and discussed. Then the study design, data collection process, instrument design and measurement items are described. Measurement scales for each of the constructs along with the source, original items, and modified items are listed in this chapter. Finally, construct validity, the use of exploratory and confirmatory factor analysis, and mitigation of common method bias as well as the tools and analytical techniques employed are presented.

Sample Population

Undergraduate and graduate students at a southeastern university and participants from an online panel compose the subjects for this study. The value and appropriateness of using students as subjects have been debated across disciplines and is often challenged on the basis of generalizability (Compeau et al. 2012; McKnight et al. 2002). In some contexts, college students are a unique population and great care must be taken when using them as the unit of study, if an objective of the research is to generalize to a population beyond students. Using both students and the general population represented by a national online panel increases the generalizability of this research.

This study presents a new context-specific privacy calculus model to better explain, predict, and clarify the process mobile device users employ when choosing whether or not to disclose personal information contained in their PMD. The goal of this research is to generalize this model to the larger population of PMD users. To achieve this goal, subjects must understand how to use a PMD and place value on the personal information it contains. They must understand how to install an app and be able to assess their familiarity (or lack of familiarity) with the app, developer, or brand. They must also be able to form an opinion (accurate or not) as to whether the permissions requested by an app are appropriate for its function, or are in excess of its function. Both graduate and undergraduate students fulfill these requirements.

In addition to fulfilling the requirements, students are arguably the ideal population for a study involving mobile device usage. This study presents a novel decision process that offers an explanation for how individuals decide to disclose, or not disclose, the personal information contained on their PMDs. In the context of this study, students are an appropriate sample for three reasons. First, the age group to which students belong comprise a key demographic in the U.S. smartphone and mobile device market. The 18-24 age group has an 80% penetration of smartphone usage, which is the highest percentage penetration of any age group (Webster 2014). According to a 2015 study by the Pew Research Center (Smith 2015), younger (18-29) users dominate the percentage of subscribers utilizing the core features of smartphones (text messaging, Internet use, voice/video calls, email, SNS, video, and music). Second, this study measures the decision to install, or not to install an app, and students routinely make install and no-install decisions (Madden et al. 2010). Third, although technical expertise and proficiency are not by-products of youth, this age group clearly has a solid understanding of how to operate a mobile device, and the mobile device plays an important role for the student to maintain community and connection with his or her peers (Lenhart et al. 2015). These three attributes of students are foundational to generalizing results to a larger population of personal mobile device users: a general understanding and familiarity with the mobile device, the ability to install or not install an app, and an assessment of the individual's perceived need for an app. However, to increase generalizability, I will engage a more general set of users, including students, by using Amazon Turk (MTurk).

Because an individual's perceived need for an app is unique to that individual, an important step in the design of this study was to select an appropriate set of apps for review. Weather apps were selected as that set. A list of the weather apps selected for this study appears in Table 2. The assumptions and rationale used in making this choice include the following.

- Weather is a broad category of app and should appeal to most users on some level.
- Weather apps are more easily substituted than other types of apps. For example, though Facebook and Google Plus are both social networking apps, they cannot be substituted for each other. The benefits afforded by Facebook (connecting to a specific set of people) are not the same benefits afforded by Google Plus. Despite the user's preference for a particular brand of weather app, the benefits afforded by one weather app versus another are largely similar and data presented may have originated from the same source or otherwise be extremely similar.
- It is likely that users will understand the purpose of the weather app whereas users might not understand, or fully appreciate, the features of other apps such as Snapchat, GroupMe, or Google Now.
- Compared with other apps, it may be easier for users to consistently identify permissions that exceed function (excessive access).

- It is likely that users will have at least some familiarity with one or more of the weather apps selected for the study.
- A sample population will likely have a full range of perceived need for a weather app with some expressing a very high need for weather while others may express low need.

The population for this study is further narrowed by the type of mobile device. Because pre-Marshmallow Android permissions are both explicitly stated and accepted in an all-or-nothing manner (Felt et al. 2012), studying permission decisions is more straightforward on Android devices, though all mobile devices that contain and allow access to personal information are applicable. Apple's iPhone enables users to turn sensitive permissions on and off per app at any time (Jung et al. 2012). The Android Marshmallow release mimics Apple's approach to permission management. So while all mobile devices containing and allowing access to personal information are appropriate for this study, pre-Marshmallow Android devices offer the greatest clarity in the disclosure decision. This study only assesses users that have Android-based smartphones using an operating system prior to the Android Marshmallow release. The survey will NOT display on a desktop, laptop or non-Android device. Subjects must be using an Android-based device versions 2.x through and including version 5.x to access the survey. Forcing subjects to actually use their own Android-powered smartphones provides a real-world scenario with real risk and real disclosure. It also enables us to directly collect app installation information from their device using a custom app developed specifically for this research and discussed later in this chapter.

An additional benefit offered by Android devices is how permissions are communicated and accepted. The installation information is explicitly presented to the user. The permissions and capabilities of Android apps are both stated more prominently to the user (see Figure 3) than for iOS devices and are seemingly much more intrusive than Apple iOS apps. As stated earlier, because permissions often allow apps broad and deep access to sensitive information and features, and because those permissions are accepted as a whole, installing an app on any mobile device is tantamount to personal information disclosure. Specifically, disclosure in this case means that simply by installing NFL Mobile (see Figure 3), for example, a user has disclosed what apps are on his phone; how often he uses them; the events on his calendar; the contact information for every person on his phone; his precise location at all times location is available; whether he is on the phone and the number of the remote caller; the ability to read, copy, modify and delete all the photos and files in USB storage that are on his device; view the names of Wi-Fi connections available to him; and know his unique identifying information contained within the PMD. NFL Mobile also has the ability to send SMS messages at any time without the knowledge of the user but potentially incurring SMS fees to the user (Wijesekera et al. 2015).

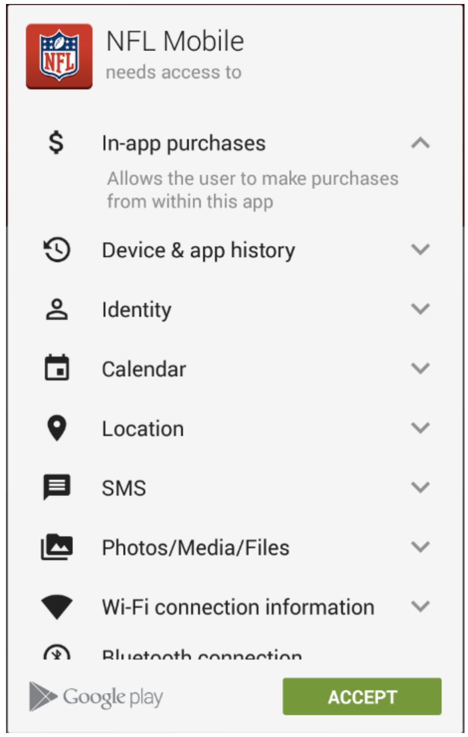


Figure 3 List of Permission Groups Requested by an Android App (NFL Mobile)

Study Design

This study is designed to test a personal mobile device privacy calculus model that explains and predicts *actual* disclosure of personal information contained within a PMD. The mobile device category is broad and not every mobile device available today, or in the future, fits the context of this study. Only devices that contain sensitive personal information, and potentially provide access to said information are within the scope of this study. The number of PMDs meeting this criteria are increasing at great speed. Sensitive information includes geographic location (precise and imprecise), contacts, electronic communication (including Bluetooth, near-field communication, text, video, email, instant messages, etc.), and access to body and environmental sensors (camera, health monitors, microphone, accelerometer, motion, etc.). Smartphones are the central focus of this study, however, other mobile devices such as tablets, smartwatches and other wearables, to the extent they provide access to the aforementioned sensitive information, also fit this context.

Figure 4 presents an overview of the study. Prior to the app evaluation portion of the study, subjects are directed to run a utility that provides a list of apps already installed on their device. This list represents actual prior personal information disclosure decisions.

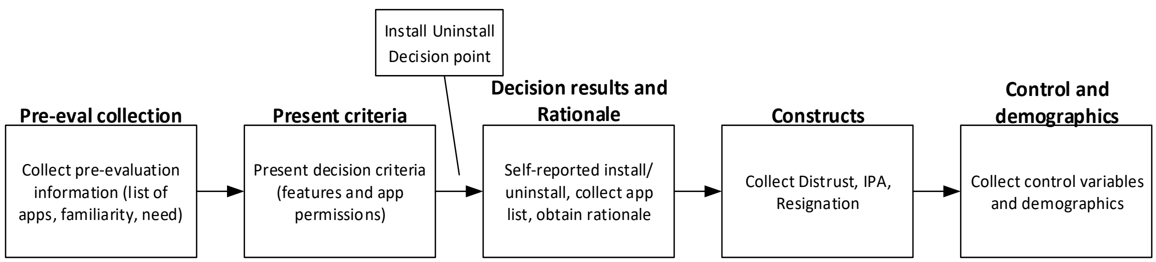


Figure 4 Study Overview

Users also self-report which of the weather apps they have already installed and which weather app (within the study or not) is their primary weather app. The familiarity with the apps is captured, and subjects complete an assessment of need for weather-related apps. General feature information about the apps is presented to the user being careful to not bias the user towards heightened privacy awareness. An installation/uninstallation decision is presented and post-evaluation information is collected. Post-evaluation information includes self-reported actual installation, or uninstallation, along with the list of apps and permissions collected by the aforementioned BTS App Listing Utility. Finally, the user's rationale for installing, uninstalling or not installing an app is collected along with the subject's demographic information.

Instrument Design

Subjects will be recruited from Mississippi State University and online panels. Again, to avoid biasing subjects and heightening their privacy and risk awareness, the study is framed as a general review of several weather apps, rather than a specific study on security or privacy. A more detailed graphic depicting the survey process is presented in Figure 5. The survey instrument is provided in APPENDIX A.

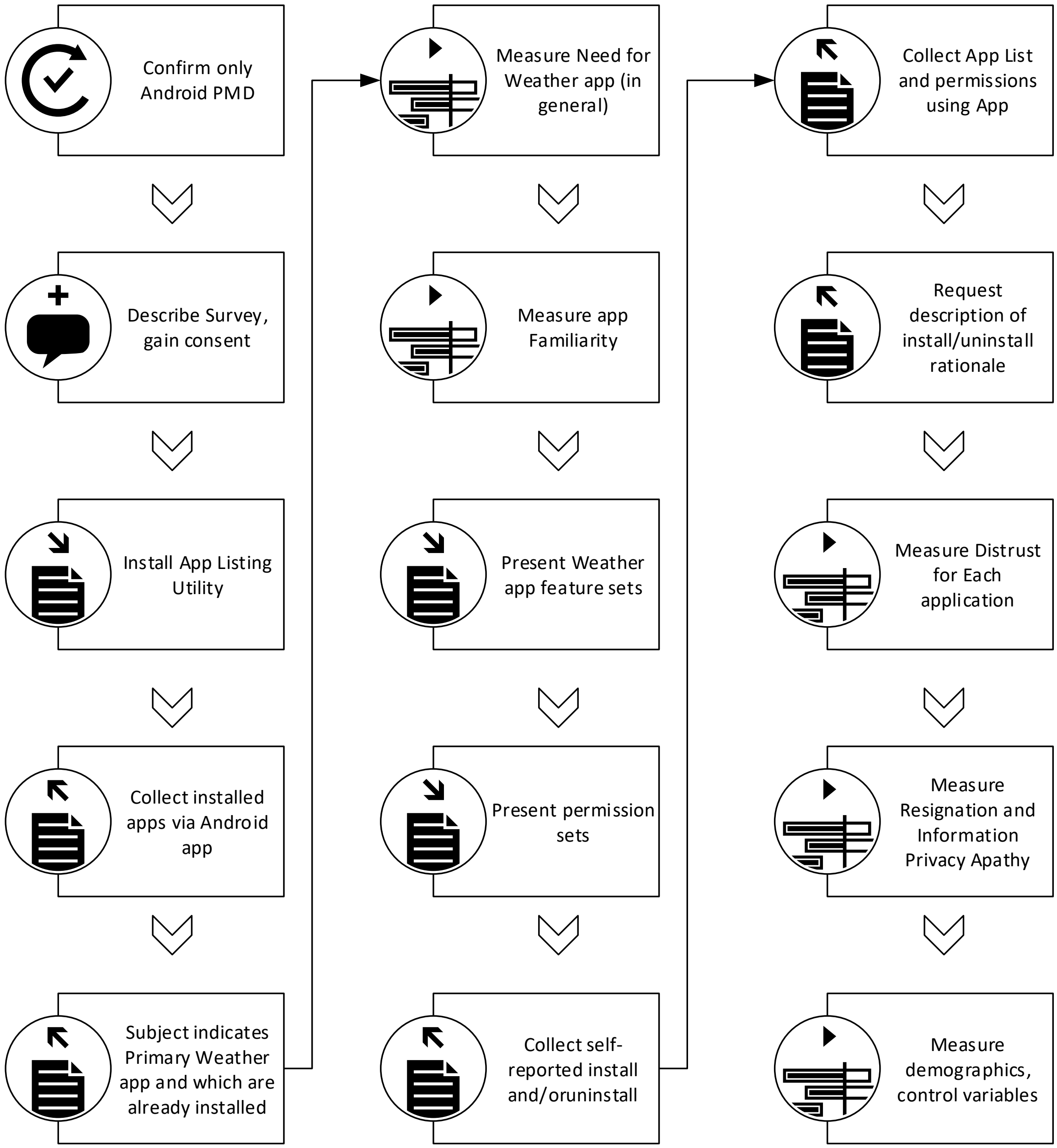


Figure 5 Process Flow

Pre-Evaluation Collection

What follows is a more detailed explanation of the study design as depicted in Figures 4 and 5.

Because I am asking subjects to actually install or uninstall an app, and because I collect the actual apps installed on the user's device, the survey must be completed using an Android-powered PMD. Consequently, the survey instrument automatically filters out any non-Android participants. If a subject attempts to access the survey with a desktop or laptop browser or via an iPhone, they will be directed away from the survey and informed that the survey must be completed using an Android-powered PMD. Subjects are then asked about their proficiency level for configuring a smartphone, and I explain why the BTS App Listing Utility is privacy-safe so as not to bias the sample of users based on installing an obscure app the collects information.

The purpose of the utility is to automate the process of listing apps and their corresponding permissions. One may object that installing an app designed to collect information may bias the sample of individuals willing to participate in this study. The rationale is that a user who is willing to disclose information is already predisposed to disclosure. I avoid disclosure-bias by communicating the safety of the BTS App Listing Utility in the recruitment materials, consent language, and on the app user interface.

Almost every app installed on a PMD requests several, if not dozens of permissions to access personal information (see Figure 3). Personal information on an Android device is only accessible if the user grants permissions to the app (Zhu et al. 2014). The app developed for this study does not request any permissions. At the point of installation, the user is notified that the BTS App Listing Utility requires no special permission to run. Consequently, the app has no access to any personal information, nor any information that would uniquely identify the user. This fact is clearly communicated to all potential participants. A rational participant should understand that this app is among the safest apps they have ever downloaded. Consequently, use of this app by the subject does not bias the sample. The app and brief instructions on how to use it are displayed in the user interface of the utility (see Figure 6).

The subject is then directed to download the utility and use it to copy and paste the list of apps and permissions into the survey. The BTS App Listing Utility interface is presented in Figure 6).

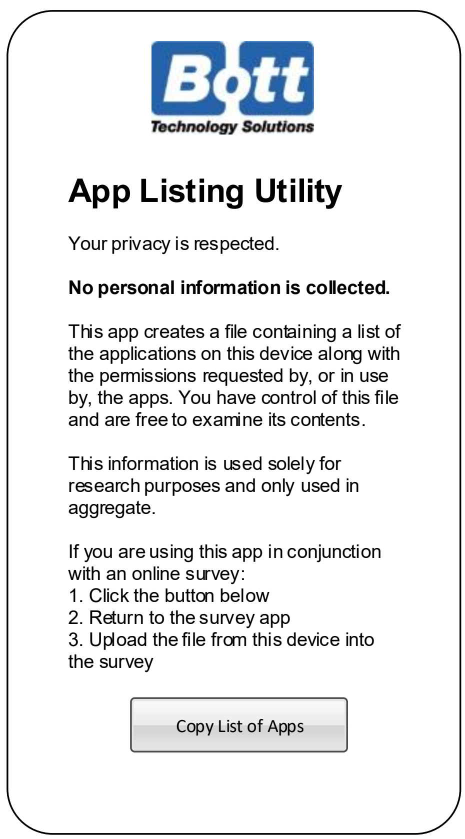


Figure 6 BTS App Listing Utility User Interface

After the user taps the “Copy List of Apps” button, the BTS App Listing Utility captures the list of apps present on the PMD along with their corresponding permissions. Participants are then directed to paste that information directly into the survey. This process provides a precise list of apps, the version of the apps, and their corresponding permissions. These lists are actual disclosure. The user is able to inspect the information to be shared and remains in full control of it, bolstering our claim to avoid disclosure bias.

Data are provided in JavaScript Object Notation (JSON) format for easy transfer into Microsoft SQL Server. A single app record is highlighted (see Figure 7), and one of the permissions is also highlighted. This record is for the Facebook app and its corresponding permissions (Access Coarse Location is highlighted). Each permission has a name, a protection level, and a status. Only Android 6.x and later users may grant or block individual permissions (as depicted in this case).


```
{"appName":"Facebook","packageName":"com.facebook.katana","versionName":"73.0.0.18.66"
,"permissions":[{"permissionName":"android.permission.READ_CONTACTS","status":"BLOCKED
","protectionLevel":"Dangerous"},{"permissionName":"android.permission.WRITE_CONTACTS"
,"status":"BLOCKED","protectionLevel":"Dangerous"},{"permissionName":"android.permissi
on.BLUETOOTH","status":"GRANTED","protectionLevel":"Normal"},{"permissionName":"androi
d.permission.BLUETOOTH_ADMIN","status":"GRANTED","protectionLevel":"Normal"},{"permiss
ionName":"android.permission.RECEIVE_BOOT_COMPLETED","status":"GRANTED","protectionLev
el":"Normal"},{"permissionName":"android.permission.ACCESS_COARSE_LOCATION","status":"
BLOCKED","protectionLevel":"Dangerous"},{"permissionName":"android.permission.WAKE_LOC
K","status":"GRANTED","protectionLevel":"Normal"},{"permissionName":"android.permissio
n.VIBRATE","status":"GRANTED","protectionLevel":"Normal"},{"permissionName":"android.p
ermission.GET_ACCOUNTS","status":"BLOCKED","protectionLevel":"Dangerous"},{"permission
Name":"android.permission.MANAGE_ACCOUNTS","status":"GRANTED","protectionLevel":"Norma
l"},{"permissionName":"android.permission.AUTHENTICATE_ACCOUNTS","status":"GRANTED","p
rotectionLevel":"Normal"},{"permissionName":"android.permission.READ_SYNC_SETTINGS","s
tatus":"GRANTED","protectionLevel":"Normal"},{"permissionName":"android.permission.WRI
TE_SYNC_SETTINGS","status":"GRANTED","protectionLevel":"Normal"},{"permissionName":"an
droid.permission.ACCESS_FINE_LOCATION","status":"BLOCKED","protectionLevel":"Dangerous
"},{"permissionName":"android.permission.BROADCAST_STICKY","status":"GRANTED","protect
ionLevel":"Normal"},{"permissionName":"com.facebook.katana.provider.ACCESS","status":"
GRANTED","protectionLevel":"Signature"}]}
```


Figure 7 Facebook App List Record and Corresponding Permissions

Note the app (Facebook) is highlighted along with one of the “Dangerous” permissions, ACCESS_COARSE_LOCATION. This permission is BLOCKED by an Android 6.x user

To prevent bias towards a particular weather app, the user is asked to provide the name of their primary weather app prior to revealing the weather apps used in this study. The user then indicates which, if any, apps are already installed on the PMD, and then provides a personal assessment of need for weather apps. Included in the need assessment are general review questions to maintain the appearance of a weather app review (e.g., "My weather app is easy to use" and "My weather app has all the features I need"). Then the subject indicates how familiar he is with each of the weather apps in the study.

Present App Decision Criteria

After indicating familiarity, subjects are presented with a condensed list of salient features for each of the weather apps followed by a chart depicting a subset of the permissions requested by each app (see Figure 8).

Android Permission	Accuweather	Local Weather (by matto)	The Weather Channel	Weather (Macro Pinch)	Weather Underground	Yahoo
Device & App History - retrieve running apps	No	No	No	No	No	Yes
Identity - find accounts	Yes	No	Yes	No	No	Yes
Identity - add/remove accounts	No	No	No	No	No	Yes
Contacts - find accounts	Yes	No	Yes	No	No	Yes
Location - approximate	Yes	No	Yes	No	Yes	Yes
Location - precise	Yes	No	Yes	Yes	Yes	Yes
Phone - read status and identity	Yes	No	Yes	No	No	No
Photos/Media/Files - modify	Yes	No	Yes	No	Yes	Yes
Photos/Media/Files - read	Yes	No	Yes	No	Yes	Yes
Storage - read	Yes	No	Yes	No	Yes	Yes
Storage - modify/delete	Yes	No	Yes	No	Yes	Yes
Wi-Fi connection information	No	No	Yes	No	No	Yes
Device ID and Call Info - read phone status	Yes	No	No	No	No	No
Other - use accounts on the device	No	No	Yes	No	No	Yes
Total Permissions Requested	**16**	**2**	**18**	**5**	**12**	**22**

Figure 8 Permission Chart

The graphic above is presented to the user within the survey and lists sensitive permissions and which apps request which permissions and the total permissions requested by each app. Not all permissions requested are displayed. Consequently, the number of Yes indicators will not match the Total Permissions Requested.

After reviewing feature sets and required permissions, the user is strongly encouraged, but not required, to install the actual app from the Google Play store. From within the Google Play store, if the subject desires, he or she can view additional information about the app such as user ratings, user feedback, and screenshots of the user interface.

Decision Results and Rationale

After reviewing the six apps, as mentioned above, users are strongly encouraged to act upon what they have encountered by installing or uninstalling one or more of the apps. For all apps, users indicate whether they installed, uninstalled, kept, or ignored the app. The outcomes of keep or install apply to users that already have the respective app installed on their smartphone. Although the uninstallation of one app in favor of a more suitable or desirable app may imply discontinuance (Bhattacherjee 2001), in this specific situation, I argue that the user is merely substituting one app for another. In the specific instance of obtaining weather information, the user is continuing the same behavior using a different vehicle. Weather apps reporting on the same location report identical data (high temp/low temp, precipitation, etc.). In many cases, the ultimate source of weather data may actually be the same across different apps (e.g., NOAA).

This is a unique situation and does not apply to all apps. Compare the situation of a user uninstalling a social network app such as Facebook and replacing it with Google Plus. In this case, switching is discontinuance because the benefits afforded by one are not similar to the other. The benefits and purposes realized using Facebook are not continued using Google Plus. Only in rare cases, if any, would the community of peers, acquaintances, content, and sharing frequency be the same across more than one SNS provider.

Collect Distrust, IPA, and Resignation

To prevent bias and foreshadowing, subjects' level of resignation and information privacy apathy (IPA) is assessed only after they have completed reviewing the mobile apps. Specific measurement items for Distrust, IPA, and Resignation are discussed in the next section.

Collect Control Variables and Demographic Information

The final phase of the survey instrument involves collecting demographic information such as gender, ethnicity, year of birth, educational level, the number of apps installed on their phone, as well as the number of years of post-education full-time employment and prior privacy invasion experience. Again, to avoid biasing the subject, privacy awareness questions are asked during this phase rather than prior to making an installation (disclosure) decision.

Measurement

The unit of analysis in this study is the individual PMD user. The constructs composing the personal mobile device privacy calculus are latent constructs. Because they are latent constructs, the factors comprising an individual's decision to disclose or not disclose personal information on a PMD are not directly observable. I plan to conduct a two-phase process to assess content validity, construct validity, and reliability via a pilot test before primary data collection. Following guidance from Churchill (1979) and Mackenzie et al. (2011), scales were developed or adapted using feedback from expert panel reviews and will be further refined after obtaining data from the pilot study. What follows is a list of the constructs (see Table 1), the items, and description of the method of measurement, origin, and modification to the items, if any.

Table 1 Construct Definitions

Construct	Adapted Definition	Definition Sources
Excessive Access	Permissions requested by an app beyond what is necessary for app functionality.	(Sarma et al. 2012)
Distrust	A PMD user's confident expectation of opportunistic data collection and use.	(Komiak and Benbasat 2008; Lewicki et al. 1998)
Familiarity	A PMD user's recognizability based on prior experience with the app itself.	(Luhmann 1979)
Perceived Need	The requirement of an app because it is essential or very important to the PMD user.	(Mishra and Lalumière 2010)
Resignation	A PMD user is in a state of resignation an undesirable outcome is deemed inevitable and nothing will affect or change it.	(Maier and Seligman 1976; Turow et al. 2015)
Information Privacy Apathy	A state of indifference towards the disclosure of personal information.	(Acquisti et al. 2015; Yoo et al. 2012)

Disclosure

The dependent variable for this research is disclosure. Disclosure in the context of this study is the installation of an app. As discussed earlier in this paper, prior to the Marshmallow release, app installation required an all-or-nothing acceptance of the permissions requested by the particular app (Elenkov 2014). For example, if the Facebook app requests 61 permissions, the user must either grant all 61 permissions or choose not to install Facebook on their PMD. Starting with Marshmallow, permissions are more selective. This selective model is similar to the Apple iOS model where users may turn permissions on all the time, when in use, or never.

The all-or-nothing approach to permissions, though sub-optimal for the user, offers a clean and efficient method to measure actual disclosure. It provides insight into the decision process employed by PMD users when choosing to disclose information. Prior research clearly indicates measuring *intent* in the context of information privacy is less than reliable (Keith et al. 2013). Many studies point to an inconsistency between users intent to protect privacy and actual actions taken regarding privacy protection (Alashoor and Baskerville 2015; Barnes 2006; Bélanger and Crossler 2011; Norberg et al. 2007; Smith et al. 2011; Wittes and Liu 2015). This has been discussed previously in this paper as the privacy paradox. Because of this potential inconsistency, and for greater accuracy and relevancy, this research measures actual disclosure by cataloging the actual apps installed and the permissions granted to each app. Note that different versions of the same app may request different sets of permissions. For example, MyWeatherApp 1.0 may initially only request a few permissions within the various permission groups (e.g., location, storage, identity, etc.). Subsequent versions may obtain additional permissions within groups without notification. Consequently, cataloging apps using the BTS App Listing Utility is useful to capture accurate permission levels.

According to Yahoo, users have an average of 95 apps installed on their phone (Sawers 2015). Each app has between zero and potentially more than 50 individual permissions (Elenkov 2014). It is not feasible to manually collect this information from the user. Survey fatigue, lack of skill, and budgetary constraints require automated collection of downloaded apps and permissions. In the current versions of the Android operating system, users have little or no control over the factory installed apps and system apps present on their PMD. Consequently, these apps are excluded from this study. Only apps that have been downloaded by the user are considered for analysis.

Actual disclosure is the dependent variable and it is measured as continuous variable. Four states capture subjects' disclosure decisions. Prior to the study, subjects either already have a particular app installed, or do not have it installed. After I present the apps in this study, subjects either want the app, or they do not want the app. This results in four options for the subject (Uninstall, Ignore, Keep, Install). Each of the options is a progressively greater act of non-disclosure or disclosure. At each end of the four node continuum, users take an action to disclose. They either actively uninstall or actively install an app on their PMD. The middle two actions are passive. They either ignore an app (passive non-disclosure) or keep an app that they previously installed (passive disclosure). The combination of these four options forms a continuous variable.

Recall that subjects that the choice to install or keep an app is a choice to disclose some level of personal information. Subjects that uninstall or ignore are choosing to not disclose personal information. Decisions are measured per app, and each app has a different disclosure level corresponding to the number of overall permissions and sensitive permissions requested. The six apps are divided into High permissions and Low permission groups. In order of the number of requested permissions, the Low permission group contains Local Weather by Matto (no sensitive permissions requested), Weather (MacroPinch), and Weather Underground. The High permission group contains the three most popular, and most privacy invasive apps: The Weather Channel, Yahoo Weather, and AccuWeather (see Table 2 for a listing of the apps and the number of sensitive permissions they request in excess of what is required for app functionality).

Table 2 Weather Used Apps in this Study

Icon	Group	Name	Permissions	Sensitive Permissions
AccuWeather Accuweather.com	High	AccuWeather	16	4
The Weather Chann The Weather Channel		The Weather Channel	18	5
Yahoo Weather Yahoo		Yahoo Weather	22	4
Weather Undergrou Weather Underground	Low	Weather Underground	12	0
Weather MacroPinch		Weather (MacroPinch)	5	0
Local weather matto		Local Weather (by Matto)	2	0

Excessive Access

Apps running on a mobile device sometimes legitimately require permissions to information stored on the device and capabilities of the device to perform their intended function. For example, a map app requires access to GPS capabilities of the device so that it can provide the user's current location. Apps with a single function or limited capabilities require few or no permissions to operate. For example, a "flashlight" app simply illuminates the LED light on the device and requires no permissions to function. In the latter case, if a flashlight app requires GPS capabilities, that permission request is excessive. Similarly, weather apps require permissions to function: location (to automatically display the local forecast), full network access, receive data from the Internet, read permission to storage (to upload photos). However, most weather apps do not need access to data storage, ability to delete accounts, retrieve a list of apps running, retrieve contacts on the device, or access browsing history. The presence of these permissions, which are presented to the user (see Figure 8) constitutes Excessive Access.

After the subject makes a decision to install, uninstall, or not to install the set of apps, I ask the subject a series of questions to determine the reasons and rationale for those decisions (see Table 3).

Table 3 App Installation Rationale Item

Item ID	**Item**	**Original Item**	**Reference**
Rea1	Please indicate the reasons for not installing or uninstalling this app: • Incomplete or lacking feature set • I have no use for it. • I am uncomfortable with the app permissions requested • Redundant with app(s) already installed.	Developed for this study	

Distrust

After each app installation decision, distrust will be measured using the items in Table 4.

Table 4 Distrust Items

Item ID	Item	Original Item	Reference
DIS1	This app developer will exploit customers' personal information given the chance.	This e-vendor will exploit customers' vulnerability given the chance.	(Cho 2006)
DIS2	This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest.	This e-vendor will engage in damaging and harmful behavior to customers to pursue its own interest.	
DIS3	This app developer creates apps that collect information in a deceptive manner.	This e-vendor perform its business with customers in a deceptive and fraudulent way.	

Familiarity

Individuals making a disclosure decision regarding a specific app do so with varying levels of familiarity with the app itself, its developer, the brand name associated with the app or some combination of the three. Familiarity is characterized by users having prior experience with the app, the brand, or vicarious experience with the app through others. Familiarity, of course, can be either positive or negative. Individual were asked to give an assessment of their overall weather app experience.

Perceived Need

As discussed in Chapter 2, when humans (and animals) are presented with a high-risk or low-risk outcome, risk-sensitivity theory predicts that they will shift from risk-aversion to risk-proneness in high need situations (Mishra and Lalumière 2010). Similar to the Personal Internet Interest construct posited in the extended privacy calculus model (Dinev and Hart 2006), Perceived Need may override Distrust resulting in personal information disclosure. The items in Table 5 were measured using a fully anchored 5 point Likert scale (strongly agree to strongly disagree).

Table 5 Perceived Need Items

Item ID	Item	Original Item	Reference
Need1	If I were to buy a new phone, my weather app would be among the very first apps I would reinstall.	Original items were developed for this study.	
Need2	I use my weather app every day		
Need3	My weather app is extremely important to me		
Need4	It is extremely important to me that I receive severe weather alerts from my weather app		
Need5	Knowing the weather forecast is very important to me		
Need6	My weather app is located in the best location for access (e.g., on the bottom row that appears on every screen)		

Resignation

Much extant research assumes individuals make a trade-off or perform a rational cost-benefit assessment between the benefits of obtaining something (in this case an app) and the risks of providing personal information (Culnan and Armstrong 1999; Dinev et al. 2006; Dinev and Hart 2006; Kehr et al. 2015; Li et al. 2010; Xu et al. 2009). A recent study challenges the assumption that subjects perceive that they truly have a choice in the decision-making process (Turow et al. 2015). The study indicates that 57% of individuals, when presented with a trade-off of giving up their personal information in exchange for supermarket discounts, gave up their personal information because they were resigned to the inevitability of surveillance, and the power that third parties already possess to harvest their data. Even when presented with a broader understanding of the trade-off and how it might benefit the individuals, only 32% supported the deal (Turow et al. 2015). The items for resignation are presented in Table 6.

Table 6 Resignation Items

<table>
<tr><th>Item ID</th><th>Item</th><th>Original Item</th><th>Reference</th></tr>
<tr><td>RES1</td><td>No matter how much effort I put into protecting my mobile privacy, I feel I have no control over the outcome.</td><td>No matter how hard I try, things never seem to work out the way I want them to.</td><td rowspan="3">(Quinless and Nelson 1988)</td></tr>
<tr><td>RES2</td><td>Other organizations have more control over my personal information than I do.</td><td>Other people have more control over their success and/or failure than I do.</td></tr>
<tr><td>RES3</td><td>I feel that I have little control over the outcomes of protecting my personal information.</td><td>I feel that I have little control over the outcomes of my work.</td></tr>
<tr><td>RES4</td><td>Many organizations already have more information about me than I want them to have.</td><td colspan="2" rowspan="2">Developed for this study.</td></tr>
<tr><td>RES5</td><td>It is wasted effort to protect my privacy.</td></tr>
</table>

Information Privacy Apathy

Apathy is characterized by a lack of interest, enthusiasm or concern (Charlton and Birkett 1995; Csikszentmihalyi 1975; Stuss et al. 2000). In the context of the study, Information Privacy Apathy (IPA) is a lack of interest or indifference towards the collection of personal information on a mobile device. Indicators of information privacy apathy include little interest, less care, and less worry. Another indicator that privacy is of little concern is bypassing explicit permission notification provided during the installation of an app on an Android device. One possible challenge for this study is that the clear majority (83%) of users do not pay attention to the permissions screens at install time (Kelley et al. 2013). The items are listed in Table 7 and were measured using a fully-anchored 5-point Likert scale.

Table 7 Information Privacy Apathy Items

Item ID	Item	Original Item	Reference
IPA1	I have little interest in privacy issues when installing an app from the Google Play store.	I have little interest in information privacy issues as when I purchase through Facebook.	(Sharma and Crossler 2014; Yoo et al. 2012)
IPA2	I care less about information privacy while downloading an app from the Google Play store.	I care less about information privacy anymore while purchasing through Facebook.	(Sharma and Crossler 2014)
IPA3	I do not worry about privacy issues while downloading an app on the Google Play store.	I do not worry about privacy issues anymore while purchasing through Facebook.	(Sharma and Crossler 2014)
IPA4	When I download an app from the Google Play store, I pay almost no attention to the permissions information.	Developed in this study	

Control Variables and Demographic Information

Because this study involves individual-level perceptions, demographic information will also be collected. Specifically, gender, ethnicity, year of birth, educational level, the number of apps installed on their phone (which may be compared to the actual number of apps) as well as the number of years of post-education full-time employment and prior privacy invasion experience.

Privacy Awareness

Privacy Awareness is included in the present study as a control variable. Because privacy awareness is based on an individual's experience, perception, and cognition of mobile devices and permissions, each individual's privacy level is likely to be unique. An individual's privacy awareness is comprised of:

- an understanding and perception of whether or not entities (e.g., first-party developers or third-party companies) are receiving, or have received personal information from the mobile device, and
- the content of the personal information others receive or have received in detail,
- how information collected from a mobile device is being used or may be used in the future as well as,
- what amount of information collected from the mobile device might reach and/or interrupt individual. (Pötzsch 2009)

A mobile user who understands permissions would likely perceive himself as someone of whom friends would ask advice concerning the impact or meaning of permissions. Within the survey, I assess each individual's level of privacy awareness using the items in Table 8.

Table 8   Privacy Awareness Items

Item ID	Item	Original Item	Reference
PA1	I can list the companies and entities that have access to my personal information on my mobile device.	Developed for this study based on criteria from (Pötzsch 2009)	(Pötzsch 2009)
PA2	I know what personal information others have received from my mobile device.		
PA3	I have a good idea how personal information from my mobile device is being used now and in the future.		
PA4	I have a good idea of how much personal information from my mobile device has been collected or transmitted to others.		
PA5	I have often decided NOT to install an app because of the permissions required.	Have you ever not installed an app because of permissions?	(Felt et al. 2012)
PA5	My peers would turn to me if they had questions regarding app permissions.	Developed for this study.	

Construct Validity

Construct validity assesses how well a given measurement scale measures the theoretical construct it purports to measure. Convergent and discriminant validity are two methods to assess the extent to which a measure adequately and reliably represents the underlying phenomenon (construct) it is supposed to measure Reliability is a measure of consistency across different observations of the same construct. Convergent validity refers to the degree which measures that should be related are indeed related (Fornell and Larcker 1981). Discriminant validity examines whether measures that are not supposed to be related are indeed unrelated (Campbell and Fiske 1959). A common statistical method for demonstrating convergent and discriminant validity is exploratory factor analysis (EFA)

Exploratory and Confirmatory Factor Analysis

This study will perform an exploratory factor analysis using principal components analysis with a Varimax rotation using IBM SPSS 23. EFA is a statistical technique for both identifying and reducing the number of factors in a given set of items by identifying underlying relationships between the measured variables. Factors are allowed to correlate freely with no constraints (DeVellis 2012). EFA is useful for discovering relationships between items based on expectations derived from theory and for identifying and correcting measurement issues prior to performing confirmatory factor analysis (CFA). Varimax rotation is used to simplify the columns of the factor matrix without modifying the coordinate system. Instead, the axes are rotated orthogonally to align optimally with the coordinates. Following the EFA, a confirmatory factor analysis will be performed.

Confirmatory Factor Analysis (CFA) will be performed using IBM SPSS AMOS 23. Like EFA, CFA is a statistical technique used to verify the factor structure of a set of observed variables. Unlike an EFA, the researcher specifies a priori hypothesized relationships based on prior literature. Instead of allowing all items to correlate freely, CFA constrains how measurement items relate to latent constructs based on the measurement model (Bollen and Lennox 1991). The objective of this process is to confirm what was initially observed in the EFA and ultimately provide strong evidence for internal and external validity. The measurement model will be examined for goodness of fit, average variance extracted, standardized item loadings, and latent construct correlations.

Common Method Bias

Common method bias (CMB) is the inflation (or in rare cases, deflation) of the true correlations among observed variables created by taking measurements using a common method. It can be a significant source of measurement error, potentially leads to Type I and Type II errors and is a primary threat to construct validity (Campbell and Fiske 1959; Straub et al. 2004). It is systematic error variance attributable to the measurement method rather than attributable to the construct (Podsakoff et al. 2003). The present study uses a common method to measure observed variables. Consequently, common method bias must be mitigated and addressed.

CMB can be addressed proactively using procedural remedies and posthoc using statistical remedies. Procedurally, ensuring items in this study have been carefully constructed and are clear, concise, and succinct mitigates ambiguity and misinterpretation (Mackenzie et al. 2011). The present study utilized an expert panel as described by (Petter et al. 2007) to ensure proper understanding and communication of the domain concepts and rectify item context errors thereby improving the scale items. Expert panels were composed of university faculty, graduate students, and undergraduate students. Instrument items were reviewed for clarity of message, realism, content validity, and face validity. Several changes were suggested and implemented to increase clarity and avoid redundancy. Based on future pilot test data results, expert panels may be reconvened to clarify or modify items to streamline the process and further reduce common method effects if any are indicated. To mitigate social desirability bias, leniency bias, and acquiescence, assurance of subjects' anonymity will be clearly communicated.

To assess CMB posthoc, AMOS 23 will be used to perform an unmeasured latent common method factor analysis (Podsakoff et al. 2003). An unmeasured latent variable is added to the model and related to each of the constructs' indicators. The relationship (regression weights) are constrained to a singular value and the variance set to 1. After running the model, chi-square values are compared. If a significant result is obtained, this indicates CMB is present, and the unmeasured common latent factor must be included in results.

Data Analysis Techniques

To test the relationship among constructs, structural equation modeling using IBM AMOS 23 will be used. First, the measurement model will be examined and then the structural model per (Anderson and Gerbing 1988). Structural equation modeling (SEM) is a second generation statistical modeling technique that is well-suited for testing theory. SEM analyzes the influence predictor variables have on numerous dependent variables simultaneously and accounts for measurement error (Steenkamp and Baumgartner 2000). SEM also makes it possible to identify errors in measurement to separate those errors from the data. Furthermore, it enables researchers to "answer a set of interrelated research questions in a single, systematic, comprehensive analysis" (Gefen et al. 2000).

The decision process results in a disclosure decision for each app in the study. Three constructs (familiarity, distrust, and excessive access) are measured specifically for each app, while others are only measured once. To accurately reflect the influence of the three app-specific constructs, analysis will be performed once per app (six times). The highest disclosing apps (AccuWeather, The Weather Channel, and Yahoo) have nearly identical disclosure levels and I intend to analyze them as a group. To ensure validity prior to grouping, an invariance test will be run to confirm factor loadings do not differ across groups and ensure items are measuring the same phenomenon across apps. I will assess both configural and metric invariance. Configural invariance is established when the unconstrained model has a good fit and metric invariance is established if the chi-square difference test statistic is not significant (Steenkamp and Baumgartner 1998).

The remaining constructs are single-measured items. Both IPA and Resignation are items that pertain to personal attributes and are not app-specific (Quinless and Nelson 1988; Yoo et al. 2012). The weather category of app was specifically chosen for its substitutionary attributes. As discussed earlier, weather data is often exactly the same possibly obtained from the same source. Consequently, need is measured per category (weather). Need, IPA, and resignation will be the same measure across apps for each subject. By measuring each app, influences of distrust, excessive access, and familiarity can be separated and attributed to the specific app.

Summary

In this chapter, I described the sample population, data collection techniques and the instrument development process related to this study. I also described the process flow for the study, the mitigation of common method bias, app of exploratory and confirmatory factor analysis as well as the data analysis techniques. Measurement scales will be tested in a pilot study to ensure construct validity before proceeding to the main investigation. Results from the pilot study will be used to adjust the scales as needed prior to using them in the main investigation to assess the hypotheses provided in Chapter 2.

CHAPTER IV

DATA ANALYSIS AND RESULTS

Introduction

In this chapter, I present the results of the pilot study and main study. First, I present the results of the pilot study including demographic information, reliability measures as well as an assessment of convergent and discriminant validity. Then, the results of the main study are presented. Demographic statistics, reliability measures, and evidence supporting convergent and discriminant validity as well as model fit are reported. Then common method bias is assessed and control variables are measured against the model. With the significant control measures present in the model, the structural model is then analyzed including mediating and moderating relationships. Finally, the previously described High and Low app permission groups are analyzed for significant differences and the results are presented.

Pilot Study

A pilot study was completed using Amazon Mechanical Turk (MTurk) to assess the performance of the measurement items used to measure the phenomenon. A sample of 65 panelists from MTurk participated in the study, but 7 cases were removed because of incomplete responses leaving a total sample size of 58. To be qualified to respond to the survey, subjects were required to meet the following criteria at the time of the survey: reside in the United States, complete the survey using only an Android-powered device, be over the age of 18, and have information they consider personal on their device. The sample was 59% male and 41% female, with an average age of 30.6. Fifty-five percent of respondents indicated their ethnicity was white, 20.7% Asian, 13.8% Black/African American, and 8.6% Hispanic, Latino, or Spanish origin. Fifty percent of respondents had a Bachelor’s degree or higher whereas 33.5% had attended college without completing a degree. Users were asked to rate their understanding of how to configure their smartphone and 94.8% were at least moderately knowledgeable. Each participant was paid 85 cents for completing the survey. See Table 9 for a more complete list of demographic information.

Table 9 Demographic Frequency and Percentages (N = 58) for Pilot Study

Variable	Measure	Frequency	Percentage
Gender: What is your gender?	Male	34	58.6
	Female	24	41.4
Age	19-29	32	55.2
	30-39	19	32.8
	40 and over	7	12.1
Ethnicity: What is your race or origin?	White	32	55.2
	Asian	12	20.7
	Black/African American	8	13.8
	Hispanic, Latino or Spanish origin	5	8.6
	American Indian or Alaskan Native	1	1.7
Education	High school graduate (or equivalent)	9	15.5
	Some college, but less than 1 year	7	12.1
	One or more years of college, but not Bachelor's degree	13	22.4
	Bachelor's degree	21	36.2
	Master's degree (or other post-graduate professional degree)	7	12.1
	Doctoral degree	1	1.7
Level of knowledge about configuring smartphone	Extremely knowledgeable	19	32.8
	Very knowledgeable	18	31.0
	Moderately knowledgeable	18	31.0
	Slightly knowledgeable	3	5.2
	Not knowledgeable at all	0	0
Work experience: How many years of post-education, full-time employment do you have?	Zero	4	6.9
	Less than 1 year	4	6.9
	1 to 5 years	19	32.8
	5 to 10 years	19	32.8
	10 to 20 years	7	12.1
	More than 20years	5	8.6

Exploratory Factor Analysis

To assess the relationship between the items and their respective constructs, a recommended two-step exploratory and confirmatory analysis was performed (Anderson and Gerbing 1988). During an exploratory factor analysis (EFA), no measurement model is specified a priori, and items are allowed to freely correlate with each other thereby identifying the underlying structure or providing indications of problematic items. Items that load on more than one factor simultaneously are cross-loading. Cross-loading factors with loadings greater than 0.4 and items with single-factor loadings less than 0.6 are problematic (Hair et al. 2010) and should be corrected prior to performing a confirmatory factor analysis (CFA).

Results of the EFA are presented in Table 10. A total of five items show indications of problems based on the results of the EFA. Three items intended to measure perceived need (PercNeed_6, PercNeed_7, and PercNeed_8) failed to load with the other five measurement items. All three items were dropped. To achieve better model fit, Resignation items 4 and 5, PercNeed_5 and Priv_Aware items 1 and 6 were also removed. Items with cross-loadings greater than 0.4 and were also dropped.

Table 10 Initial Rotated Factor Matrix Using Pilot Data

	Component				
Item	**1**	**2**	**3**	**5**	**6**
PercNeed_1	.788				
PercNeed_2	.833				
PercNeed_3	.847				
PercNeed_4	.895				
PercNeed_5	.759				
PercNeed_6					.895
PercNeed_7					.808
PercNeed_8					.393
Resignation_1		.821			
Resignation_2		.884			
Resignation_3		.888			
Resignation_4		.689			
Resignation_5		.567	.577		
IPA_1			.862		
IPA_2			.865		
IPA_3			.881		
IPA_4			.902		
DisWeather_1				.878	
DisWeather_2				.860	
DisWeather_3				.891	

Values suppressed below 0.4; PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

After removing problematic items, an EFA was again performed and exhibited no cross-loadings above 0.4 or extraneous factor loadings. See Table 11.

Table 11 Principal Components Analysis after Removing Problematic Items

	Factor			
Item	**1**	**2**	**3**	**4**
PercNeed_1	.796			
PercNeed_2	.883			
PercNeed_3	.868			
PercNeed_4	.908			
Resignation_1		.859		
Resignation_2		.891		
Resignation_3		.930		
IPA_1			.884	
IPA_2			.882	
IPA_3			.905	
IPA_4			.908	
DisWeather_1				.897
DisWeather_2				.877
DisWeather_3				.892

Values suppressed below 0.4; PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

Confirmatory Factor Analysis

The second step of the two-step process is to perform a confirmatory factor analysis (CFA). Items in the measurement model are no longer allowed to freely correlate. Instead, the a priori measurement model is specified constraining items to their respective constructs. In similar process to the EFA, problematic items are identified and either remedied or removed. Opportunities to achieve a better model fit are indicated by large values in the modification indices. However, modification indices were small (7 or below). Fit statistics indicate overall model fit is adequate and no items require alteration or removal. See Table 12 for measurement model fit statistics for pilot study data.

Table 12 Measurement Model Fit Statistics – Pilot Study

Goodness of Fit Statistic	**Recommended Value**	**Calculated Value**
χ^2	--	144.325
Degrees of Freedom (df)	--	125
χ^2 statistical significance (p-value)	--	.114
χ^2 index (χ^2 / df)	$\leq 3; \leq 5$	1.155
Incremental Fit Index (IFI)	$\geq .90$	.977
Tucker-Lewis Index (TLI)	$\geq .90$	.971
Comparative Fit Index (CFI)	$\geq .90$	.976
Root Mean Square Error of Approximation (RMSEA)	$\leq .06; \leq .08$	.052

Having indicators of good model fit, the next step is to assess convergent validity, discriminant validity, and reliability. All standardized loadings for items exceed the recommended 0.7 threshold and similarly composite reliability for all items are above the 0.7 recommended level. Additionally, all average variance extracted (AVE) values are greater than 0.5 providing adequate evidence that items are both valid and reliable. Results from the analysis are provided in Table 13.

Table 13	Standardized Loadings, Composite Reliability, and AVE for Multi-item, Latent Constructs

Construct	Item	Standardized Loading	Reliability	AVE
PercNeed	PercNeed_1	0.813 (ref)	.906	.708
	PercNeed_2	0.833 (7.279)		
	PercNeed_3	0.895 (8.034)		
	PercNeed_4	0.822 (6.846)		
Resignation	Resignation_1	0.810 (7.767)	.897	.744
	Resignation_2	0.833 (7.930)		
	Resignation_3	0.939 (ref)		
IPA	IPA_1	0.932 (10.928)	.934	.781
	IPA_2	0.850 (8.986)		
	IPA_3	0.857 (9.142)		
	IPA_4	0.893 (ref)		
Distrust	DisWeather_1	0.918 (11.804)	.935	.826
	DisWeather_2	0.891 (10.932)		
	DisWeather_3	0.918 (ref)		

PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

To demonstrate that the variance explained by our constructs is attributed mostly to the associated measurement items and not to those of other constructs, the intercorrelations of constructs values are examined. For all constructs, the square root of the average variance extracted (AVE) exceeds the other constructs, which offers further evidence of discriminant validity of the data collected in the pilot study. See Table 14 for descriptive statistics, square root of AVE values and intercorrelation of constructs.

Table 14 Descriptive Statistics and Intercorrelations of Constructs

	Mean	SD	PercNeed	Resignation	IPA	Distrust
PercNeed	3.60	1.74	(.841)			
Resignation	3.63	1.60	.208	(.862)		
IPA	4.63	1.75	.139	.150	(.884)	
Distrust	4.78	1.35	.008	.243	.447	(.909)

Square root AVE shown in (); PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

Main Study

Data for the main study were also collected via MTurk using the survey instrument described in Chapter 3 and provided in APPENDIX A. Respondents were restricted to those living in the United States, with human intelligence task (HIT) approval rates 95% or higher, and with more than 100 approved HITs. Respondents were paid for taking the survey. Survey data were first examined for unusable or incomplete data. Next, respondent characteristics were compiled, and then the data were assessed using exploratory and confirmatory factor analyses. Common method bias was assessed and measured control variables were added to the model and analyzed for significant impact. Then the structural model was analyzed, moderation and mediation examined, and finally, a two-group analysis was performed on the data based on a High-Low permission split of the weather apps as described in Chapter 3 (see Table 2).

Respondent Characteristics

A total of 741 respondents completed the survey, however, 51 responses were dropped for incomplete answers or obvious patterned answers resulting in a sample size of 690. The sample is 54.5% female with an approximate median age of 34.3 (only year of birth was collected for increased anonymity so age is approximate). Seventy-six percent were white and 75.8% have attended college for a year or longer with 51.6% having a bachelors, masters, or terminal degree. Work experience and self-assessed expertise level was also collected and presented. See Table 15 for the demographic information from the main study.

Table 15 Demographic Frequency and Percentages (N = 690) for Main Study

Variable	**Measure**	**Frequency**	**Percentage**
Gender: What is your gender?	Male	314	45.5
	Female	376	54.5
Age	18-29	266	38.6
	30-39	284	50.0
	40 and over	139	20.1
Ethnicity: What is your race or origin?	White	525	76.1
	Asian	40	5.8
	Black/African American	66	9.6
	Hispanic, Latino or Spanish origin	42	6.1
	American Indian or Alaskan Native	9	1.3
Education	Some high school	6	0.9
	High school graduate (or equivalent)	82	11.9
	Some college, but less than 1 year	79	11.4
	One or more years of college, but not Bachelor's degree	229	33.2
	Bachelor's degree	225	32.6
	Master's degree (or other post-graduate professional degree)	57	8.3
	Doctoral degree	12	1.7
Level of knowledge about configuring smartphone	Extremely knowledgeable	186	27.0
	Very knowledgeable	268	38.8
	Moderately knowledgeable	189	27.4
	Slightly knowledgeable	41	5.9
	Not knowledgeable at all	6	0.9
Work experience: How many years of post-education, full-time employment do you have?	Zero	36	5.2
	Less than 1 year	32	4.6
	1 to 5 years	178	25.8
	5 to 10 years	183	26.5
	10 to 20 years	164	23.8
	More than 20years	97	14.1

Exploratory Factor Analysis

IBM SPSS 23 was used for exploratory factor analysis (EFA) to assess initial reliability scores and construct validity. EFA results indicated improved loadings for measurement items retained for the main study. Principal components analysis with Varimax rotation was used to assess convergent and discriminate validity. All construct items exhibited an acceptable level of reliability with loadings above 0.70 (Nunnally and Bernstein 1994) and indicated convergent validity (Campbell and Fiske 1959; Peter 1981; Straub et al. 2004). No items cross-loaded with values greater than 0.40 on other items which indicates discriminant validity (Hair et al. 2010). See Table 16 for the results of the exploratory factor analysis.

Table 16 Exploratory Factor Analysis Using Principal Components Analysis

	Component			
Item	**1**	**2**	**3**	**4**
PercNeed_1	.846			
PercNeed_2	.871			
PercNeed_3	.921			
PercNeed_4	.793			
Resignation_1		.881		
Resignation_2		.875		
Resignation_3		.911		
IPA_1			.894	
IPA_2			.902	
IPA_3			.874	
IPA_4			.797	
DisWeather_1				.898
DisWeather_2				.897
DisWeather_3				.897

Values suppressed below 0.4; PercNeed = Perceived Need; IPA = Information Privacy Apathy; Priv_Aware = Privacy Awareness; DisWeather = Distrust in weather app (app-specific)

Confirmatory Factor Analysis

Again, in contrast to the EFA, within a confirmatory factor analysis (CFA) measurement items are not free to correlate among items, but are constrained to their respective constructs based on theory. IBM AMOS 23 was used to assess the measurement model to examine indicators of model fit, reliability, convergent validity, and discriminant validity.

Results from the CFA indicated good model fit from the measurement model (See Table 9). Naturally the χ^2 value (χ^2=300.35; df=125) increased due to the more than tenfold increase in sample size (N=58 to N=690) and the χ^2 index was within the recommended value. The remaining indexes examined support good model fit

(NFI=.960; IFI=.976; TLI=.971; CFI=.976; RMSEA=.045). See Table 17 for the statistics and Figure 9 for a diagram of the measurement model.

Table 17 Main Study Measurement Model Goodness of Fit Statistics

Goodness of Fit Statistic	Recommended Value	Calculated Value
χ^2	--	300.351
Degrees of Freedom (df)	--	125
χ^2 statistical significance (p-value)	--	.000
χ^2 index (χ^2 / df)	$\leq 3; \leq 5$	2.403
Normed Fit Index (NFI)	$\geq .90$	.960
Incremental Fit Index (IFI)	$\geq .90$	.976
Tucker-Lewis Index (TLI)	$\geq .90$	.971
Comparative Fit Index (CFI)	$\geq .90$	.976
Root Mean Square Error of Approximation (RMSEA)	$\leq .06; \leq .08$	.045

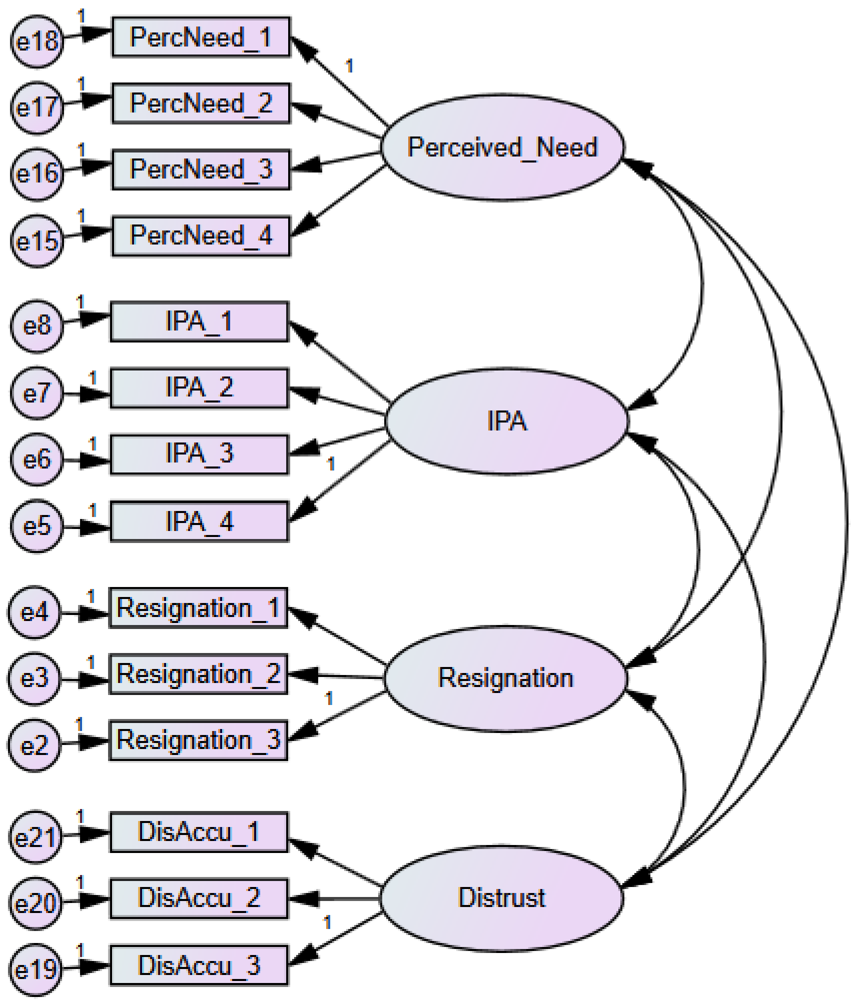


Figure 9 Measurement Model

The data collected for the main study also demonstrated reliability and both convergent and discriminant validity. Composite reliability for each construct is well above 0.70, the recommended threshold (Fornell and Larcker 1981) with the lowest value at 0.886 and all AVE's exceeding 0.5. Together these indicators provide adequate support for reliability and convergent validity of the measurement items and are provided in Table 18.

Table 18 Standardized Loadings, Composite Reliability, and AVE for Multi-item, Latent Constructs

Construct	Item	Standardized Loading (t-Values)	Reliability	AVE
PercNeed	PercNeed_1	0.779 (ref)	.886	.662
	PercNeed_2	0.831 (23.638)		
	PercNeed_3	0.929 (25.977)		
	PercNeed_4	0.697 (19.121)		
Resignation	Resignation_1	0.833 (26.893)	.893	.735
	Resignation_2	0.841 (27.202)		
	Resignation_3	0.897 (ref)		
IPA	IPA_1	0.855 (21.496)	.893	.676
	IPA_2	0.897 (22.310)		
	IPA_3	0.808 (20.397)		
	IPA_4	0.719 (ref)		
Distrust	DisWeather_1	0.901 (38.676)	.944	.922
	DisWeather_2	0.945 (43.143)		
	DisWeather_3	0.918 (ref)		

PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

Discriminant validity was further assessed by comparing construct correlations with the square root of average variance extracted (AVE) scores. None of the construct correlation scores exceed the square root AVE scores thereby providing evidence of discriminant validity in our main data collection. The analysis of intercorrelation of constructs and descriptive statistics is provided in Table 19.

Table 19 Descriptive Statistics and Intercorrelations of Constructs

	Mean	SD	PercNeed	Resignation	IPA	Distrust
PercNeed	4.65	1.87	(.813)			
Resignation	4.22	1.66	-.046	(.857)		
IPA	3.28	1.69	-.092	.066	(.822)	
Distrust	2.83	1.37	-.009	.128	-.052	(.922)

Square root AVE shown in (); PercNeed = Perceived Need; IPA = Information Privacy Apathy; DisWeather = Distrust in weather app (app-specific)

Common Method Bias

Common method bias (CMB) refers to shared variance among variables due to the use of a common method of collecting data (Malhotra et al. 2006). Failing to reduce or control CMB can result in inflated reliability estimates and therefore faulty conclusions (Podsakoff et al. 2012). In the present study, procedural steps were taken to reduce the likelihood of introducing common method bias. Scale items were carefully constructed to avoid ambiguity as previously described, respondent anonymity was protected, and because of the medium (MTurk), other biases such as social desirability bias, acquiescence bias, and leniency bias were avoided or minimized. Nevertheless, because the collection was via a single source (MTurk) and achieved using a single instrument, the impact of CMB must be assessed.

To perform this assessment, an unmeasured latent method construct (ULMC) was added to the measurement model to determine if its introduction resulted in a significant change to model fit (Podsakoff et al. 2003; Straub et al. 2004). If a significant change is present due to the introduction of the ULMC, it is an indicator that CMB is significantly impacting the measurement model and the ULMC must be retained to account for the unwanted variance.

To assess the degree of difference in two models, a χ^2 difference test is performed. Adding the ULMC increases the degrees of freedom by one. Consequently, a difference between the models of 3.84 or more (at 0.05 significance) is an indication that variance is attributable to the addition of the ULMC and indicates the presence of CMB. The difference in χ^2 values is 0 and indicates common method variance does not have a significant impact on the dataset (see Table 20).

Table 20 Results of Common Method Bias Analysis Using Unmeasured Latent Method Construct (ULMC)

	With ULMC		**Without ULMC**	
Model	χ^2	df	χ^2	df
Unconstrained	131.319	71	131.319	70

Maximum likelihood estimation; DisWeather = Distrust proxy

Analysis of Measured Control Variables

A control variable is a variable that is held constant to reduce the confounding of variables, or to clarify a relationship between other variables. Information privacy research has used various control variables such as gender, past privacy experiences in various forms, age, privacy awareness, information sensitivity, education level, Internet experience, and previous privacy invasions (Li et al. 2014; Wittes and Liu 2015; Xu et al. 2009; Zhao et al. 2012).

To clarify relationships in the present study by determining if external factors had a significant influence on the mobile privacy calculus model, several control variables were collected: Age (BirthYr), gender, mobile device expertise (Expert), level of education attained (LevelEduc), and privacy awareness (Priv_Aware). To assess the level of impact on the structural model, relationships were created between the control variables and all the dependent variables and co-varied with all the independent variables. Using AMOS, the significance and estimates were examined and only two of the control variables were significant across all weather apps: BirthYr and Priv_Aware. Consequently, both variables were included in subsequent analyses. Detailed analyses of the control variables is provided in APPENDIX B.

Structural Model Evaluation

Rather than a path model, a full structural model was used to examine model fit and relationships between constructs. Although using a full structural model potentially results in greater measurement error when compared with a path model, the full structural model is more robust and avoids inflation of model fit. Prior to assessing relationships between constructs, the overall model must be analyzed for goodness of fit. AMOS was used to analyze the model.

The structural model was measured for each individual weather app and also using High and Low app permission groups. Because the Excessive Access construct is measured per app based on actual access requested (e.g., a single value for an app), it is not included in the individual app measurement, but is included in the High and Low permission group models. The addition of the Excessive Access construct accounts for the degree of freedom (df) increase from 169 to 184 in Table 21. With the exception of the χ^2 (6.647) for the High permission combined model, which slightly exceeds the upper recommended value of 5.0 because of the large sample size (N=2,070), all other model fit statistics are within recommended ranges. This indicates that the structural models adequately fit the data and it is appropriate to continue analysis of the relationships between constructs. See Table 21 for detailed analysis.

Table 21 Model Fit Analysis Results for Individual Apps and Combined Models

Goodness of Fit Statistic	Recommended Value	Low N=2,070	High N=2,070	Accu N=690	LW N=690	TWC N=690	WU N=690	WMP N=690	Yahoo N=690
χ^2	--	1052.681	1223.118	382.214	386.114	470.649	477.17	380.23	510.477
Degrees of Freedom (df)	--	184	184	169	169	169	169	169	169
χ^2 statistical significance (p-value)	--	.000	.000	.000	.000	.000	.000	.000	.000
χ^2 index (χ^2 / df)	$\leq 3; \leq 5$	5.721	6.647	2.262	2.285	2.785	2.823	2.25	3.021
Normed Fit Index (NFI)	$\geq .90$	.952	.943	.943	.954	.942	.941	.954	.940
Incremental Fit Index (IFI)	$\geq .90$	.960	.951	.967	.974	.962	.961	.974	.959
Tucker-Lewis Index (TLI)	$\geq .90$	.950	.939	.959	.967	.952	.951	.967	.949
Comparative Fit Index (CFI)	$\geq .90$	.960	.951	.967	.974	.962	.961	.974	.959
Root Mean Square Error of Approximation (RMSEA)	$\leq .06; \leq .08$	.048	.052	.043	.043	.051	.051	.043	.054

Accu = AccuWeather; LW = Local Weather; TWC=The Weather Channel; WU = Weather Underground; WMP = Weather by MacroPinch; Yahoo = Yahoo! Weather;

Relationships between constructs in the full structural model were examined next. First, path estimates were examined in both the High and Low permissions models (See Figure 10 and Figure 11, respectively) and then each individual app was examined (see APPENDIX C).

Within the Low model, five of the eight hypotheses modeled as direct effects were supported. Hypothesis 3, modeled as Perceived Need moderating the relationship between Distrust and Disclosure, was not supported and is discussed in the next section. Familiarity ($\beta = .000$, $p = .995$) had no effect on Distrust, however Excessive Access had a positive effect (β .258, $p < .001$) on Distrust. Resignation (β .063, $p = .033$) had a positive effect on Information Privacy Apathy. Distrust had a negative effect on Disclosure ($\beta = -.141$, $p < .001$) as did IPA ($\beta = -.058$, $p = .012$), though IPA was theorized to have a positive effect. Both Familiarity ($\beta = .322$, $p < .001$) and Resignation had a positive effect on Disclosure (β = .211, p < .001), but Perceived Need (β = .053, p =.068) had no significant effect. In total, the Low model only explains 7.4% of variance in actual disclosure of personal information on a personal mobile device (See Figure 10). A summary of the path analysis for the Low permission model is provided in Table 22 and squared multiple correlation values are provided in Table 24.

Within the High model, seven of the eight hypotheses modeled as direct effects were supported. Again, hypothesis 3, was not supported and is discussed in the next section. Familiarity (β = -.117, p < .001) had a negative effect on Distrust. As theorized, Excessive Access had a positive effect (β .143, p < .001) on Distrust. Resignation had a positive effect (β .112, p < .001) on IPA. Distrust had a negative effect on Disclosure (β = -.151, p < .001), but IPA (β = .032, p = .156) had no significant effect on Disclosure. Both Familiarity (β = .672, p < .001) and Resignation (β = .546, p < .001) had a positive effect on Disclosure, but Perceived Need (β = -.021, p =.536) had no significant effect. In total, the High model explains 21.7% of variance in actual disclosure of personal information on a personal mobile device (see Figure 11). A summary of the path analysis for the High permission model is provided in Table 23 and squared multiple correlation values are provided in Table 24.

Table 22 Path Estimates and Hypothesis Support for the Low Permission Combined Model

Hypothesis (direction)	Path Coefficient (β)	t-Values	p-value	Supported?
H1: Distrust → Disclosure (-)	-.141	-6.322	***	Yes
H2: PercNeed → Disclosure (+)	-.021	-0.894	.371	No
H3: PercNeed moderates Distrust → Disclosure (-)	.053	1.824	.068	No
H4: Familiarity → Distrust (-)	.000	0.006	.995	No
H5: Familiarity →Disclosure (+)	.322	7.089	***	Yes
H6: Excessive Access → Distrust (+)	.258	11.766	***	Yes
H7: Resignation → Disclosure (+)	.211	3.535	***	Yes
H8: Resignation → IPA (+)	.063	2.134	.033	Yes
H9: IPA → Disclosure (+)	-.058	-2.498	.012	No, reversed

*** = < .001; IPA = Information Privacy Apathy; PercNeed = Perceived Need

Table 23 Path Estimates and Hypothesis Support for the High Permission Combined Model

Hypothesis (direction)	Path Coefficient (β)	t-Values	p-value	Supported?
H1: Distrust → Disclosure (-)	-.151	-7.016	***	Yes
H2: PercNeed → Disclosure (+)	.152	4.775	***	Yes
H3: PercNeed moderates Distrust → Disclosure (-)	-.021	-.619	.536	No
H4: Familiarity → Distrust (-)	-.117	-5.015	***	Yes
H5: Familiarity → Disclosure (+)	.672	9.022	***	Yes
H6: Excessive Access → Distrust (+)	.143	6.151	***	Yes
H7: Resignation → Disclosure (+)	.546	3.109	***	Yes
H8: Resignation → IPA (+)	.112	4.023	***	Yes
H9: IPA → Disclosure (+)	.032	1.717	.156	No

*** = < .001; IPA = Information Privacy Apathy; PercNeed = Perceived Need

Table 24 Squared Multiple Correlations for All Models

Squared Multiple Correlations								
	Accu	**LW**	**TWC**	**WMP**	**WU**	**Yahoo!**	**Low**	**High**
Distrust	.03	.06	.01	.05	.02	.02	.09	.05
IPA	.05	.05	.05	.05	.05	.05	.05	.06
Disclosure	.11	.04	.08	.04	.13	.02	.07	.22

Accu = AccuWeather; LW = Local Weather; TWC=The Weather Channel; WU Weather Underground; WMP = Weather by MacroPinch; Yahoo = Yahoo! Weather;

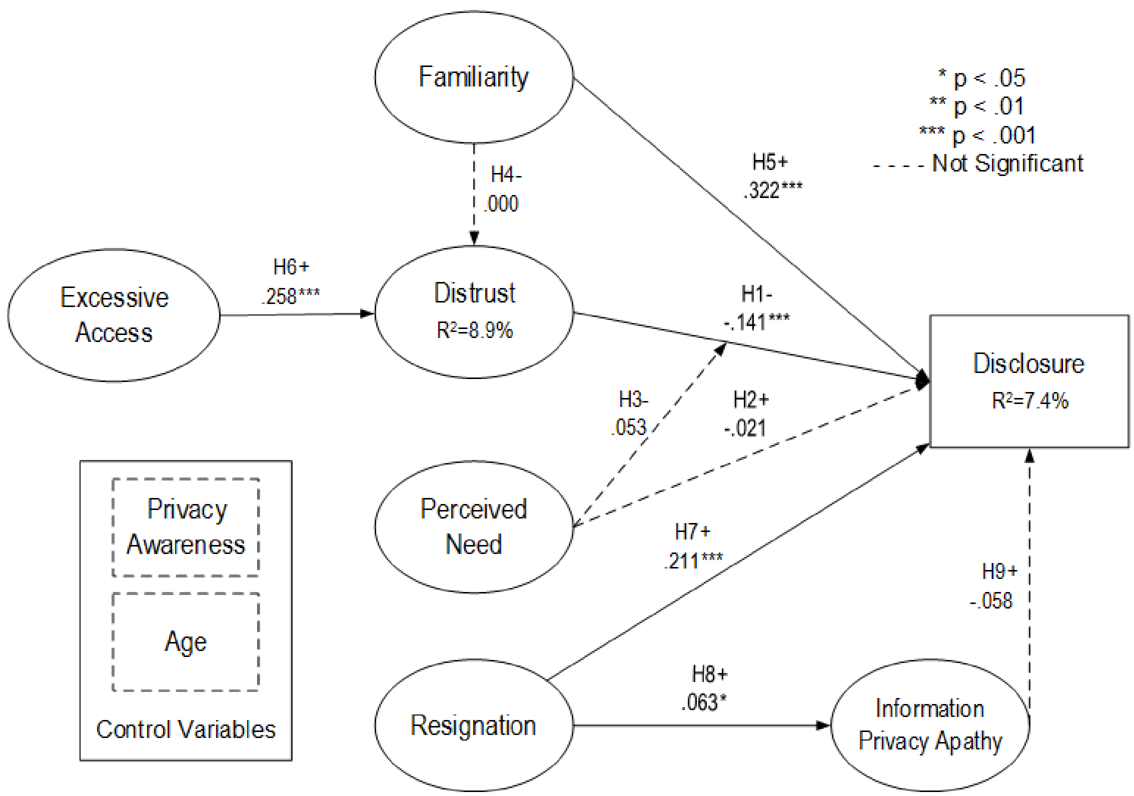


Figure 10 Low Permissions Full Structural Model with Path Estimates and Significance

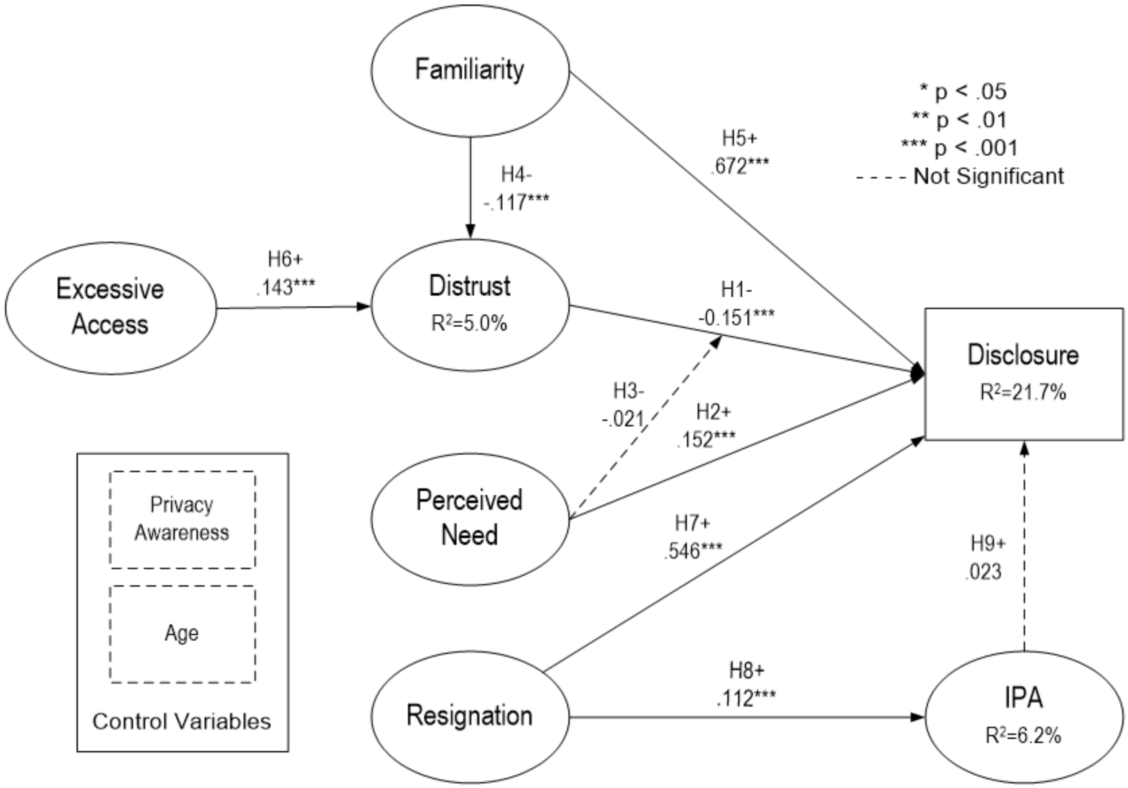


Figure 11 High Permissions Full Structural Model with Path Estimates and Significance

Analysis of Moderated Relationships

A moderating variable affects the strength or direction of the relationship between two other variables. In the present study, Perceived Need is hypothesized to weaken the relationship between Distrust and Disclosure. Two options for testing for moderation include a two-group analysis and pairwise parameter comparison. Both options require data be split into two groups, which has incurred criticism because splits are often arbitrary or otherwise lack justification (Edwards and Lambert 2007). A more accepted method to test for a moderating influence is to introduce an interaction product term. Consequently, the present study uses a two-way interaction method to assess moderation and the level of influence Perceived Need has on the relationship between Distrust and Disclosure.

First, standardized values for Distrust, Perceived Need, and Disclosure were created. Then from those standardized values a new variable (Distrust_x_PercNeed) was created by multiplying the standardized values of each of the items for Distrust by each of the items for PercNeed. Recall that analyses for the present research use a full structural rather than composite model. In neither model (High nor Low) did Perceived Need have influence on the relationship between Distrust and Disclosure. See Table 25 for the detailed analysis of the moderation test and APPENDIX D for analysis of moderation for each individual app.

Table 25 Moderation Test Results for PercNeed Moderating Distrust → Disclosure

Group	Distrust_x_PercNeed →ZDisclosure		t-Values	Supported?
	Estimate	p-value		
Low	.053	.068	1.824	No
High	-.021	.536	-.619	No

Analysis of Mediated Relationships

Three mediated relationships are posited in the mobile device privacy calculus model. Distrust mediates the influence of Familiarity on Disclosure; Information Privacy Apathy (IPA) mediates the influence of Resignation on Disclosure, and Distrust mediates Excessive Access on Disclosure. Although much information systems extant research utilizes the Sobel test for mediation analysis, bootstrapping is a more rigorous and more acceptable method to test for mediating effects (Hayes 2009).

Bootstrapping creates a sample distribution of the indirect effect and repeatedly resamples it *n* times. The process uses replacement and allows reuse of samples.

Resampling should occur between 1,000 and 5,000 times (Hayes 2009). Bootstrapping was used to determine whether significant indirect effects exist (2000 resamples were specified).

In both models (High and Low permissions), two indirect effects were significant, but one set of effects differed. For both models, Excessive Access (EA) had significant indirect effects, however, in the High permission model, the mediation was partial, but in the Low model, Distrust fully mediated EA to Disclosure. Also within the Low model, the indirect effect of Resignation on Disclosure was reversed, but in the High model, Resignation had no significant direct effect. Conversely, in the Low model, Familiarity had no significant indirect effect on Disclosure, but did have a significant indirect effect on Disclosure in the High model being partially mediated by Distrust. A detailed description of each mediation test is provided in Table 26 and analysis for mediation for each individual app is provided in APPENDIX E.

Table 26 Mediation Testing for Direct and Indirect Effects for High and Low Permission Groups

App	Relationship	Direct effect (t-Values)	Indirect effect	Confidence interval		p-value	Type
				High	Low		
Low	Familiarity→Distrust→Disclosure	.322 (7.089)	.000	.003	-.003	.988	N
Low	Resignation→IPA→Disclosure	.211 (3.535)	-.003R	.000	-.009	.031	N
Low	Excessive Access → Distrust → Disclosure	.015 (0.633)	-.005	-.004	-.007	**.001**	F
High	Familiarity→Distrust→Disclosure	.672 (9.647)	.006	.009	.003	**.001**	P
High	Resignation→IPA→Disclosure	.546 (2.842)	.009	.025	-.002	.105	N
High	Excessive Access → Distrust → Disclosure	-.157 (-6.448)	-.006	-.004	-.009	**.001**	P

P = partial mediation; F = full mediation; N = no mediation; R = reversed; 95% bias-corrected confidence intervals; 2000 bootstrap samples

Below is a summary of which hypotheses were supported for the combined models and for each of the six apps (see Table 27).

Table 27 Summary of Hypothesis Support for Low and High Permission Groups

	Low	High
H1: Distrust → Disclosure (-)	**Yes**	**Yes**
H2: PercNeed → Disclosure (+)	No	**Yes**
H3: PercNeed moderates Distrust → Disclosure (-)	No	No
H4: Familiarity → Distrust (-)	No	**Yes**
H5: Familiarity → Disclosure (+)	**Yes**	**Yes**
H6: Excessive Access (+)	**Yes**	**Yes**
H7: Resignation → Disclosure (+)	**Yes**	**Yes**
H8: Resignation → IPA (+)	**Yes**	**Yes**
H9: IPA → Disclosure (+)	Rev	No

Rev = significant, but opposite hypothesized direction

Two-Group Analysis

The set of six weather apps examined in this study were split into High and Low permission groups as described in Chapter 3. What follows are the results of examining the differences between the High and Low groups. Specifically, each construct relationship was compared across the groups to determine whether the difference is significant and which relationship is stronger.

Using AMOS, one relationship between two constructs was constrained across the models, while the rest of the relationships in both models were unconstrained. After running the calculations, the difference in χ^2 values was obtained to determine if a significant difference existed. If the difference is significant, the individual parameter estimates are also examined to determine which of the relationships is stronger. This process was repeated for each construct relationship and the results are presented in Table 28.

Of the eight relationships between constructs in the research model, six significantly differ between the High and Low app permission groups, but neither the relationship between Excessive to Distrust, nor Distrust to Disclosure demonstrated significant differences between the High and Low models. Every significant relationship except IPA → Disclosure was stronger in the High permission app group (see Table 28).

Table 28 Two-group Analysis of High and Low App Permission Groups

Relationship	$\Delta\chi^2$	**p-value**	**High EA Group Estimate**	**Low EA Group Estimate**
Familiarity → Distrust	13.214	***	**-.117**	.000
Excessive Access → Distrust	1.021	.312	N/A	N/A
Distrust → Disclosure	.064	.800	N/A	N/A
PercNeed → Disclosure	19.71	***	**.152**	-.021
Resignation → IPA	9.641	.002	**.112**	.063
IPA → Disclosure	7.627	.006	**.032**	-.058
Resignation → Disclosure	24.274	***	**.546**	.211
Familiarity → Disclosure	9.277	.002	**.672**	.322

EA = Excessive Access

Summary

In this chapter, pilot study results were presented, including results from an exploratory factor analysis and a confirmatory factor analysis. Using these two processes, support was found for construct validity and reliability as well as good model fit for the measurement model. Following the pilot study, results from the main study were presented. Results from the two-step approach recommended by Anderson and Gerbing (1988) provided strong support for convergent validity, discriminant validity, and reliability of the survey instrument. Common method variance was assessed and lacked significant influence and the structural model exhibited good model fit. Perceived Need show no significant influence as a moderator between Distrust and Disclosure, but four of the six mediating relationships across both models (High and Low) demonstrated either full or partial mediation. Hypothesis tests on the Low model indicated 5 of 9 supported hypotheses while the High model indicated 7 of 9 supported hypotheses.

CHAPTER V

CONCLUSION

Introduction

Extant information in privacy disclosure research relies heavily on the privacy calculus model proposed by Dinev and Hart (2006), which was conceived prior to the existence of personal mobile devices in use today. The objective of this dissertation is to examine a privacy calculus model specific to personal mobile devices that predicts and explains personal information disclosure. The proposed model deliberately omits the risk-benefit analysis, which is the core concept of the traditional privacy calculus. Instead, six constructs are proposed: Excessive Access, Familiarity, Distrust, Perceived Need, Resignation, and Information Privacy Apathy. Excessive Access, Familiarity, and Distrust apply to the app Context. Perceived Need applies to the app category context (e.g., the need for weather information rather than the need for a specific weather app). Resignation and Information Privacy Apathy apply to the individual context. This chapter presents a detailed discussion of the findings provided in Chapter IV, the contributions those findings make to theory and practice, a post-hoc analysis of the data collected, a discussion about the limitations of the present study, and a map of future research of privacy calculus models for personal mobile devices.

Discussion

Users of mobile apps enter into a privacy calculus prior to making personal information disclosure decisions (Keith et al. 2013; Xu et al. 2012). One of the objectives of this dissertation is to suggest an alternative to the traditional, deliberate, and conscious risk-benefit process associated with intent to disclose personal information (Dinev and Hart 2006).

To test the hypotheses of this alternative privacy calculus, respondents were asked to give reviews of six weather apps. The study was framed as a review rather than a privacy study to avoid priming respondents, which would encourage them to answer privacy questions in socially desirable ways. Weather apps were chosen because they are a nearly optimal type of app for this study. Everyone understands weather, and has varying degrees of need for weather information (from no need to very high need). Because the core features and information of weather apps are similar, they are roughly interchangeable, yet distinguishable by unique features. Furthermore, it is highly unlikely for users to form an extreme connection or addiction to weather apps as they might a game or to social media which could skew results. However, in one aspect, the choice of weather apps may have been problematic. Because weather apps appeal so broadly to PMD users, weather apps are almost always included with the base configuration of PMDs by the manufacturer. The presence of weather apps installed by default, coupled with the interchangeable nature of the apps may have confounded Perceived Need. In the present study, 37.4% of respondents either use their built-in weather app, or indicated they have not installed any weather app (which may again indicate using the built-in app). Consequently, one probable explanation for the lack of significance of Perceived

Need, is that one or more apps are already available in the default Android configuration, which lowers Perceived Need of an additional app providing the same information.

Structural Model Results

The low coefficient of determination results have at least two interpretations. First, additional factors beyond what is hypothesized in the research model are influencing privacy decisions. Congruent with hypothesis 5, in both models, Familiarity displayed a strong influence over Disclosure and also, as predicted in hypothesis 7, Resignation also has a significant impact on Disclosure. In both models, Familiarity and Resignation have the strongest influence on Disclosure, however, only 7.4% of the variance of Disclosure is explained in the Low model. The amount of variance explained in the High model is 21.7%. Logically, other factors beyond what is hypothesized are impacting the disclosure of personal information.

Second, the operationalization of disclosure may not be optimal, though it is reliable and valid. Disclosure, as described in chapter 3 is modeled as a continuous variable, however, it only provides four points of measure: uninstalling, ignoring, keeping, or installing. Four data points may not be granular enough to capture the complexity of personal information disclosure via apps. Because apps run the gamut of disclosure from no information (legitimate flashlight app) to thousands of data points (Facebook), a more granular disclosure mechanism may be warranted. In the present study, the six weather apps also request a significant range of information.

Despite prior research indicating the important role apathy plays in privacy and security (Boss et al. 2009; Charlton and Birkett 1995; Cone et al. 2007; Kirsch and Boss 2007; Sharma and Crossler 2014; Yoo et al. 2012) as well as within self-efficacy

(Bandura 1982), IPA had no significant impact in either model. The characteristic of users who either place a low value on their data, or who place a low value on their privacy, was not a significant influence on personal information disclosure. One possible explanation for the lack of significance of IPA is that though it is reliable and valid as a measure of dispositional individual apathy, IPA may be more effective if measured situationally (e.g., in the context of an app category or a single app). The tendency to adopt a perspective of futility or apathy regarding protection of personal information is modeled as a disposition of an individual and is measured in that way. IPA specifically measures an *individual's* apathy towards disclosure across all apps in the Google Play store. Perhaps the intended measure should be at the app level (situational) instead of the individual level. This would be less consistent with psychology literature upon which the item is based, but more consistent with information privacy literature that has adopted a situational approach to privacy (Kehr et al. 2015; Li et al. 2010; Solove 2006). Similar to how Kehr et al. (2015) measures Information Sensitivity and Affect in a situational manner, IPA may prove to be more effective if operationalized at the app level rather than the individual level. In the PMD context, different apps request and use different types and levels of information. App-level measurement is also consistent with Li et al. (2010)'s concept of different domains evoking different privacy concerns.

For the Low permission model, users' assessment of apps that requested excessive access to their information increased their level of distrust of the app which significantly influenced reduced disclosure of personal information on their mobile device. Greater familiarity with the app, brand, or developer significantly increased users' actual disclosure of personal information. However, users' perceived need had no influence on disclosure nor did it weaken or strengthen the level of distrust leading to disclosure or non-disclosure. Similarly in the Low permission model, a user's level of information privacy apathy had no significant impact on whether or not a user disclosed personal information on their PMD.

Within the High permission model, users' perceived need for weather apps did significantly influence disclosure of personal information. One reason may be that apps with increased permissions typically offer a greater number of features that increase the strength of a users' perceived need and thereby increase disclosure. However, in the same manner as the Low permission model, Perceived Need did not significantly strengthen or weaken the relationship between Distrust and Disclosure. In both High and Low models, Resignation and Familiarity are most influential on Disclosure, but in neither model does IPA have significant impact on Disclosure.

Two-Group Analysis Findings

Results from analyzing apps with a high level of permissions compared to apps with a low level of permissions yielded consistent, expected, and interesting results. Every significant indicator of difference was relatively stronger in the High group (IPA→Disclosure showed a significant difference, but is not supported by any app, nor by either model). The Excessive Access → Distrust relationship and Distrust → Disclosure relationship did not significantly differ between the High and Low models. A high level of permissions is correlated with a greater level of popularity (Chia et al. 2012) which holds true in the present study. Because High permission apps are highly popular and have nationally recognized brands (The Weather Channel, Yahoo!, AccuWeather), Familiarity → Disclosure and Familiarity → Distrust both have relatively stronger influences in the High model.

Also of interest is the comparison of Resignation → Disclosure between the two models. Of all the relationships between constructs compared between the two models, Resignation → Disclosure has the greatest difference score. This may be explained by how individuals rationalize disclosure of a large amount of information. Individuals entering into a decision process to disclose an excessive amount personal information may rationalize that disclosure by exhibiting a greater level of Resignation leading to disclosure than those confronted with a low level of disclosure. This is consistent with Sharma and Crossler (2014) who posit that users may believe their information is already "out there."

Overall Findings

Prior privacy calculus research has relied heavily on the notion that users perform a rational, conscious and deliberate risk-benefit analysis prior to disclosure. Consistent with rational choice theory, mobile users are expected to perform an assessment of benefits and costs (risks) (Paternoster and Simpson 1996); they maximize benefits as they attempt to anticipate future consequences of disclosure (Becker and Murphy 1988). In the present study, findings indicate other forces outside of this risk-benefit analysis are significant and warrant additional research. Resignation, a construct introduced in the present research as a new component of the mobile privacy calculus, showed significant influence in both High and Low models and motivates further research. Information Privacy Apathy was unsupported in all models, which suggests a new approach is required to uncover the influence of IPA on disclosure, if such influence exists. Perceived

Need also had lower than expected impact on the overall model, which may mean re-examining how Perceived Need is measured or increasing the granularity of how personal information disclosure is measured. Even though coefficient of determination values were low, the model demonstrated significance for 5 of 9 and 7 of 9 hypotheses for the Low and High model, respectively. Hypothesis support combined with a 21.7% coefficient of determination value for disclosure in the High permission model indicates the proposed model has value as a starting point to further develop a privacy calculus model for personal mobile devices.

Research Contribution

Results from the present study offer new avenues of explanatory and predictive mechanisms for information disclosure on a personal mobile device. The overall findings provide new perspectives into mobile privacy calculus research and suggest new modes of thinking about how individuals actually disclose information on personal mobile devices. The present study provides a solid example of how to capture and model actual disclosure on a PMD. It also confirmed that both from a technical and cultural standpoint, collection of actual disclosure data is pragmatic and scalable. Future information privacy research should use similar methods to collect actual disclosure data from individuals using real-world apps rather than from contrived and obscure apps presented within the safety of the university context. Practical insights and recommendations are provided for app developers, regulators, and those involved with constructing privacy policy. Contributions to theory and practice are discussed below.

Contribution to Theory

The overall findings support the continued research to derive a mobile privacy calculus model with greater explanatory and predictive power. The present study offers several contributions to the mobile privacy calculus research.

Actual disclosure data was collected directly from mobile devices using a novel Android app. The app provides confirmation of self-reported data as well as permission and privacy data that is too detailed and cumbersome for the user to report manually. Collection of actual data avoids confounding results that plague other privacy research that measure intention (Joinson et al. 2010). The app provides these benefits without requesting any sensitive permissions, which would potentially bias the sample to individuals less sensitive to disclosing information.

A new construct was introduced to Information Security research. Resignation was adapted from the concept of learned helpless in psychology (Maier and Seligman 1976). It was developed, tested, and refined in the present study. Resignation showed significance in both High and Low permission models. Results offer motivation for future researchers to consider the role of Resignation as an explanatory variable towards personal information disclosure.

Few studies have developed and tested apps in a real-world setting—most opting to use surveys, present scenarios, or offer contrived mobile apps for evaluation within a university setting (Sutanto et al. 2013). The study demonstrates how to leverage actual real-world apps available on the Google Play store rather than from contrived, artificial apps. Actual configuration of real-world apps provides realism difficult or impossible to achieve with laboratory apps. This level of realism enables the study to draw stronger theoretical conclusions.

Measuring IPA within the individual context IPA was definitively insignificant. The insignificance of IPA is also an interesting research question and opportunity for further research into its potential role. Consistent with privacy research suggesting situational cues may offer greater explanatory power than dispositional or attitudinal approaches (Kehr et al. 2015), findings suggest measuring apathy as a situation-specific construct would be more effective.

The relevance of Excessive Access as a component of the mobile privacy calculus is confirmed. Although this is consistent with prior research regarding increased perceived risks (Kehr et al. 2015; Keith et al. 2013), the present research sharpens our understanding by referencing intrusiveness compared to app functionality. For example, a weather app providing local conditions logically requests permissions to access location, but requesting permission to read and send email may be viewed as excessive. Grouping respondent observations by High and Low permissions requested by the app demonstrated the significance of Excessive Access as a component to better understand how users make information disclosure decisions. Relationships between constructs were significantly different between the two groups, which underscores the role that Excessive Access has on the privacy decision process.

The present study also provided additional insight into control variables that significantly influence mobile privacy calculus research. Consistent with prior mobile privacy calculus research, Privacy Awareness and age (Sutanto et al. 2013) were significant control variables, however, contrary to Keith et al. (2013), mobile computing self-efficacy was not a useful control variable.

Finally, the present research provides an example of how to avoid priming respondents on privacy and security. One of the challenges to previous research regarding the privacy calculus is the priming effect caused simply by asking privacy protective questions (Joinson et al. 2010). Privacy paradox research indicates that individuals cite confounding factors when questioned about future privacy practices (Dienlin and Trepte 2015; Norberg et al. 2007). Social desirability may motivate users to answer positively about their future intentions to protect privacy when their actual disclosure behavior is ultimately contrary (Wilson and Valacich 2012). In the present study, great care was taken to present the survey instrument as an overall review of which privacy was simply one aspect thus avoiding a priming effect.

Contribution to Practice

Information is the primary currency in the age of Big Data and understanding how users decide to share information helps app developers and regulators better understand and serve the needs of customers while maximizing the amount of information that can be obtained from them (George et al. 2014). Coupled with the increasing dependence and ubiquity of PMDs, this research has implications for a wide range of participants in mobile privacy—consumers, app developers, privacy advocates, policymakers and governmental legislators, and distribution channels such as the Google Play store, Apple's App Store, and Amazon's Appstore.

Findings underscore the concept that users make disclosure decisions in ways other than a careful assessment of risk versus benefit. Although there is some indication that users react cautiously to apps that request excessive access (King 2012; Xu et al. 2009), the present study suggests familiarity with apps and resignation towards data protection are stronger components of the disclosure decision process. Practitioners desiring greater levels of information disclosure would benefit from high levels of familiarity and resignation.

Another conclusion from this study is that app developers should focus less on winning the risk-benefit scenario and more on limiting permissions requests to those that are necessary for functionality. They should focus less on engendering trust than avoiding distrust. For apps with high permission levels, familiarity with the brand or developer lowers distrust, however they should also understand that excessive access increases distrust, and distrust results in users withholding information.

Results also have implication for privacy advocates, policymakers, and legislators. This group should not draw conclusions regarding the homogeneity of users' willingness to disclose data. Seemingly voluntary disclosure is likely not the result of an agreeable and deliberate choice by the users. Rather, findings show that users may be disclosing personal information because they are resigned to the fact that no actions they take as individuals has any positive impact towards protecting their information. This is consistent with prior research that demonstrated that the more individuals understood about how their data was collected and used, the more (not less) likely they were to disclose data (Turow et al. 2015). To assume that their disclosure equals voluntary consent and agreement is a faulty assumption.

Finally, distribution channels should take note of the implicit trust conferred on their channel (Reinfelder et al. 2014) and work diligently to protect it. Results indicate that distrust of specific apps or developers is a significant factor preventing individuals from using the channel. Efforts to increase transparency of app capabilities is paramount to maintaining the user's trust, to give control and thereby reduce distrust.

Post-Hoc Analysis

In this section, further analysis is provided to explore other methods of examining the apps and ultimately underscore the effectiveness of the current study. First, the analysis of individual path estimates is provided, then an alternative two-group analysis is presented, and overall findings are discussed.

Individual App Path Analysis

Because the High and Low permission groups are each made up of three individual apps, examining each app by itself is a logical step in the post hoc analysis. Relationships that are significant, but reversed in direction are anomalous, and may provide interesting insights about the model. Of the six apps examined, the only individual app with reversed significant results is Local Weather. Recall from Chapter 3 (see Figure 8) that Local Weather (LW) requires no sensitive permissions and is the least downloaded (see Table 30). It is also the second most obscure app among the six apps examined. Taken together, hypotheses four and five predict that as the user's familiarity with an app increases, distrust will decrease and disclosure will increase. The latter is supported by Local Weather, but curiously, the former is reversed (see Table 29). This may indicate that for this specific app, the experience reported by users is negative. Namely, that as their familiarity with LW increased, so did their distrust.

The reversed association of the user's familiarity with distrust may also offer an explanation for the reversal of hypothesis nine regarding the influence of IPA on disclosure. The hypothesized relationship between IPA and disclosure is that as apathy increases so does disclosure. However, in this case, it is possible that because of distrust, the reverse of hypothesis nine may apply. Specifically, that *because* I distrust LW, greater care (arguably the negative of apathy) is associated with greater disclosure, which explains a decrease in apathy correlating with an increase in disclosure. This explanation, however, would require measuring IPA at the app-level rather than as an individual attribute as originally developed for this study.

Equally as curious is that IPA, aside from the reversals in the Low and LW analyses, is not significant for any app (see Table 29). Drawing from psychology, apathy as a general concept is an attribute of an individual (Marin 1990). However, apathy may have different levels of impact for different types of situations, or in the present study, apps that access and use different types of information. Apathy is operationalized for the individual in relation to attitudes towards apps in the Google Play store (see APPENDIX A). Based on the findings, one likely explanation for the lack of significance and reversed direction is that IPA should be measured at a different level. In the same manner that Kehr et al. (2015) measured Information Sensitivity and Affect as situational factors, IPA may also perform better as an indicator of apathy if it is measured situationally at the app level. Specifically, IPA may perform better if measured in context of the type, sensitivity, and breadth of information to be disclosed. This is discussed further in the structural model results.

Table 29 Summary of Hypothesis Support

	Low	High	Accu	LW	TWC	WMP	WU	Yahoo
H1: Distrust → Disclosure (-)	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
H2: PercNeed → Disclosure (+)	No	**Yes**	**Yes**	No	No	No	No	**Yes**
H3: PercNeed moderates Distrust → Disclosure (-)	No	No	No	No	No	No	**Yes**	No
H4: Familiarity → Distrust (-)	No	**Yes**	**Yes**	Rev	No	No	**Yes**	**Yes**
H5: Familiarity → Disclosure (+)	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	No
H6: Excessive Access (+)	**Yes**	**Yes**	N/A	N/A	N/A	N/A	N/A	N/A
H7: Resignation → Disclosure (+)	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	No
H8: Resignation → IPA (+)	**Yes**	**Yes**	No	No	No	No	No	No
H9: IPA → Disclosure (+)	Rev	No	No	Rev	No	No	No	No

Accu = AccuWeather; LW = Local Weather; TWC=The Weather Channel; WU Weather Underground; WMP = Weather by MacroPinch; Yahoo = Yahoo! Weather;

App Popularity as an Alternative Grouping of Apps

Because the dependent variable of this study is disclosure, a logical method of dividing apps into group is between those requesting high levels versus those requesting low levels of information access. To that end, analyses in this study were done using apps that have a significantly different number of sensitive and overall permissions as previously described (see Table 2). However, other research has used mobile app and platform popularity as a division criterion (Almuhimedi et al. 2015; Enck et al. 2014; Federal Trade Commission 2012; Mansfield-Devine 2012; Pan et al. 2011). To assess the usefulness of popularity as an alternate divisor, each of the six app's popularity was obtained from the Google Play store. Although the Google Play store does not list actual installation figures, they classify apps by number of downloads. Using these figures, the six apps were divided into a High, Medium, and Low popularity groups. The criteria used to divide the apps is provided in Table 30.

Table 30 Criteria for Grouping Weather Apps by High and Low Popularity

Application	**Number of downloads**	**Group Popularity**
The Weather Channel	50 million – 100 million	High
AccuWeather	50 million – 100 million	
Yahoo! Weather	10 million – 50 million	Medium
Weather by Macro Pinch	10 million – 50 million	
Weather Underground	5 million – 10 million	Low
Local Weather	1 million – 5 million	

Although an increase in popularity is often correlated with an increase in permissions, in this case Weather by Macro Pinch (WMP) only requests 5 permissions. Though WMP is more popular than Weather Underground, and in the same download class as Yahoo! Weather, it requests far fewer permissions. Nevertheless, an analysis of popular apps versus unpopular apps yielded few significant differences, suggesting that using popularity as a means of categorization is not as useful as excessive access. See Table 31, Table 32, and Table 33 for a detailed analysis of comparing the research model using observations from comparing High, Medium and Low.

Table 31 Two-group Analysis of Apps with High and Low Popularity

Relationship	$\Delta\chi^2$	**p-value**	**High Popular Estimate**	**Low Popular Estimate**
Familiarity → Distrust	8.671	.003	**-.140**	-.023
Excessive Access → Distrust	.591	.442	N/A	N/A
Distrust → Disclosure	1.997	.158	N/A	N/A
PercNeed → Disclosure	3.471	.062	N/A	N/A
Resignation → IPA	4.779	.029	**.118**	.065
IPA → Disclosure	8.278	.004	**.064**	-.050
Resignation → Disclosure	.538	.463	N/A	N/A
Familiarity → Disclosure	.324	.569	N/A	N/A

Table 32 Two-group Analysis of Apps with High and Medium Popularity

Relationship	$\Delta\chi^2$	**p-value**	**High Popularity Estimate**	**Medium Popularity Estimate**
Familiarity → Distrust	11.005	.001	**-.140**	.005
Excessive Access → Distrust	.228	.633	N/A	N/A
Distrust → Disclosure	12.624	.000	**-.203**	-.135
PercNeed → Disclosure	3.049	.081	N/A	N/A
Resignation → IPA	7.689	.006	**.118**	.064
IPA → Disclosure	6.895	.009	**.064**	-.038
Resignation → Disclosure	.130	.719	N/A	N/A
Familiarity → Disclosure	1.196	.274	N/A	N/A

Table 33 Two-group Analysis of Apps with Medium and Low Popularity

Relationship	$\Delta\chi^2$	**p-value**	**Medium Popular Estimate**	**Low Popular Estimate**
Familiarity → Distrust	.481	.488	N/A	N/A
Excessive Access → Distrust	2.149	.143	N/A	N/A
Distrust → Disclosure	3.698	.054	N/A	N/A
PercNeed → Disclosure	.091	.762	N/A	N/A
Resignation → IPA	.344	.557	N/A	N/A
IPA → Disclosure	.288	.592	N/A	N/A
Resignation → Disclosure	9.922	.002	-.058	**.152**
Familiarity → Disclosure	16.224	.000	.054	**.281**

Dividing the groups by popularity is a less informative division with only four, three, and two relationships, respectively, out of eight indicating a significant difference. Dividing the apps by Excessive Access resulted in six of eight significant relationships.

Limitations

All research is flawed and has intrinsic limitations. Limitations for the present study include choice of app, sample selection, and context of personal mobile device.

Although weather apps may be among the most widely used and therefore most applicable and generalizable, weather apps do not offer the affordances of other apps such as Facebook, GroupMe, Snapchat, and games in general evoke. Additional research using apps with high Perceived Need is necessary.

The sample is limited to the United States. Extant research strongly supports differences in privacy attitudes for different cultures and different geographic regions (Dinev et al. 2005, 2006; Lowry et al. 2011; Posey et al. 2010). Conclusions from this study may only generalize to the United States.

Respondents were limited to PMDs using the Android operating system. Android and iOS devices are very similar and offer the same hardware features and similar apps. However, limited research has suggested a possible difference in platforms (Reinfelder et al. 2014), though results are inconclusive. Although unlikely because of their similarity, a possible limitation exists that the findings are generalizable only to users of the Android platform.

Future Research

More experimentation and field studies in the area of PMD information disclosure are required. Because intent is the predominant dependent variable in privacy research, and intent is a poor predictor of actual disclosure (Keith et al. 2013), more actual disclosure data is needed (Crossler et al. 2013; Warkentin et al. 2012, 2016). The technology is available to capture users' actual disclosure decisions and future research must include data collected from those decisions.

A wider range of apps should be tested. As discussed in the previous section, users have varying degrees of attachment and need for mobile apps bordering on addiction and obsession (Lin et al. 2015). Future research should examine the privacy calculus for personal mobile devices in the context of intense perceived need. Specifically, research into apps with potential for very high perceived need (e.g., Facebook, Snapchat, highly popular games) should be examined at the permission level. Data should be gathered on precisely which permissions have been granted or denied for such an app to better understand the components, and the strength of those components in the personal mobile device privacy calculus.

Another potentially fruitful area of research is applying different categories of apps to the model. For example, the components of decision-making for sharing information gaming apps may significantly differ from high-end and expensive private airplane tools or financial trading software. Does the category of an app correlate with lower distrust and higher disclosure? If the app has a relatively high cost, does that result in lower distrust?

Another interesting area of research is a comparison between privacy awareness and privacy concerns of individuals using different platforms. A simplistic 2014 study of 700 German students regarding the privacy and security differences in iOS and Android users indicated mixed results between the platforms (Reinfelder et al. 2014). The study, though only examining security and privacy in a cursory manner, highlights the need for further investigation on this topic. Based on the highly-publicized confrontation between the FBI and Apple, Inc. there may be a widely held perception that an iPhone is inherently more secure than an Android device. The FBI had great difficulty breaching the security of an iPhone, but eventually gained access (Kravets 2016). The cost to gain access was reportedly over $1 million and the FBI indicated it was only for a specific older model of the iPhone (Lichtblau and Benner 2016). If this perception is true, it has profound impacts on conclusions made from studies considering only a single type of device (including this dissertation and nearly all extant research using mobile devices). To avoid potential bias in this area, the present study examined several control variables including configuration expertise and privacy awareness, however, specific research into the potentially different mindsets or behavior intrinsic to specific device platform owners may prove fruitful.

Another potentially fruitful area of research coming from this dissertation is information privacy apathy (IPA). Although some research involving IPA exists, much more research into this area is warranted. One of the surprising results of the present study is a lack of significance influence of IPA on Disclosure. Prior research as well as informal discussions with many subjects has indicated that information privacy apathy exists (van den Hoogen 2009; Sharma and Crossler 2014; Yoo et al. 2012). Additional research may be necessary to better operationalize information privacy apathy in the context of smartphones and other mobile devices.

Similarly, Resignation was introduced as a construct in this paper. As more and more devices become internet-enabled (i.e., the Internet of Things [IoT]), and as data analytics, or big data, achieve greater maturity and capability, individual information privacy is threatened. Protecting one's personal information from unauthorized access and secondary use may very well seem impossible. The concept that no actions taken will have any effect towards protecting one's information, or resignation, will only increase in significance and importance to explain and predict user behavior.

Researchers must be diligent to avoid priming respondents about proper information privacy practices. Almost without exception, privacy calculus studies prime their subjects by asking questions focused on proper privacy measures. Keith et al. (2016) performs a pretest to measure privacy concern, Kehr et al. (2015) measures general privacy concerns and institutional trust prior to their main data collection. Other research similarly performs assessments or measurements to privacy concerns or awareness which prime the user to potentially answer in socially desirable ways (Keith et al. 2013; Malhotra et al. 2004; Moloney and Potì 2013). Item priming effects refer to positioning predictor variables in such a way as to imply a causal relationship with other variables (Podsakoff et al. 2003). It is similar to asking a subject if they plan to floss their teeth. Just by asking the question you have influenced the answer. It is socially desirable to answer yes. The subject may have no intent to floss, but by asking the question, intent has been transferred to the subject. Better is to actually observe the subject's flossing behavior without inadvertently directing them to do it.

Studies that attempt to deceive subjects using apps have used contrived apps (Kehr et al. 2015), which limits realism or have used them in university settings (Keith et al. 2013), which by the context alone engenders high levels of institutional trust (Pavlou 2002). Participants who are asked to rate a contrived app as part of a study confer trust on that app because it is part of the study. Likewise, students who are introduced to an app for the first time in the context of research and extra credit for participation naturally (and rightly) assume that their privacy will not be compromised. Future research must avoid a privacy-safety bias. This research provides an example of how to obtain actual data from the real-world using real apps obtained from the dominant app market.

A follow-up qualitative study on how privacy disclosure decisions are made would also be a good tool to better understand user's actual thinking during the app installation process. Several studies have used a method whereby subjects talk through every aspect of their decision process as they make decisions similar to a free form output of all thoughts related to what they are doing. For example, Komiak and Benbasat (2008) asked subjects to think aloud while interacting with recommender agents. Utterances were recorded, transcribed and independently analyzed by multiple judges to identify salient characteristics of their decision-making process. By training the user to speak a constant stream of thought without interruption, it may be possible to uncover new insights into how users actually form decisions to disclose personal information on a mobile device.

For example, as they are installing, did they scroll down to examine permissions or bypass permissions altogether? If examining permissions, what questions did they ask themselves? When prompted by an app for additional permissions, what is their thought process? The subject's actual commentary would be recorded and coded. Specific components or themes present would be identified and studies for additional insight into the mobile app disclosure process. This process would work equally as well on an iPhone as it would an Android device.

Very few research projects to date have taken advantage of the ability to track user behavior on the smartphone device. Both the iPhone and Android devices enable users to turn on and turn off various security permissions. Extant research is limited to a single snapshot in time of an individual's configuration settings. Little or no research exists today that tracks the users disclosure decisions over time. While tracking permission changes on a mobile device, users could be confronted with excessive information access requests and actual disclosure decisions could be captured to further develop the privacy calculus model.

Conclusion

The power and reach of personal mobile devices is continually increasing. The capabilities of a PMD to monitor, store, and transmit personal information are staggering and those capabilities are expanding. Entire business models are based on the ability to obtain information. Having an understanding of how individuals arrive at a decision to disclose or not to disclose personal information using a PMD is highly valuable. The present research has placed a question mark over the traditional privacy calculus as it applies to traditional desktop and web computing environments.

The findings described in this study are relevant for both practitioners and information privacy researchers. By demonstrating the significance of a novel privacy calculus model for PMDs, practitioners have initial guidance on what to emphasize and what not to emphasize when seeking personal information disclosures. Researchers have gained an additional construct and intermediary model towards a better understanding of actual disclosure on a personal mobile device. The present model, devoid of the deliberate risk-benefit trade-off, still showed significance in seven of its nine hypotheses. A new and more effective privacy calculus model for PMDs exists and the present research is an incremental step towards defining that model and provides a stepping stone for future work developing a privacy calculus for personal mobile devices.

REFERENCES

Acquisti, A. 2002. "Protecting privacy with economics: Economic incentives for preventive technologies in ubiquitous computing environments," in *Proceedings of Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02)*, Citeseer.

Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *Proceedings of the 5th ACM Conference on Electronic Commerce*, ACM, pp. 21–29.

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), American Association for the Advancement of Science, pp. 509–514.

Acquisti, A., and Gross, R. 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy Enhancing Technologies*, Springer, pp. 36–58.

Acquisti, A., and Grossklags, J. 2003. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior," in *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3).

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

Addonizio, G. 2016. "The privacy risks surrounding consumer health and fitness apps, associated wearable devices, and HIPAA's limitations," in *Law School Student Scholarship*.

Ajzen, I. 1985. *From Intentions to Actions: A Theory of Planned Behavior*, Berlin: Springer.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs: Prentice-Hall.

Alashoor, T., and Baskerville, R. 2015. "The privacy paradox: The role of cognitive absorption in the social networking activity," in *Thirty Sixth International Conference on Information Systems, Fort Worth*, pp. 1–20.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L., and Agarwal, Y. 2015. “Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging,” *Proc. of the 2015 ACM conference on Human factors in computing systems (CHI)* (doi: 10.1145/2702123.2702210).

Anderson, J. C., and Gerbing, D. W. 1988. “Structural equation modeling in practice: A review and recommended two-step approach.,” *Psychological Bulletin* (103:3), American Psychological Association, p. 411.

Anderson, M. 2015. “Summary: Key takeaways on mobile apps and privacy,” *Pew Research Center* (available at http://www.pewresearch.org/fact-tank/2015/11/10/key-takeaways-mobile-apps/; retrieved January 1, 2015).

Andriatsimandefitra, R., Tong, V. V. T., and Mé, L. 2012. “User data on Android smartphone must be protected,” *Cybercrime*, p. 18.

Apple, I. 2016. “Apple ID Frequently Asked Questions,” (available at https://appleid.apple.com/faq; retrieved May 15, 2016).

Balebako, R., Jung, J., Lu, W., Cranor, L. F., and Nguyen, C. 2013. “‘Little brothers watching you:’ Raising awareness of data leaks on smartphones,” in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, p. 12.

Bandura, A. 1982. “Self-efficacy mechanism in human agency,” *American Psychologist* (37:2), pp. 122–147 (doi: 10.1037/0003-066X.37.2.122).

Barnes, S. B. 2006. “A privacy paradox: Social networking in the United States,” *First Monday* (11:9).

Becker, G. S., and Murphy, K. M. 1988. “A theory of rational addiction,” *Journal of political Economy* (96:4), The University of Chicago Press, pp. 675–700.

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

Bhattacherjee, A. 2001. “Understanding information systems continuance: An expectation-confirmation model,” *MIS Quarterly* (25:3), pp. 351–370.

Bollen, K., and Lennox, R. 1991. “Conventional wisdom on measurement: A structural equation perspective,” *Psychological Bulletin* (110:2), pp. 305–314 (doi: 10.1037//0033-2909.110.2.305).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. “If someone is watching, I’ll do what I’m asked: Mandatoriness, control, and information security,” *European Journal of Information Systems* (18:2), pp. 151–164 (doi: 10.1057/ejis.2009.8).

Bradbury, D. 2015. "The kids are alright [Privacy Online]," *Engineering & Technology* (10:1), IET, pp. 30–33.

Campbell, D. T., and Fiske, D. W. 1959. "Convergent and discriminant validation by the multitrait-multimethod matrix.," *Psychological Bulletin* (56:2), American Psychological Association, p. 81.

Charlton, J., and Birkett, P. E. 1995. "The development and validation of the computer apathy and anxiety scale," *Journal of Educational Computing Research* (13:1), pp. 41–59.

Chellappa, R. K., and Shivendu, S. 2007. "An economic model of privacy: A property rights approach to regulatory choices for online personalization," *Journal of Management Information Systems* (24:3), pp. 193–225 (available at https://login.proxy.library.msstate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000252906300008&site=eds-live).

Chia, P. H., Yamamoto, Y., and Asokan, N. 2012. "Is this app safe?: A large scale study on application permissions and risk signals," in *Proceedings of the 21st International Conference on World Wide Web*, ACM, pp. 311–320.

Cho, J. 2006. "The mechanism of trust and distrust formation and their relational outcomes," *Journal of Retailing* (82:1), pp. 25–35.

Compeau, D. R., Marcolin, B., Kelley, H., and Higgins, C. 2012. "Research commentary—Generalizability of information systems research using student subjects—A reflection on our practices and recommendations for future research," *Information Systems Research* (23:4), pp. 1093–1109 (doi: 10.1287/isre.1120.0423).

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. 2007. "A video game for cyber security training and awareness," *Computers & Security* (26:1), pp. 63–72 (doi: 10.1016/j.cose.2006.10.005).

Cranor, L., Guduru, P., and Arjula, M. 2006. "User interfaces for privacy agents," *ACM Transactions on Computer-Human Interaction* (13:2), pp. 135–178 (doi: 10.1145/1165734.1165735).

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), Elsevier Ltd, pp. 90–101 (doi: 10.1016/j.cose.2012.09.010).

Csikszentmihalyi, M. 1975. "Play and intrinsic rewards," *Journal of Humanistic Psychology*, Sage Publications.

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

Culnan, M. J., and Armstrong, P. K. 1999. “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation,” *Organization Science* (10:1), INFORMS: Institute for Operations Research, pp. 104–115.

Degirmenci, K., Guhr, N., and Breitner, M. H. 2013. “Mobile applications and access to personal information: A discussion of users’ privacy concerns,” in *Thirty Fourth International Conference on Information Systems*, pp. 1–21.

DeVellis, R. F. 2012. “Guidelines in Scale Development,” in *Scale Development: Theory and Applications* (Third.), pp. 73–114.

Dienlin, T., and Trepte, S. 2015. “Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors,” *European Journal of Social Psychology* (45:3), John Wiley and Sons Ltd, pp. 285–297.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V., and Serra, I. 2005. “Internet Users ’ Privacy Concerns and Attitudes towards Government Surveillance – An Exploratory Study of Cross- Cultural Differences between Italy and the United States,” in *18th Bled eConference eIntegration in Action*, pp. 1–13.

Dinev, T., Bellotto, M., Hart, P., Russo, V., and Colautti, C. 2006. “Privacy calculus model in e-commerce – a study of Italy and the United States,” *European Journal of Information Systems* (December 2004), pp. 389–402 (doi: 10.1057/palgrave.ejis.3000590).

Dinev, T., and Hart, P. 2006. “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research* (17:1), pp. 61–80 (doi: 10.1287/isre.1060.0080).

Dinev, T., Hart, P., and Mullen, M. R. 2008. “Internet privacy concerns and beliefs about government surveillance – An empirical investigation,” *Strategic Information Systems* (17:3), pp. 214–233 (doi: 10.1016/j.jsis.2007.09.002).

Edwards, J. R., and Lambert, L. S. 2007. “Methods for integrating moderation and mediation: a general analytical framework using moderated path analysis.,” *Psychological methods* (12:1), pp. 1–22 (doi: 10.1037/1082-989X.12.1.1).

van Eerde, W., and Thierry, H. 1996. “Vroom’s expectancy models and work-related criteria: A meta-analysis.,” *Journal of Applied Psychology* (81:5), pp. 575–586 (available at http://psycnet.apa.org/journals/apl/81/5/575/).

Elenkov, N. 2014. *Android Security Internals: An In-Depth Guide to Android’s Security Architecture*, No Starch Press.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. 2014. "TaintDroid: an information flow tracking system for real-time privacy monitoring on smartphones," *ACM Transactions on Computer Systems* (32:2), pp. 1–29 (available at http://dl.acm.org/citation.cfm?id=2494522).

Featherman, M. S., Valacich, J. S., and Wells, J. D. 2006. "Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters," *Information Systems Journal* (16:2), Wiley Online Library, pp. 107–134.

Federal Trade Commission. 2012. "Protecting consumer privacy in an era of rapid change," *FTC Report*.

Federal Trade Commission. 2013a. "Mobile privacy disclosures: Building trust through transparency," *FTC Report*.

Federal Trade Commission. 2013b. "FTC staff report recommends ways to improve mobile privacy disclosures," *FTC Report*.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. 2011. "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, pp. 3–14.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. 2012. "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, p. 3.

Fornell, C., and Larcker, D. F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, JSTOR, pp. 39–50.

Fowler, G. A. 2015. "Windows 10 Isn't Spyware but It Wants Your Data," *Wall Street Journal Blog*.

Gates, C. S., Chen, J., Li, N., and Proctor, R. W. 2014. "Effective risk communication for Android apps," *Dependable and Secure Computing, IEEE Transactions on* (11:3), IEEE, pp. 252–265.

Gefen, D. 2000. "E-commerce: The role of familiarity and trust," *Omega* (28:6), Elsevier, pp. 725–737.

Gefen, D., Benbasat, I., and Pavlou, P. A. 2008. "A research agenda for trust in online environments," *Journal of Management Information Systems* (24:4), M.E. Sharpe Inc., pp. 275–286.

Gefen, D., Karahanna, E., and Straub, D. W. 2003. "Trust and TAM in online shopping: An integrated model," *MIS Quarterly* (27:1), MIS Quarterly & The Society for Information Management, pp. 51–90.

Gefen, D., Straub, D. W., and Boudreau, M.-C. 2000. “Structural equation modeling and regression: Guidelines for research practice,” *Communications of AIS* (4:August), pp. 1–79.

George, G., Haas, M. R., and Pentland, A. 2014. “Big data and management,” *Academy of Management Journal* (57:2), Academy of Management, pp. 321–326.

Gerlich, R. N., Drumheller, K., Babb, J., and De’Armond, D. 2015. “App consumption: An exploratory analysis of the uses & gratifications of mobile apps,” *Academy of Marketing Studies Journal* (19:1), Jordan Whitney Enterprises, Inc, p. 69.

Google, I. 2016. “Frequently Asked Questions about creating a Google Account,” (available at https://support.google.com/accounts/answer/1728595?hl=en; retrieved May 15, 2016).

Gulati, R., and Sytch, M. 2008. “Does familiarity breed trust? Revisiting the antecedents of trust,” *Managerial and Decision Economics* (29:2–3), Wiley Online Library, pp. 165–190.

Hadad, C. 2015. “#Being13: Inside the Secret World of Teens,” *CNN* (available at http://www.cnn.com/specials/us/being13; retrieved January 1, 2016).

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2010. *Multivariate Data Analysis* (7th ed.), Upper Saddle River, NJ: Prentice Hall.

Harbach, M., Hettig, M., Weber, S., and Smith, M. 2014. “Using personal examples to improve risk communication for security & privacy decisions,” in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, ACM, pp. 2647–2656.

Hayes, A. F. 2009. “Beyond Baron and Kenny: Statistical Mediation Analysis in the New Millennium,” *Communication Monographs* (76:4), pp. 408–420 (doi: 10.1080/03637750903310360).

van den Hoogen, S. 2009. “Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century,” *Dalhousie Journal of Interdisciplinary Management* (5:Spring).

Howe, N., and Strauss, W. 2009. *Millennials Rising: The Next Great Generation*, Random House LLC.

Jaeger, E. 2014. “Facebook Messenger: Eroding user privacy in order to collect, analyze, and sell your personal information,” *The John Marshall Journal of Computer & Information Law* (31:3), HeinOnline, p. i.

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

Jones, B. H., and Heinrichs, L. R. 2012. “Do business students practice smartphone security?,” *Journal of Computer Information Systems*, pp. 22–30.

Jung, J., Han, S., and Wetherall, D. 2012. “Short paper: enhancing mobile application permissions with runtime feedback and constraints,” in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, pp. 45–50.

Kacelnik, A., and Bateson, M. 1996. “Risky theories—the effects of variance on foraging decisions,” *American Zoologist* (36:4), The Oxford University Press, pp. 402–434.

Kane, S. Thurm. Y. I., and Thurm, S. 2010. “Your Apps Are Watching You,” *The Wall Street Journal* (available at http://www.wsj.com/articles/SB100014240527487043680045760277518670397 30).

Karahanna, E., Straub, D. W., and Chervany, N. L. 1999. “Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs,” *MIS Quarterly* (23:2), pp. 183–213.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. “Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus,” *Information Systems Journal*, Wiley Online Library.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. “Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior,” *International Journal of Human-Computer Studies* (71:12), Elsevier, pp. 1163–1173 (doi: 10.1016/j.ijhcs.2013.08.016).

Kelley, P. G., Cranor, L. F., and Sadeh, N. 2013. “Privacy as part of the app decision-making process,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 3393–3402.

Kim, J., and Park, J. 2005. “A consumer shopping channel extension model: attitude shift toward the online store,” *Journal of Fashion Marketing and Management: An International Journal* (9:1), Emerald Group Publishing Limited, pp. 106–121.

King, J. 2012. “How Come I’m Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations,” *Symposium on usable privacy and security (SOUPS)* (July), pp. 1–14.

Kirsch, L., and Boss, S. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines Information Privacy and Security," in *28th International Conference on Information Systems*.

Komiak, S. Y. X., and Benbasat, I. 2008. "A two-process view of trust and distrust building in recommendation agents: A process-tracing study," *Journal of the Association for Information Systems* (9:12), Association for Information Systems, pp. 727–747.

Kravets, D. 2016. "FBI paid 'grey hats' for zero-day exploit that unlocked seized iPhone," *Ars Technica (April 2016)*.

Kurkovsky, S., and Syta, E. 2010. "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security," in *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*, Citeseer, pp. 441–449.

Laibson, D. 1997. "Golden eggs and hyperbolic discounting," *The Quarterly Journal of Economics* (112:2), Oxford University Press, pp. 443–477.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues* (33:3), Wiley-Blackwell, pp. 22–42.

Lee, Y.-K., Chang, C.-T., Lin, Y., and Cheng, Z.-H. 2014. "The dark side of smartphone usage: Psychological traits, compulsive behavior and technostress," *Computers in Human Behavior* (31), Elsevier, pp. 373–383.

Lenhart, A., Smith, A., Anderson, M., Duggan, M., and Perrin, A. 2015. "Teens, technology and friendships: Videogames, social media and mobile phones play an integral role in how teens meet and interact with friends," *Pew Internet, Science, & Tech*.

Lewicki, R. J., McAllister, D. J., and Bies, R. J. 1998. "Trust and distrust: New relationships and realities," *Academy of Management Review* (23:3), Academy of Management, pp. 438–458 (available at 10.5465/AMR.1998.926620).

Li, H., Sarathy, R., and Xu, H. 2010. "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems* (2010), pp. 1–29.

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

Li, R., Li, W., Geng, S., and An, Y. 2014. "Measurement of Privacy Leakage Tolerance on the Mobile Internet.," in *PACIS*, p. 272.

Lichtblau, E., and Benner, K. 2016. "FBI Director Suggests Bill for iPhone Hacking Topped $1.3 Million," *The New York Times* (21).

Lin, Y.-H., Lin, Y.-C., Lee, Y.-H., Lin, P.-H., Lin, S.-H., Chang, L.-R., Tseng, H.-W., Yen, L.-Y., Yang, C. C. H., and Kuo, T. B. J. 2015. "Time distortion associated with smartphone addiction: Identifying smartphone addiction via a mobile application (App)," *Journal of Psychiatric Research* (65), Elsevier, pp. 139–145.

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

Luhmann, N. 1979. "Trust and power. 1979," *John Willey & Sons*.

Luhmann, N. 2000. "Familiarity, confidence, trust: Problems and alternatives," *Trust: Making and Breaking Cooperative Relations* (6), Citeseer, pp. 94–107.

Lutz, C., and Strathoff, P. 2014. "Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses," *SSRN Electronic Journal*.

Mackenzie, S. S. B., Podsakoff, P. M. P., and Podsakoff, N. N. P. 2011. "Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques," *MIS Quarterly* (35:2), pp. 293–334 (available at http://dl.acm.org/citation.cfm?id=2017510).

Madden, M., Lenhart, A., Cortesi, S., and Gasser, U. 2010. "Pew Internet and American life project," *Washington, DC, USA: Pew Research Center*.

Madden, M., and Rainie, L. 2015. "Americans' attitudes about privacy, security and surveillance," *Pew Research Center, May* (20).

Maier, S. F., and Seligman, M. E. 1976. "Learned helplessness: Theory and evidence.," *Journal of Experimental Psychology* (105:1), American Psychological Association, p. 3.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research* (15:4), pp. 336–355 (available at http://pubsonline.informs.org/doi/abs/10.1287/isre.1040.0032).

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research," *Management Science* (52:12), pp. 1865–1883.

Mansfield-Devine, S. 2012. “Paranoid Android: just how insecure is the most popular mobile platform?,” *Network Security* (2012:9), pp. 5–10 (doi: 10.1016/S1353-4858(12)70081-8).

Marin, R. S. 1990. “Differential diagnosis and classification of apathy,” *Am J Psychiatry* (147:1), Am Psychiatric Assoc, pp. 22–30.

Marsan, C. D. 2000. “‘Net privacy law: It’s only a matter of time,” *Network World*, p. 26.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. “Developing and validating trust measures for e-Commerce: An integrative typology,” *Information Systems Research* (13:3), pp. 334–359 (doi: 10.1287/isre.13.3.334.81).

McKnight, D. H., Kacmar, C. J., and Choudhury, V. 2004. “Dispositional trust and distrust distinctions in predicting high- and low-risk internet expert advice site perceptions,” *e-Service Journal* (3:2), United States, Indiana University Press, pp. 35–58 (doi: 10.1353/esj.2005.0004).

Miltgen, C. L., and Peyrat-Guillard, D. 2014. “Cultural and generational influences on privacy concerns: a qualitative study in seven European countries,” *European Journal of Information Systems* (23:2), Nature Publishing Group, pp. 103–125.

Mishra, S., and Lalumière, M. L. 2010. “You can’t always get what you want: The motivational effect of need on risk-sensitive decision-making,” *Journal of Experimental Social Psychology* (46:4), Elsevier, pp. 605–611.

Moloney, M., and Potì, V. 2013. “A Behavioral Perspective on the Privacy Calculus Model,” *Available at SSRN 2310535* (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2310535).

Mylonas, A., Meletiadis, V., Mitrou, L., and Gritzalis, D. 2013. “Smartphone sensor data as digital evidence,” *Computers & Security* (38), Elsevier, pp. 51–75.

Neisse, R., Geneiatakis, D., Steri, G., Kambourakis, G., Fovino, I. N., and Satta, R. 2016. “Dealing with User Privacy in Mobile Apps,” in *Protecting Mobile Networks and Devices: Challenges and Solutions*, CRC Press, p. 67.

Nicas, J. 2015. “Why your gadgets can now ‘See’ in 3-D,” *The Wall Street Journal*, pp. 1–5 (available at http://www.wsj.com/articles/more-devices-gain-3-d-vision-1444859629).

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. “The privacy paradox: Personal information disclosure intentions versus behaviors,” *Journal of Consumer Affairs* (41:1), pp. 100–126 (doi: 10.1111/j.1745-6606.2006.00070.x).

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric theory*McGraw-Hill series in psychology (3rd Reprin.), McGraw-Hill (available at http://books.google.com/books?id=r0fuAAAAMAAJ).

Pan, W., Aharony, N., and Pentland, A. 2011. "Composite social network for predicting mobile apps installation," *arXiv preprint arXiv:1106.0359*.

Paternoster, R., and Simpson, S. 1996. "Sanction threats and appeals to morality: Testing a rational choice model of corporate crime," *Law and Society Review* (30:3), pp. 549–583 (available at http://www.jstor.org/stable/10.2307/3054128).

Pavlou, P. A. 2002. "Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation," *The Journal of Strategic Information Systems* (11:3), Elsevier, pp. 215–243.

Perlroth, N., and Bilton, N. 2012. "Mobile apps take data without permission," *NY Times*.

Peter, J. P. 1981. "Construct Validity: A Review of Basic Issues and Marketing Practices," *Journal of Marketing Research* (18:2), pp. 133–145.

Peterson, C., Maier, S. F., and Seligman, M. E. P. 1995. *Learned Helplessness: A Theory for the Age of Personal Control*, Oxford University Press.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623–656.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing* (19:1), pp. 27–41 (doi: 10.1509/jppm.19.1.27.16941).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *The Journal of Applied Psychology* (88:5), pp. 879–903 (doi: 10.1037/0021-9010.88.5.879).

Podsakoff, P. M., MacKenzie, S. B., and Podsakoff, N. P. 2012. "Sources of method bias in social science research and recommendations on how to control it," *Annual Review of Psychology* (63), pp. 539–569 (doi: 10.1146/annurev-psych-120710-100452).

Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities," *European Journal of Information Systems* (19:2), Nature Publishing Group, pp. 181–195 (doi: 10.1057/ejis.2010.15).

Pötzsch, S. 2009. "Privacy awareness: A means to solve the privacy paradox?," in *The Future of Identity in the Information Society*, Springer, pp. 226–236.

Prensky, M. 2001. "Digital natives, digital immigrants Part 1," *On The Horizon* (9:5), MCB UP Ltd, pp. 1–6.

Purdy, K. 2012. "Can an Android Phone run without Google?," *IT World* (available at http://www.itworld.com/article/2832391/mobile/can-an-android-phone-run-without-google-.html; retrieved May 15, 2016).

Quinless, F. W., and Nelson, M. A. 1988. "Development of a Measure of Learned Helplessness," *Nursing Research* (37:1), pp. 11–15.

Raento, M., Oulasvirta, A., and Eagle, N. 2009. "Smartphones an emerging tool for social scientists," *Sociological Methods & Research* (37:3), Sage Publications, pp. 426–454.

Reinfelder, L., Benenson, Z., and Gassmann, F. 2014. "Differences between Android and iPhone users in their security and privacy awareness," in *Trust, Privacy, and Security in Digital Business*, Springer, pp. 156–167.

Salesforce.com. 2014. "Mobile Behavior Report," *Mobile Behavior Report*, pp. 1–36 (available at salesforce.com/marketingcloud; retrieved March 6, 2016).

Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., and Molloy, I. 2012. "Android permissions: a perspective combining risks and benefits," in *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, ACM, pp. 13–22.

Sawers, P. 2015. "Android Users Have an Average of 95 Apps Installed on their Phones, According to Yahoo Aviage Data," *The Next Web* (available at http://thenextweb.com/apps/2014/08/26/android-users-average-95-apps-installed-phones-according-yahoo-aviate-data/#gref; retrieved January 1, 2016).

Schreider, T. 2003. "Privacy Is in the Eye of the Beholder," *Information Systems Control Journal* (6), INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, pp. 46–48.

Schütz, P., and Friedewald, M. 2011. "Privacy: What are we actually talking about?," in *Privacy and Identity Management for Life*, Springer, pp. 1–14.

Seligman, M., and Maier, S. 1967. "Failure to escape traumatic shock.," *Journal of Experimental Psychology* (74:1), pp. 1–9 (available at http://psycnet.apa.org/journals/xge/74/1/1/).

Seneviratne, S., Seneviratne, A., Mohapatra, P., and Mahanti, A. 2014. "Predicting user traits from a snapshot of apps installed on a smartphone," *ACM SIGMOBILE Mobile Computing and Communications Review* (18:2), ACM, pp. 1–8.

Sharma, S., and Crossler, R. E. 2014. “Disclosing too much? Situational factors affecting information disclosure in social commerce environment,” *Electronic Commerce Research and Applications* (13:5), Elsevier B.V., pp. 305–319 (doi: 10.1016/j.elerap.2014.06.007).

Sheng, H., Nah, F. F.-H., and Siau, K. 2008. “An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns,” *Journal of the Association for Information Systems* (9:6), p. 15.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., and Borgthorsson, H. 2014. “Leakiness and creepiness in app space: Perceptions of privacy and mobile app use,” in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, ACM, pp. 2347–2356.

Siewiorek, D. 2012. “Generation smartphone,” *Spectrum, IEEE* (49:9), IEEE, pp. 54–58.

Simon, H. A. 1996. *The Sciences of the Artificial* (Vol. 136), MIT press.

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. 2006. “Concern for information privacy and online consumer purchasing,” *Journal of the Association for Information Systems* (7:6), Association for Information Systems, pp. 415–443.

Smith, A. 2015. “US Smartphone Use in 2015,” *Pew Research Center*, pp. 18–29.

Smith, H. J., Dinev, T., and Xu, H. 2011. “Information privacy research: An interdisciplinary review,” *MIS Quarterly* (35:4), pp. 989–1015.

Smith, H., Milberg, S., and Burke, S. 1996. “Information privacy: Measuring individuals’ concerns about organizational practices,” *MIS Quarterly* (June), pp. 167–197 (available at http://www.jstor.org/stable/10.2307/249477).

Solon, O. 2012. “How much data did Facebook have on one man? 1,200 pages of data in 57 categories,” *Wired Magazine* (available at http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook/viewall).

Solove, D. 2006. “A taxonomy of privacy,” *University of Pennsylvania Law Review* (477) (available at http://www.jstor.org/stable/40041279).

Solove, D. J. 2003. “The origins and growth of information privacy law,” *PLI/PAT* (748), p. 29.

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. “E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior,” in *Proceedings of the 3rd ACM conference on Electronic Commerce*, ACM, pp. 38–47.

Sprenger, P. 1999. “Sun on Privacy: ‘Get Over It,’” *Wired News* (26), pp. 1–99.

Statista. 2016. “Number of available applications in the Google Play Store from December 2009 to February 2016,” *The Statistics Portal* (available at http://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/; retrieved October 5, 2016).

Steenkamp, J.-B. E. M., and Baumgartner, H. 1998. “Assessing measurement invariance in cross-national consumer research,” *Journal of Consumer Research* (25:1), JSTOR, pp. 78–107.

Steenkamp, J.-B. E. M., and Baumgartner, H. 2000. “On the use of structural equation models for marketing modeling,” *International Journal of Research in Marketing* (17:2), Elsevier, pp. 195–202.

Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. 1983. “A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations.,” *Journal of Applied Psychology* (68:3), pp. 459–468 (doi: 10.1037//0021-9010.68.3.459).

Stone, E. F., and Stone, D. L. 1990. “Privacy in organizations: Theoretical issues, research findings, and protection mechanisms,” *Research in Personnel and Human Resources Management* (8:3), Greenwich, CT: JAI Press, pp. 349–411.

Straub, D. W., Boudreau, M., and Gefen, D. 2004. “Validation Guidelines for IS Positivist Research,” *Communications of the Association for Information Systems* (13:24), pp. 380–427.

Stuss, D. T., Van Reekum, R., and Murphy, K. J. 2000. “Differentiation of states and causes of apathy,” *The neuropsychology of emotion*, Oxford University Press New York, pp. 340–363.

Sutanto, J., Palme, E., and Tan, C. 2013. “Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users,” *MIS Quarterly* (37:4), pp. 1141–1164.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. 2011. “The effect of online privacy information on purchasing behavior: An experimental study,” *Information Systems Research* (22:2), INFORMS, pp. 254–268 (doi: 10.1287/isre.1090.0260).

Turow, J., Hennessy, M., and Draper, N. 2015. “The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation,” *The Annenberg School for Communication, University of Pennsylvania*.

U.S. Department of Commerce. 2016. “Quarterly Retail E-Commerce Sales 4th Quarter 2015,” Washington, D.C. (available at https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf).

Vijayan, J. 2013. “Flashlight app vendor settles with FTC over privacy violations,” *Computerworld* (available at http://www.computerworld.com/article/2486577/application-security/flashlight-app-vendor-settles-with-ftc-over-privacy-violations.html).

Vroom, V. H. 1964. *Work and Motivation*, Oxford, England: Wiley.

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. “Continuance of protective security behavior: A longitudinal study,” *Decision Support Systems* (92), Elsevier, pp. 25–35.

Warkentin, M., Johnston, A. C., and Shropshire, J. D. 2011. “The influence of the informal social learning environment on information privacy policy compliance efficacy and intention,” *European Journal of Information Systems* (20:3), Nature Publishing Group, pp. 267–284 (doi: 10.1057/ejis.2010.72).

Warkentin, M., Shropshire, J., and Johnston, A. 2006. “Why Do We ‘Check the Box’?--A Study of Security Action Automation and Capitulation,” in *Proceedings of the 2006 ISOneWorld Security Conference*, Las Vegas (available at http://www.isy.vcu.edu/~gdhillon/Old2/secconf/pdfs/53.pdf).

Warkentin, M., Straub, D., and Malimage, K. 2012. “Featured Talk : Measuring Secure Behavior : A Research Commentary,” in *Annual Symposium on Information Assurance & Secure Knowledge Management*, Albany, pp. 1–8.

Warren, S., and Brandeis, L. 1890. “The Right to Privacy,” *Harvard Law Review* (4:5), pp. 193–220 (available at http://www.jstor.org/stable/1321160).

Webster, T. 2014. “2014 Smartphone Ownership Demographics - Edison Research,” *Edison Research*.

Weichselbaum, L., Neugschwandtner, M., Lindorfer, M., Fratantonio, Y., van der Veen, V., and Platzer, C. 2014. “Andrubis: Android malware under the magnifying glass,” *Vienna University of Technology, Tech. Rep. TRISECLAB-0414* (1).

Weissman, C. G. 2015. “Here’s how health app could expose all sorts of new information about you,” *Business Insider* (available at http://www.businessinsider.com/health-app-data-tracking-2015-4; retrieved October 5, 2016).

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. 1967. *Privacy and Freedom*, New York: Ig Publishing.

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K. 2015. "Android permissions remystified: a field study on contextual integrity," in *24th USENIX Security Symposium (USENIX Security 15)*, pp. 499–514.

Wilson, D., and Valacich, J. S. 2012. "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus," in *Thirty Third International Conference on Information Systems*.

Wittes, B., and Liu, J. C. 2015. "The Privacy Paradox: The Privacy Benefits of Privacy Threats," The Bookings Institution, pp. 1–21.

Xu, H., Gupta, S., Rosson, M. B., and Carroll, J. M. 2012. "Measuring mobile users' concerns for information privacy," *Thirty Third International Conference on Information Systems* (Ftc 2009), pp. 1–16 (available at http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10/).

Xu, H., Luo, X. (Robert), Carroll, J. M., and Rosson, M. B. 2011. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems* (51:1), pp. 42–52 (doi: 10.1016/j.dss.2010.11.017).

Xu, H., Teo, H.-H., Tan, B. C. Y., and 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), pp. 135–174 (doi: 10.2753/MIS0742-1222260305).

Yadin, A. 2012. "Millennials and Privacy in the Information Age: Can They Coexist?," *IEEE TECHNOLOGY AND SOCIETY MAGAZINE* (December) (available at http://146.163.150.3/~wwhite/IS376/Readings/08_MillenialsAndPrivacyInInfoAge.pdf).

Yoo, C. W., Ahn, H. J., and Rao, H. R. 2012. "An exploration of the impact of information privacy invasion," in *Thirty Third International Conference on Information Systems*, pp. 1–18.

Yu, A. 2014. "Weekly Innovation: A Radiation Detector In Your Smartphone," *NPR* (available at http://www.npr.org/sections/alltechconsidered/2014/01/17/263369742/weekly-innovation-a-radiation-detector-in-your-smartphone; retrieved December 5, 2016).

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

Zhu, H., Xiong, H., Ge, Y., and Chen, E. 2014. "Mobile app recommendations with security and privacy awareness," in *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM, pp. 951–960.

APPENDIX A

SURVEY INSTRUMENT

The survey for this dissertation was taken only on Android-based mobile devices. It has been exported below.

DeviceTest Browser Meta Info

Browser (1)

Version (2)

Operating System (3)

Screen Resolution (4)

Flash Version (5)

Java Support (6)

User Agent (7)

WrongDevice Thank you for your interest in taking this survey about Android applications. As stated in the description of this survey, participants must complete this survey on an Android-powered device. If you are interested in participating in this survey, please re-launch the survey using your Android device. If you are using an Android device, the survey did not properly recognize your device.--- End of Survey ---

Q59 Before the survey begins, please verify that the ID in the field below is your correct Amazon Mechanical Turk ID. If is your ID, please click Next. If this is not your ID, of if no ID is displayed, please enter your ID and click Next.

DeviceInfo Browser Meta Info

Browser (1)

Version (2)

Operating System (3)

Screen Resolution (4)

Flash Version (5)

Java Support (6)

User Agent (7)

Consent Hello and thank you for taking the time to read this page. I am a doctoral student from Mississippi State University. I invite you to participate in my research study evaluating specific Android applications. You are eligible to take part in this study because you are at least 18 years of age and have personal information on a smartphone using the Android operating system. Only specific versions of the Android operating system are desired for this study. You must be able to locate the version of your operating system (e.g., go to Settings --> About Phone --> Android Version). One of the tasks of this study is to install a Free (no ads) Android app (called the BTS App Listing Utility) and paste a list of apps and their permissions into this survey. The BTS App Listing Utility: * Does NOT require or request ANY sensitive permissions to information or features on your device.* Does NOT collect any personal information about you. * Does NOT attempt to uniquely identify you in any way--your responses are anonymous. * Only information about the applications installed on your device are gathered. * None of your personal data associated with any application are collected. * All of your personal information remains on your device. The app does not have permission to access your personal data. * Information used in this study is only used in aggregate for statistical analysis. If you decide to participate in this study, you will be asked to complete an anonymous survey to provide feedback about specific Android applications. The time to complete the survey is approximately 12 minutes. You will NOT be asked to share embarrassing or sensitive information nor will any identifying information be required or retained. Your participation is voluntary and you may quit at any time without penalty. There is no known risk for participating in this study. Your participation will help increase our understanding of Android users' opinions about weather applications. If you do not wish to participate, simply close the browser. Thank you in advance for your participation, Gregory J. Bott PhD Student Mississippi State University

18yo I am at least 18 years of age and I voluntarily agree to participate.

- ❍ Yes (1)
- ❍ No (2)

PersonalInfo Please select the item that best describes your Android personal mobile device.

- ❍ I do NOT store personal information on my Android device. (1)
- ❍ My Android contains information that is personal to me. (2)

LengthUsage How long have you been using an Android smartphone?

- Less than 6 months (1)
- Between 6 months and 1 year (2)
- Between 1 and 2 years (3)
- Between 2 and 3 years (4)
- More than three years (5)

Expert How would you rate your knowledge of how to configure your smartphone?

- Extremely knowledgeable (1)
- Very knowledgeable (2)
- Moderately knowledgeable (3)
- Slightly knowledgeable (4)
- Not knowledgeable at all (5)

NotPersonal You indicated that you do not have information on your Android mobile device that you consider personal. As stated in the requirements, you must have personal information on your phone to participate in this survey. Thank you for your interest.

Not18 You indicated that you are younger than 18 years old. As stated in the survey requirements, you must be 18 or older to participate in this survey. Thank you for your interest.

AndrVer Please indicate the version of your Android operating system. To find the version of the operating system in use on your device, go to Settings --> About phone -->

Android version. A number should be displayed (e.g., 4.1.1, 6.0.1, etc.). What is the first number displayed?

- ❍ 2.x (1)
- ❍ 3.x (2)
- ❍ 4.x (3)
- ❍ 5.x (4)
- ❍ 6.x (5)
- ❍ 7.x (7)
- ❍ Other or I don't know (6)

InstallSuccess

To save time and effort required to list applications and their permissions, please download and install the BTS App List Utility and follow the instructions on the app screen.

The only purpose of this app is to create a file listing the apps on your phone and the permissions granted to those apps.

Absolutely no personal or identifying information is collected. Your responses will remain anonymous.

This application requires NO SPECIAL PERMISSIONS and does NOT have access to your personal information.

The data is in plain text (formatted for a database) and accessible to confirm that only app information (not your personal data) is generated.

Please tap the graphic below to install BTS App List Utility.

Download on Google play

- ○ I successfully installed the BTS App List Utility.
- ○ I did not install the BTS App List Utility.

Data1 After starting the application, tap COPY LIST OF APPS, and then you will see a message stating "Data copied to Clipboard." Please long press within the text box below to paste information from your Android mobile device into the text box: (please be patient...this may take a minute or so)

Paste1Success Were you able to paste the required information into the text box in the previous question?

❍ I successfully pasted the generated information. (1)
❍ I was not able to paste the information. (2)

NamePrimary What is the name of your primary weather app?

AlreadyInstalled Which of the following apps are already installed on your Android device? (select one or more, or the none option)

❑ AccuWeather (1)
❑ Local Weather (by Matto) (2)
❑ The Weather Channel (3)
❑ Weather (MacroPinch) (4)
❑ Weather Underground (5)
❑ Yahoo Weather (6)
❑ None of these are installed (7)

PercNeed Considering only the primary weather app you use, indicate your level of agreement or disagreement with the following questions.

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
If all my apps were suddenly	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
gone (e.g., new phone or factory reset), my weather app would be among the very first apps I would reinstall. (1)							
I use my weather app every day (2)	❍	❍	❍	❍	❍	❍	❍
My weather app is extremely important to me (3)	❍	❍	❍	❍	❍	❍	❍
It is extremely important to me that I receive severe weather alerts from my weather app (4)	❍	❍	❍	❍	❍	❍	❍
Knowing the weather forecast is	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
very important to me (5)							
My weather app is very easy to use (6)	❍	❍	❍	❍	❍	❍	❍
My weather app has all the features I need (7)	❍	❍	❍	❍	❍	❍	❍
My weather app is located in the best location for access (e.g., on the bottom row that appears on every screen) (8)	❍	❍	❍	❍	❍	❍	❍

Familiarity Please indicate your level of FAMILIARITY with each of the following applications.

	Extremely familiar (1)	Very familiar (2)	Moderately familiar (3)	Slightly familiar (4)	Not familiar at all (5)
Image:Accuweather (1)	❍	❍	❍	❍	❍
Image:Localweather (2)	❍	❍	❍	❍	❍
Image:Twc (3)	❍	❍	❍	❍	❍
Image:Weather MacroPinch (4)	❍	❍	❍	❍	❍
Image:Weather Underground (5)	❍	❍	❍	❍	❍
Image:Yahoo Weather (6)	❍	❍	❍	❍	❍

DescrFeatures Below are feature of each app to help you decide which application(s) you would like to install, uninstall, keep, or ignore.

AccuWeather
Accuweather.com

- Avg. Review 4.3 (> 1.5 million reviews)
- MinuteCast - minute-by-minute precipitation forecasts localized to your exact GPS location
- Worldwide snow, ice, rain, wind, and probability of thunderstorm forecasts
- US severe weather alerts
- Radar for North America and Europe overlaid on Google Maps
- Current news and weather videos (English and Spanish)
- 15-day forecast
- Sunrise and sunset times

Local weather
matto

- Avg. Review: 3.9 (>5,800 reviews)
- Overview daily forecast for next week
- Hourly forecast (graphic, temp, wind direct
- Bookmark cities from the USA and around the world

The Weather Chann
The Weather Channel

- Avg. Review 4.3 (> 1.4 million reviews)
- Dynamic home screen (uses your current location)
- Hourly, 15-day and weekend forecast
- "feels like" weather, humidity, dew point, sunrise, sunset, wind speed, UV index, visibility, barometric pressure
- Severe and Breaking Weather Alerts
- Lightning Alerts based on your GPS location
- Pollen, Rain, and Snow alerts
- Social Weather (upload pictures to report weather)
- Weather widgets

Weather Undergrou
Weather Underground

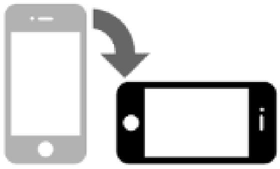
- Avg. Review: 4.5 (> 198,000 reviews)
- Hyper-local weather forecasts
- Weather station support
- Current weather in any location worldwide
- Crowd reporting
- Hour-by-Hour weather forecasts
- 10-day weather forecasts
- Sunrise/sunset
- Precipitation forecasts: probability, quantity, and duration

Yahoo Weather
Yahoo

- Avg. Review: 4.4 (> 1.1 million reviews)
- Animated sunrise, sunset, wind, and pressure modules
- Hour-by-Hour weather forecasts
- Add up to 20 cities
- 5-day and 10-day weather forecasts
- Precipitation forecasts: probability, quantity, and duration
- Weather radar for any location: rainfall radar, plus cloud, thunderstorm, snow and temperatures
- Social: share weather photos, optional link to Flickr

DescrPerms

This page is best viewed landscape:



Below is a table of permissions required by the six weather applications for review:

YES = App requires this permission
No = App does not require this permission
* Only sensitive permissions are displayed. Total permissions do not equal number of "Yes" boxes.

Android Permission	Accuweather	Local Weather (by matto)	The Weather Channel	Weather (Macro Pinch)	Weather Underground	Yahoo
Device & App History - retrieve running apps	No	No	No	No	No	Yes
Identity - find accounts	Yes	No	Yes	No	No	Yes
Identity - add/remove accounts	No	No	No	No	No	Yes
Contacts - find accounts	Yes	No	Yes	No	No	Yes
Location - approximate	Yes	No	Yes	No	Yes	Yes
Location - precise	Yes	No	Yes	Yes	Yes	Yes
Phone - read status and identity	Yes	No	Yes	No	No	No
Photos/Media/Files - modify	Yes	No	Yes	No	Yes	Yes
Photos/Media/Files - read	Yes	No	Yes	No	Yes	Yes
Storage - read	Yes	No	Yes	No	Yes	Yes
Storage - modify/delete	Yes	No	Yes	No	Yes	Yes
Wi-Fi connection information	No	No	Yes	No	No	Yes
Device ID and Call Info - read phone status	Yes	No	No	No	No	No
Other - use accounts on the device	No	No	Yes	No	No	Yes
Total Permissions Requested	16	2	18	5	12	22
	Accuweather	Local Weather (by matto)	The Weather Channel	Weather (Macro Pinch)	Weather Underground	Yahoo

PlsInstall After having reviewed each application, you are encouraged to select the best option and actually install it on your Android device so that you can review it firsthand. Conversely, if new information leads you to no longer desire an application you have on your device, you are encouraged to actually uninstall it. You are NOT required to install or uninstall any weather application if you do not wish to do so.

Disclosure Please indicate the action you took for each application. I decided to _________ this application.

	Install (1)	Keep (2)	Ignore (3)	Uninstall (4)
AccuWeather (1)	❍	❍	❍	❍
Local Weather (by matto) (2)	❍	❍	❍	❍
The Weather Channel (3)	❍	❍	❍	❍
Weather (MacroPinch) (4)	❍	❍	❍	❍
Weather Underground (5)	❍	❍	❍	❍
Yahoo Weather (6)	❍	❍	❍	❍

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. AccuWeather - Install Is Selected

WhyInstallAccu Describe the primary reason(s) you installed AccuWeather:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Local Weather (by Matto) - Install Is Selected

WhyInstallLW Describe the primary reason(s) you installed Local weather (by matto):

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. The Weather Channel - Install Is Selected

WhyInstallTWC Describe the primary reason(s) you installed The Weather Channel:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Weather and Radar - Install Is Selected

WhyInstWMPinch Describe the primary reason(s) you installed Weather (MacroPinch):

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Weather Underground - Install Is Selected

WhyInstWU Describe the primary reason(s) you installed Weather Underground:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Yahoo Weather - Install Is Selected

WhyInstYW Describe the primary reason(s) you installed Yahoo Weather:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. AccuWeather - Ignore Is Selected

Or Please indicate the action you took for each application. I decided to _________ this application. AccuWeather - Uninstall Is Selected

NotInstAccu Please indicate the primary reason for ignoring (not installing) or uninstalling AccuWeather:

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it. (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed. (4)
- ❍ A reason not listed here. (5)

Display This Question:

If Please indicate the primary reason for ignoring (not installing) or uninstalling AccuWeather: A reason not listed here. Is Selected

NotInstAccEssay Please describe your reason for ignoring or uninstalling AccuWeather:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Local Weather (by matto) - Ignore Is Selected

Or Please indicate the action you took for each application. I decided to _________ this application. Local Weather (by matto) - Uninstall Is Selected

NotInstLW Please indicate the primary reason for ignoring (not installing) or uninstalling Local Weather (by matto):

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed (4)
- ❍ A reason not listed here. (5)

Display This Question:
If Please indicate the primary reason for ignoring (not installing) or uninstalling Local Weather (b... A reason not listed here. Is Selected

NotInstLWEssay Please describe your reason for ignoring or uninstalling Local Weather (by matto):

Display This Question:
If Please indicate the action you took for each application. I decided to _________ this application. The Weather Channel - Ignore Is Selected
Or Please indicate the action you took for each application. I decided to _________ this application. The Weather Channel - Uninstall Is Selected

NotInstTWC Please indicate the primary reason for not installing or uninstalling The Weather Channel:

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it. (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed. (4)
- ❍ A reason not listed here. (5)

Display This Question:
If Please indicate the primary reason for not installing or uninstalling The Weather Channel: A reason not listed here. Is Selected

NotInstTWCEssay Please describe your reason for ignoring or uninstalling The Weather Channel:

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Weather and Radar - Ignore Is Selected

Or Please indicate the action you took for each application. I decided to _________ this application. Weather and Radar - Uninstall Is Selected

NotInstWMP Please indicate the primary reason for not installing or uninstalling Weather (MacroPinch):

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it. (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed. (4)
- ❍ A reason not listed here. (5)

Display This Question:

If Please indicate the primary reason for not installing or uninstalling Weather and Radar (by WetterOnline): A reason not listed here. Is Selected

NotInstWMPEssay Please describe your reason for ignoring or uninstalling Weather (MacroPinch):

Display This Question:

If Please indicate the action you took for each application. I decided to _________ this application. Weather Underground - Ignore Is Selected

Or Please indicate the action you took for each application. I decided to _________ this application. Weather Underground - Uninstall Is Selected

UninReasonWU Please indicate the primary reason for not installing or uninstalling Weather Underground:

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it. (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed. (4)
- ❍ A reason not listed here. (5)

Display This Question:
If Please indicate the primary reason for not installing or uninstalling Weather (Macropinch): A reason not listed here. Is Selected

NotInstWUEssay Please describe your reason for ignoring or uninstalling Weather Underground.

Display This Question:
If Please indicate the action you took for each application. I decided to _________ this application. Yahoo Weather - Ignore Is Selected
Or Please indicate the action you took for each application. I decided to _________ this application. Yahoo Weather - Uninstall Is Selected

NotInstYW Please indicate the primary reason for not installing or uninstalling Yahoo Weather:

- ❍ Incomplete or lacking feature set (1)
- ❍ I have no use for it. (2)
- ❍ I am uncomfortable with the app permissions requested (3)
- ❍ Redundant with app(s) already installed. (4)
- ❍ A reason not listed here. (5)

Display This Question:
If Please indicate the primary reason for not installing or uninstalling Weather (Macropinch): A reason not listed here. Is Selected

NotInstYWEssay Please describe your reason for ignoring or uninstalling Yahoo Weather.

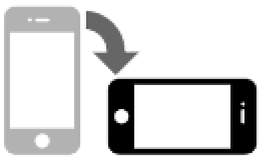
Paste2 For the second time, please navigate to to the BTS App Listing Utility, tap Back, tap the Copy App List button and then long-press inside the box below, and tap Paste to paste the list of applications.

DescPermissions

Android apps only have access to the personal information granted by user permissions.

Below is a table of those permissions. Please reference this table to answer the following questions.

This page is best viewed landscape:



YES = App requires this permission
No = App does not require this permission
* Only sensitive permissions are displayed. Total permissions do not equal number of "Yes" boxes.

Android Permission	Accuweather	Local Weather (by matto)	The Weather Channel	Weather (Macro Pinch)	Weather Underground	Yahoo
Device & App History - retrieve running apps	No	No	No	No	No	Yes
Identity - find accounts	Yes	No	Yes	No	No	Yes
Identity - add/remove accounts	No	No	No	No	No	Yes
Contacts - find accounts	Yes	No	Yes	No	No	Yes
Location - approximate	Yes	No	Yes	No	Yes	Yes
Location - precise	Yes	No	Yes	Yes	Yes	Yes
Phone - read status and identity	Yes	No	Yes	No	No	No
Photos/Media/Files - modify	Yes	No	Yes	No	Yes	Yes
Photos/Media/Files - read	Yes	No	Yes	No	Yes	Yes
Storage - read	Yes	No	Yes	No	Yes	Yes
Storage - modify/delete	Yes	No	Yes	No	Yes	Yes
Wi-Fi connection information	No	No	Yes	No	No	Yes
Device ID and Call Info - read phone status	Yes	No	No	No	No	No
Other - use accounts on the device	No	No	Yes	No	No	Yes
Total Permissions Requested	16	2	18	5	12	22

Accuweather | Local Weather (by matto) | The Weather Channel | Weather (Macro Pinch) | Weather Underground | Yahoo

DisAccu

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

DisLW

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

DisTWC

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

DisWeather

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

DisWU

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

DisYahoo

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
This app developer (or organization) will exploit customers' personal information given the chance. (1)	❍	❍	❍	❍	❍	❍	❍
This app developer will engage in damaging and harmful behavior to mobile users to pursue its own interest. (2)	❍	❍	❍	❍	❍	❍	❍
This app developer creates apps that collect information in deceptive manner. (3)	❍	❍	❍	❍	❍	❍	❍

Resignation In the context of your personal information stored on your mobile device, please answer the following questions:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
No matter how much effort I put into protecting my mobile privacy, I feel I have no control over the outcome. (1)	❍	❍	❍	❍	❍	❍	❍
Other organizations have more control over my personal information than I do. (2)	❍	❍	❍	❍	❍	❍	❍
I feel that I have little control over the outcomes of protecting my personal information. (3)	❍	❍	❍	❍	❍	❍	❍
Many organizations already have more information about me than I want them to have. (4)	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
It is wasted effort to protect my privacy. (5)	❍	❍	❍	❍	❍	❍	❍

IPA In the context of your personal information stored on your mobile device, please answer the following questions:

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I have little interest in privacy issues when installing an app from the Google Play store. (1)	❍	❍	❍	❍	❍	❍	❍
I care less about information privacy while downloading an app from the Google Play store. (2)	❍	❍	❍	❍	❍	❍	❍
I do not worry about privacy issues while downloading	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
an app on the Google Play store. (3)							
When I download an app from the Google Play store, I pay almost no attention to the permissions information. (5)	❍	❍	❍	❍	❍	❍	❍

PrivAware While considering the applications on your smartphone, please answer the following questions.

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I have often decided NOT to install an app because of the permissions required. (1)	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
I can list the companies and entities that have access to my personal information on my mobile device. (2)	❍	❍	❍	❍	❍	❍	❍
I know what personal information others have received from my mobile device. (3)	❍	❍	❍	❍	❍	❍	❍
I have a good idea how personal information from my mobile device is being used now and in the future. (4)	❍	❍	❍	❍	❍	❍	❍
I have a good idea of how much personal information from my mobile device has been collected or	❍	❍	❍	❍	❍	❍	❍

	Strongly agree (1)	Agree (2)	Somewhat agree (3)	Neither agree nor disagree (4)	Somewhat disagree (5)	Disagree (6)	Strongly disagree (7)
transmitted to others. (5)							
My peers would turn to me if they had questions regarding permissions about apps downloaded from the Google Play store. (6)	❍	❍	❍	❍	❍	❍	❍

OveralExp My overall experience with weather apps has been positive.

- ❍ Strongly agree (1)
- ❍ Agree (2)
- ❍ Somewhat agree (3)
- ❍ Neither agree nor disagree (4)
- ❍ Somewhat disagree (5)
- ❍ Disagree (6)
- ❍ Strongly disagree (7)

Gender What is your gender?

- ❍ Male (0)
- ❍ Female (1)

Race What is your race or origin?

- ❍ Black/African American (1)
- ❍ Hispanic, Latino or Spanish origin (2)
- ❍ American Indian or Alaska Native (3)
- ❍ White (4)
- ❍ Asian (5)
- ❍ Native Hawaiian or Other Pacific Islander (6)
- ❍ Some other race or origin (7)

BirthYr What is your birth year (use four digits to indicate the year - YYYY)?

LevelEduc What is the highest level of education you have completed?

- ❍ Some high School (1)
- ❍ High School graduate (or equivalent) (2)
- ❍ Some College, but less than 1 year (3)
- ❍ 1 or more years of college, but not Bachelor's degree (4)
- ❍ Bachelor's degree (5)
- ❍ Master’s degree (or other post-graduate Professional degree) (6)
- ❍ Doctoral Degree (7)

NumApps Approximately how many apps have you downloaded onto your phone?

- ❍ 0-5 (1)
- ❍ 6-15 (2)
- ❍ 16-25 (3)
- ❍ 26-36 (4)
- ❍ 36-45 (5)
- ❍ 46-55 (6)
- ❍ 56-65 (7)
- ❍ 66-75 (8)
- ❍ 76-85 (9)
- ❍ 86-99 (3)
- ❍ 100+ (11)

YrsFTE How many years of post-education, full-time employment do you have?

- 0 (1)
- Less than 1 year (2)
- 1 to 5 years (3)
- 5 to 10 years (4)
- 10 to 20 years (5)
- More than 20 years (6)

APPENDIX B

DETAILED ANALYSES OF MEASURED CONTROL VARIABLES

Measured control variables were evaluated for each app. Only year of birth (BirthYr) and privacy awareness (Priv_Aware) displayed significant relationships across all models. Only these two control variables were included in the subsequent model analysis.

Table 34 Control Variable Analysis for AccuWeather App Model

			Estimate	S.E.	C.R.	P
Distrust	<---	BirthYr	-0.057	0.006	-1.427	0.154
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.583**	***
Distrust	<---	Gender	0.03	0.113	0.74	0.46
IPA	<---	Gender	-0.054	0.11	-1.362	0.173
Distrust	<---	Expert	-0.04	0.063	-0.962	0.336
IPA	<---	Expert	0.078	0.062	1.907	0.056
Distrust	<---	LevelEduc	0.024	0.046	0.599	0.549
IPA	<---	LevelEduc	-0.043	0.046	-1.076	0.282
Distrust	<---	Priv_Aware	0.037	0.062	0.86	0.39
IPA	**<---**	**Priv_Aware**	**0.143**	**0.063**	**3.228**	**0.001**
Disc1Accu	<---	Gender	-0.039	0.052	-1.112	0.266
Disc1Accu	**<---**	**Expert**	**0.073**	**0.029**	**1.983**	**0.047**
Disc1Accu	<---	LevelEduc	0.042	0.021	1.198	0.231
Disc1Accu	<---	Priv_Aware	-0.04	0.029	-1.017	0.309

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent

Table 35 Control Variable Analysis for Local Weather App Model

			Estimate	S.E.	C.R.	P
Distrust	**<---**	**BirthYr**	**-0.09**	**0.006**	**-2.308**	**0.021**
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.582**	*****
Distrust	<---	Gender	-0.016	0.101	-0.416	0.678
IPA	<---	Gender	-0.054	0.11	-1.361	0.173
Distrust	<---	Expert	0.015	0.057	0.373	0.709
IPA	<---	Expert	0.078	0.063	1.908	0.056
Distrust	<---	LevelEduc	0.003	0.042	0.08	0.937
IPA	<---	LevelEduc	-0.043	0.046	-1.075	0.283
Distrust	**<---**	**Priv_Aware**	**-0.159**	**0.057**	**-3.654**	*****
IPA	**<---**	**Priv_Aware**	**0.142**	**0.062**	**3.208**	**0.001**
Disc2LW	<---	Gender	0.023	0.054	0.596	0.551
Disc2LW	<---	Expert	-0.051	0.031	-1.271	0.204
Disc2LW	<---	LevelEduc	-0.017	0.022	-0.447	0.655
Disc2LW	<---	Priv_Aware	0.054	0.031	1.221	0.222

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent; Priv_Aware = Privacy Awareness

Table 36 Control Variable Analysis for The Weather Channel App Model

			Estimate	S.E.	C.R.	P
Distrust	<---	BirthYr	-0.054	0.007	-1.349	0.177
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.585**	*****
Distrust	<---	Gender	0.016	0.122	0.396	0.692
IPA	<---	Gender	-0.054	0.11	-1.364	0.173
Distrust	<---	Expert	-0.025	0.069	-0.59	0.555
IPA	<---	Expert	0.078	0.062	1.902	0.057
Distrust	<---	LevelEduc	0.053	0.05	1.312	0.19
IPA	<---	LevelEduc	-0.043	0.046	-1.081	0.28
Distrust	<---	Priv_Aware	0.013	0.067	0.308	0.758
IPA	**<---**	**Priv_Aware**	**0.144**	**0.063**	**3.256**	**0.001**
Disc3TWC	<---	Gender	-0.035	0.055	-0.942	0.346
Disc3TWC	<---	Expert	0	0.031	0.009	0.993
Disc3TWC	<---	LevelEduc	-0.047	0.023	-1.286	0.198
Disc3TWC	<---	Priv_Aware	-0.039	0.031	-0.945	0.345

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent; Priv_Aware = Privacy Awareness

Table 37 Control Variable Analysis for The Weather Underground App Model

			Estimate	S.E.	C.R.	P
Distrust	<---	BirthYr	-0.071	0.006	-1.782	0.075
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.584**	***
Distrust	<---	Gender	-0.009	0.105	-0.232	0.817
IPA	<---	Gender	-0.054	0.11	-1.364	0.173
Distrust	<---	Expert	0.039	0.06	0.925	0.355
IPA	<---	Expert	0.078	0.062	1.903	0.057
Distrust	<---	LevelEduc	-0.021	0.043	-0.53	0.596
IPA	<---	LevelEduc	-0.043	0.046	-1.08	0.28
Distrust	<---	Priv_Aware	-0.033	0.057	-0.764	0.445
IPA	**<---**	**Priv_Aware**	**0.144**	**0.063**	**3.249**	**0.001**
Disc5WU	<---	Gender	-0.01	0.05	-0.27	0.787
Disc5WU	<---	Expert	-0.012	0.028	-0.305	0.761
Disc5WU	<---	LevelEduc	-0.01	0.02	-0.278	0.781
Disc5WU	<---	Priv_Aware	0.021	0.028	0.534	0.594

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent; Priv_Aware = Privacy Awareness

Table 38 Control Variable Analysis for The Weather by Macro Pinch App Model

			Estimate	S.E.	C.R.	P
Distrust	**<---**	**BirthYr**	**-0.14**	**0.006**	**-3.535**	***
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.584**	***
Distrust	<---	Gender	-0.044	0.1	-1.142	0.253
IPA	<---	Gender	-0.054	0.11	-1.364	0.173
Distrust	<---	Expert	0.023	0.056	0.562	0.574
IPA	<---	Expert	0.078	0.062	1.9	0.057
Distrust	<---	LevelEduc	-0.002	0.041	-0.039	0.969
IPA	<---	LevelEduc	-0.043	0.046	-1.079	0.28
Distrust	**<---**	**Priv_Aware**	**-0.164**	**0.056**	**-3.808**	***
IPA	**<---**	**Priv_Aware**	**0.144**	**0.062**	**3.25**	**0.001**
Disc4WMP	<---	Gender	0.035	0.047	0.911	0.362
Disc4WMP	<---	Expert	0.019	0.027	0.466	0.641
Disc4WMP	**<---**	**LevelEduc**	**0.089**	**0.019**	**2.346**	**0.019**
Disc4WMP	<---	Priv_Aware	0.02	0.027	0.466	0.641

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent; Priv_Aware = Privacy Awareness

Table 39 Control Variable Analysis for The Yahoo! Weather App Model

			Estimate	S.E.	C.R.	P
Distrust	<---	BirthYr	-0.076	0.007	-1.908	0.056
IPA	**<---**	**BirthYr**	**0.183**	**0.006**	**4.584**	***
Distrust	<---	Gender	0.011	0.133	0.283	0.777
IPA	<---	Gender	-0.054	0.11	-1.362	0.173
Distrust	<---	Expert	-0.046	0.076	-1.128	0.259
IPA	<---	Expert	0.079	0.062	1.91	0.056
Distrust	<---	LevelEduc	0.042	0.055	1.057	0.291
IPA	<---	LevelEduc	-0.043	0.046	-1.078	0.281
Distrust	**<---**	**Priv_Aware**	**0.092**	**0.075**	**2.121**	**0.034**
IPA	**<---**	**Priv_Aware**	**0.143**	**0.063**	**3.232**	**0.001**
Disc6Yahoo	<---	Gender	-0.001	0.035	-0.019	0.985
Disc6Yahoo	<---	Expert	0.016	0.02	0.406	0.684
Disc6Yahoo	<---	LevelEduc	-0.011	0.014	-0.286	0.775
Disc6Yahoo	<---	Priv_Aware	-0.019	0.02	-0.433	0.665

BirthYr = year respondent was born; LevelEduc = highest level of education attained by the respondent; Priv_Aware = Privacy Awareness

APPENDIX C

PATH ANALYSIS OF INDIVIDUAL APPS

Table 40 AccuWeather Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.251	-6.446	***	**Yes**
H2: PercNeed --> Disclosure (+)	0.114	2.908	0.004	**Yes**
H4: Familiarity --> Distrust (-)	-0.150	-3.781	***	**Yes**
H5: Familiarity --> Disclosure (+)	0.109	2.926	0.003	**Yes**
H7: Resignation --> Disclosure (+)	0.054	1.396	0.163	No
H8: Resignation --> IPA (+)	0.027	0.647	0.517	No
H9: IPA --> Disclosure (+)	0.072	1.843	0.065	No

IPA = Information Privacy Apathy

Table 41 Local Weather Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.097	-2.441	0.015	**Yes**
H2: PercNeed --> Disclosure (+)	-0.022	-0.557	0.578	No
H4: Familiarity --> Distrust (-)	0.138	3.557	***	No, reversed
H5: Familiarity --> Disclosure (+)	0.090	2.330	0.020	**Yes**
H7: Resignation --> Disclosure (+)	0.098	2.402	0.016	**Yes**
H8: Resignation --> IPA (+)	0.028	0.670	0.503	No
H9: IPA --> Disclosure (+)	-0.086	-2.136	0.033	No, reversed

IPA = Information Privacy Apathy

Table 42 The Weather Channel Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.227	-5.926	***	Yes
H2: PercNeed --> Disclosure (+)	0.075	1.908	0.056	No
H4: Familiarity --> Distrust (-)	-0.046	-1.155	0.248	No
H5: Familiarity --> Disclosure (+)	0.106	2.856	0.004	Yes
H7: Resignation --> Disclosure (+)	0.058	1.468	0.142	No
H8: Resignation --> IPA (+)	0.027	0.638	0.524	No
H9: IPA --> Disclosure (+)	0.026	0.651	0.515	No

IPA = Information Privacy Apathy

Table 43 Weather by Macro Pinch Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.132	-3.350	***	**Yes**
H2: PercNeed --> Disclosure (+)	-0.061	-1.539	0.124	No
H4: Familiarity --> Distrust (-)	0.051	1.299	0.194	No
H5: Familiarity --> Disclosure (+)	0.070	1.844	0.065	No
H7: Resignation --> Disclosure (+)	0.090	2.225	0.026	**Yes**
H8: Resignation --> IPA (+)	0.028	0.668	0.504	No
H9: IPA --> Disclosure (+)	-0.072	-1.790	0.073	No

IPA = Information Privacy Apathy

Table 44 Weather Underground Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.214	-5.717	***	**Yes**
H2: PercNeed --> Disclosure (+)	-0.012	-0.310	0.756	No
H4: Familiarity --> Distrust (-)	-0.114	-2.905	0.004	**Yes**
H5: Familiarity --> Disclosure (+)	0.260	7.184	***	**Yes**
H7: Resignation --> Disclosure (+)	0.042	1.088	0.277	No
H8: Resignation --> IPA (+)	0.028	0.653	0.514	No
H9: IPA --> Disclosure (+)	-0.028	-0.729	0.466	No

IPA = Information Privacy Apathy

Table 45 Yahoo! Weather Path Estimates and Hypothesis Support

Hypothesis (direction)	Path Coefficient (ß)	t-Values	p-value	Supported?
H1: Distrust --> Disclosure (-)	-0.060	-1.521	0.128	No
H2: PercNeed --> Disclosure (+)	0.095	2.352	0.019	**Yes**
H4: Familiarity --> Distrust (-)	-0.079	-2.023	0.043	**Yes**
H5: Familiarity --> Disclosure (+)	0.025	0.659	0.510	No
H7: Resignation --> Disclosure (+)	0.049	1.202	0.229	No
H8: Resignation --> IPA (+)	0.027	0.644	0.520	No
H9: IPA --> Disclosure (+)	-0.003	-0.071	0.943	No

IPA = Information Privacy Apathy

APPENDIX D

INDIVIDUAL APP ANALYSIS OF

MODERATED RELATIONSHIPS

Following are the detailed moderation analyses of the influence Perceived Need has as a moderator of the relationship between Distrust and Disclosure.

Table 46 Moderated Relationships per Individual Apps

	Distrust_x_PercNeed →Distrust		Distrust_x_PercNeed →ZDisclosure	
	Estimate	p-value	Estimate	p-value
AccuWeather	-.040	.383	.069	.139
Local Weather	-.153	.450	.003	.952
The Weather Channel	.011	.769	-.031	.377
Weather Underground	.003	.947	.083	**.018**
WM Pinch	-.300	.442	.020	.591
Yahoo Weather	.055	.148	.010	.796

PercNeed = Perceived Need; ZDisclosure = standardized values for Disclosure construct

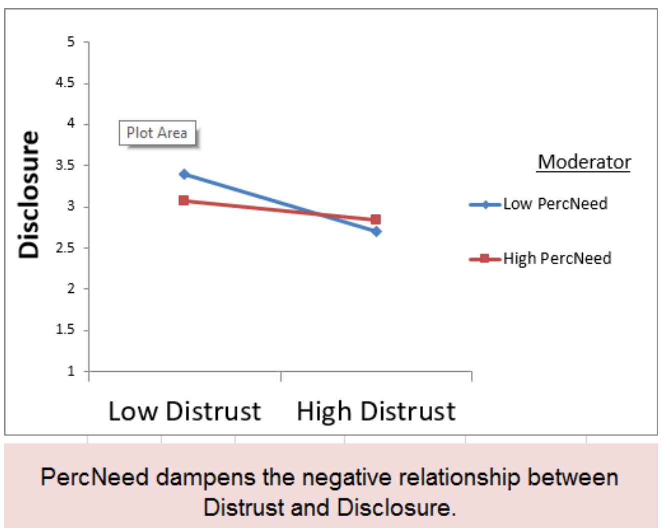


Figure 12 Moderating Effect of Perceived Need on the Relationship Between Distrust and Disclosure for Weather Underground

APPENDIX E

ANALYSIS OF MEDIATING RELATIONSHIPS

Below is the analysis of mediating relationships analyzed separately for each app.

App mediated relationships

Table 47 Individual App Mediation Analysis

App	Relationship	Direct effect (p-value)	Indirect effect	Confidence interval		p-value	Type
				High	Low		
Accu	Familiarity→Distrust→Disclosure	-.115 (.001)	-.014	-.007	-.024	.001	P
Accu	Resignation→IPA→Disclosure	.020 (.318)	.001	.008	-.003	.433	NS
LW	Familiarity→Distrust→Disclosure	-.030 (.074)	.005	.012	.001	.022	F
LW	Resignation→IPA→Disclosure	.050 (.019)	-.001	.003	-.008	.421	NS
TWC	Familiarity→Distrust→Disclosure	-.077 (.001)	-.007	.000	-.015	.043	P
TWC	Resignation→IPA→Disclosure	.031 (.199)	.001	.006	-.001	.365	NS
WMP	Familiarity→Distrust→Disclosure	-.039 (.016)	.005	.013	.000	.022	P
WMP	Resignation→IPA→Disclosure	.040 (.045)	-.001	.002	-.006	.361	NS
WU	Familiarity→Distrust→Disclosure	-.106 (.001)	-.010	-.004	-.018	.001	P
WU	Resignation→IPA→Disclosure	.019 (.019)	.000	.001	-.004	.484	NS
Yahoo	Familiarity→Distrust→Disclosure	-.036 (.004)	.000	-.003	.001	.343	NS
Yahoo	Resignation→IPA→Disclosure	.012 (.429)	.000	.002	-.001	.734	NS

Accu = AccuWeather; LW = LocalWeather; TWC = The Weather Channel; Yahoo = Yahoo! Weather