MOBILE APPS: PRIVACY ATTITUDES, KNOWLEDGE, & USER PRACTICES

by

Brien Twomey

Submitted in partial fulfillment of the

Requirements for Departmental Honors in

The Department of Information Systems and Supply Chain Management

Texas Christian University

Fort Worth, Texas

May 2, 2016

MOBILE APPS: PRIVACY ATTITUDES, KNOWLEDGE, & USER PRACTICES

Project Approved:

Supervising Professor: Beata Jones, Ph.D.

Department of: Information Systems and Supply Chain Management

Stacy Landreth Grau, Ph.D.

Department of: Marketing

ABSTRACT

With the explosive growth in number of mobile application downloads and the pervasive use of smartphones around the world, the issue of user privacy and security has evolved. The paper addressed seven research questions, as well as identified the pertinent literature surrounding the variety of issues with mobile privacy practices used by application developers and users. Within the discussion of pertinent literature, the paper addressed recent transgressions perpetrated by mobile application companies. Specifically, the paper discussed transgressions regarding the collection of users' personal data, as well as the current mobile application privacy rules and regulations in place in the United States and the rules developed in Europe. Along with the exploration of the literature, a study was conducted that focused specifically on privacy in regards to downloaded mobile applications on smartphones. The study examined the privacy attitudes, knowledge, and practices of mobile application users. Specifically, the research delved into how willing people were to give up their personal information to be able to use those mobile applications and if they were even aware that personal data is collected through their use of those applications. The analysis conducted tried to identify the existence of disconnects between users' attitudes, knowledge, and practices of privacy regarding their personal information from use of downloaded mobile applications.

TABLE OF CONTENTS

INTRODUCTION

The download of smartphone mobile applications continues to grow. In 2014 alone, there were over 125 billion downloads of mobile applications (McCarthy, 2014). The mobile application market has seen steadily increasing growth over the last few years, moving from just under 25 billion downloads in 2011 to a projected 270 billion by 2017 (McCarthy, 2014). Out of the 125 billion downloads in 2014 alone, over 90% were free applications (McCarthy, 2014). Milton Friedman (1975) makes the point clear that there is no such thing as a free lunch. His economic ideals do not make an exception for the ever-increasing mobile application market. In essence, consumers are now "paying" for these free downloaded smartphone applications with their personal information; information that they agree to give up when they click "Accept" on the terms and conditions page.

Various regulatory bodies have surprisingly taken the lead in addressing the issue of consumer information being collected by free mobile applications. Governments and regulatory bodies have pushed the forefront of the free application research, adapting preliminary guidelines and adjusting rules that either have not existed or are severely outdated (Leslie, 2015). Entities, including the State of California, have been leading the charge in creating new rules and guidelines for mobile app developers and the third party companies which buy the collected information. For instance, California's Online Privacy Protection Act, enforced in 2012 by Attorney General Kamala Harris, stressed the importance of making applications' privacy policies easily accessible to consumers (Krasnow, 2013). Unfortunately, California is only one of a handful of states that has taken any recent supervisory action on the free application front. The United States and the consumers of free mobile applications should look to Europe for the most recent documented progress and research on the topic. Currently, the European Commission is

pushing to pass an updated Data Protection Directive from 1995 (European Commission, 2012). The European Commission's work leads the field in terms of suggested protocols and development frameworks – information that is highly applicable to both consumers of mobile applications as well as developers. These regulations, including the strong popular support for initiatives like the Right to be Forgotten, have taken hold in Europe, but have received little attention in the United States. The main focus in the United States appears to be on companies that have run into recent legal trouble regarding information sharing and privacy, with HTC and Delta Airlines as two notable examples (Hale, 2013). Yet little has resulted from the exposure of these wrongdoings. A separate area of focus has been on the mobile application development companies themselves. There is scrutiny over the effectiveness of the frameworks and guidelines developed by these companies to govern their application developers. Many of the frameworks are inherently technical, including details on how to implement privacy protocols that would encrypt both personal data collected by the app as well as the data produced by the advertising agencies involved (Melson, 2015).Since free application download privacy issues is an emerging field, the information gathered and synthesized on this topic is somewhat limited, and the prior research is often excessively technical in nature, making it difficult for the everyday user to comprehend. Fortunately, the relevance of the studies that have been done to date is apparent, and the impending legislative moves and regulations being proposed cause even more focus to be placed on the privacy issue in the free application download domain.

To date, research has only covered the potential procedures and rules that entities in the United States and around the globe are enacting to protect and inform consumers of the consequences of downloading free mobile applications. There is little research on the perceptions of consumers regarding the type of information being pulled from their mobile application usage.

The collection of data, the kind of data collected, and the usage of that data is not widely known. With the complex legal jargon used in today's terms and conditions and privacy policies, the casual consumer has little true understanding of the data security and privacy concerns associated with using the free applications.

The ensuing research focuses on the data sharing and privacy issues that are entailed in everyday users agreeing to the privacy policy of a newly downloaded mobile applications. With the number of smartphones in use around the world reaching over 1.6 billion comes the rising concern for data privacy and end-user awareness (eMarketer, 2014). Specifically, the research investigates the attitudes, knowledge, and practices of smartphone users when it comes to personal information privacy on their downloaded mobile applications. The number of smartphones in use around the world is increasing, and with that growth comes the rising concern for data privacy and awareness by the end-user regarding what data is being collected, shared, and sold.

This paper begins with a review of the literature related to mobile application privacy practices employed by both the mobile applications and the users of those applications. Additionally, the literature review touches on some recent transgressions perpetrated by well-known companies regarding their collection and dissemination of users' personal data. A discussion of the rules and regulations currently in place in the United States and those being constructed in Europe follows. Then, the research questions and a methodology section are presented, followed by the analysis and results of the data collected to explore the research questions. Finally, a discussion section follows with limitations, implications of the research for both end users and businesses, and suggestions for future research.

MOBILE REVOLUTION

In 2014 there were over 2.6 billion smartphone subscriptions around the world, with a predicted 6.1 billion smartphones to be in use by 2020 (Ericsson, 2015). The time spent using these smartphones is dominated by the use of mobile applications, with 89% of all time spent on mobile phones accounted by mobile applications. (Rudolph, 2015). At the end of 2013, the average consumer was using over 26 different applications, spending over 30 hours on these applications per month (Nielson, 2014). Additionally, Rudolph (2015) shows that the average time consumers spend on their mobile applications has increased by 21% from 2014 to 2015. Finally, with mobile applications driving revenues of over 35 billion in 2014 alone and predicted to stretch to over 77 billion by 2017, it is apparent just how explosive the growth in the mobile industry has been in regards to mobile applications (Rudolph, 2015). Needless to say, the world is undergoing a mobile revolution, one that has taken the business world by storm.

In June of 2007, Apple launched the first iPhone, revolutionizing the mobile phone industry through the introduction of a true "smartphone" (Strain, 2015). Smartphones go beyond the basic functionality of being able to make phone calls. They now provide users access to complex computing capabilities and the functionality of greater connectivity, accentuated by downloadable applications. (Kang et al., 2015). These mobile applications allow smartphones to rival the power of mobile computers (Kang et al., 2015). Summerfield (2015) defines mobile applications as "applications that are downloaded and installed on your mobile device, rather than being rendered within a browser." Mobile applications, henceforth referred to as apps, are downloaded from device-specific platforms including Apple Inc.'s App Store, Google's Android Market, and Blackberry's App World depending on the consumer's operating system. Apple, Android, and Blackberry's shares continue to grow, as these three companies accounted for 97%

of the entire mobile market by the second quarter of 2014. Due to their dominance in the field, this study will focus solely on those three mobile platforms (Llamas et al., 2016).

With the ever growing importance of smartphones and the applications offered, companies all over the world in practically every industry have rushed to develop and/or sell apps (Kang et al., 2015). Businesses are seeing more and more consumer reliance on the release and upkeep of these applications, as Yang claims that they have become "an indispensable part of users' daily lives" (Kang et al., 2015). This comes as no surprise, as in the App Store marketplace alone there were over one million apps available as of January 2014 (Ranger, 2014), and over 200,000 available in the Android Marketplace in the same month (AndroLib, 2014).

COLLECTION AND USAGE

The free-market economist Friedman released a book titled, "There's No Such Thing as a Free Lunch" (Friedman, 1975). The popularization of this phrase derived from the book title has been at the core of a multitude of economic theories, centering on the idea of opportunity costs. Krugman and Wells (2012, p. 7) define opportunity costs as "what you must give up in order to get it." A synonymous phrase is "economic cost," which Krugman and Wells define as "the next sum of everything that must be given up in order to obtain an item" (Krugman and Wells, 2012, p. 7). Opportunity costs are considered by both consumers and business alike when making decisions, ensuring that they get the highest value for the actions they take. These costs are not always easily identifiable. With the advent of the digital age and the increased number of mobile phones, and with the subsequent mobile applications' widespread use, costs of downloading applications can be hidden, either intentionally or unintentionally, in the use of the services the applications provide. Focusing on free applications, Frenkel (2014) writes that "free apps cost user privacy and security," and that in some cases, "pay is based on the amount of data the

developers collect and share about users" (Frenkel, 2014, p. 1). In essence, the collection and sharing of customer personal data is what is used to pay for the use of free applications.

According to the European Commission, personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email, address, bank account, posts on social media, medical information, or phone ID numbers (European Commission, 2012). With the knowledge that customer personal data is being used to "pay" for free applications, the question follows as to what information is actually being mined by the applications that the everyday smartphone customer uses. According to The Appthority App Reputation Report for summer 2014, free apps exhibited the highest number of risky behaviors, with 99 of the top 100 iOS apps and 99 of the top 100 Android apps exhibiting at least one risky behavior (Appthority, 2014). A risky behavior is defined as "actions that put consumers and businesses at risk, through either capturing sensitive data or sharing sensitive data" (Appthority, 2014, p. 3). The information collected most often falls into one of the following four categories, although this list is not comprehensive: location tracking, address book, calendars, and unique identifiers (Appthority, 2014). The most common type of data that is collected is location-based data (Appthority, 2014). Specifically, 82% of the top free 100 Android apps and 50% of the top free 100 iOS apps track the app user's location (Appthority, 2014). This is commonly done when the developer of the application embeds a tracking code into the application's code, allowing the application to record where the mobile phone, and subsequently the consumer, is when the application is in use (Appthority, 2014).

Following what information is actually being collected by mobile applications, the next step is to identify where that information goes and how it is used. In regards to location tracking,

the information collected by the application is shared with advertising networks and analytics companies (Appthority, 2014). The location tracking information allows companies and networks to discover the specific customer's habits regarding where the consumer goes (Gralla et al., 2011). The location tracking can take shape in tracking both the physical location of the user as well as their so-called virtual location: the websites they visit when connected to the Internet. By tracking both the user's physical as well as online locations, patterns can be identified that can lead to advertisers identifying even more intimate information about a user's personal life. Commonly downloaded applications such as Angry Birds, Google Maps, and Candy Crush were even used by the National Security Agency to track user's physical locations as well as ascertain copious amounts of additional personal data from the user (Robertson, 2014). When apps have access to a user's address book on the smartphone, the contacts listed can also be mined and sold (Appthority, 2014). This is a way that app developers and the companies supporting the application can expand their customer base, and market additional mobile applications to the contacts listed on the phone (Appthority, 2014). With access to a smartphone's UDID (Unique Device Identifier), or IMEI (International Mobile Equipment Identity), app developers and data collection companies alike can "correlate user behavior across multiple apps" (Appthority, 2014). Even though platforms such as Apple's App Store claim to prohibit correlating data across multiple applications, the restriction is only enforced on the devices that are running the most updated version of iOS (Appthority, 2014). This creates real issues when a UDID or IMEI are known, user-specific data, including usernames and passwords, are associated and stored with the smartphones unique identifier. Thus they become accessible if the unique identifier is known (Appthority, 2014). Combining username and password information with the other types of data collected from the usage of free mobile applications, analytics companies and advertising

companies alike can synthesize personalized customer profiles and sell them to other marketing companies (Gralla et al., 2011). Unfortunately, as of now, not much can be done from a consumer's perspective once personal data is gathered by a mobile app (Gralla et al., 2011). Various government and regulatory bodies are pushing to change that in the near future.

COMPLIANCE AND LEGALITY

Even though companies collect vast amounts of user data in order to better understand their customers and gain customer insights to stay competitive, they often do so without thinking about the consequences of their actions on their relationship with customers (Plangger and Watson, 2015). Within the United States, the data collection practices used by developers follow loose guidelines and are often misleading in regard to what data can be collected and why. Sometimes, the developers, do not even release that information at all (O'Brien, 2012). Apple Inc.'s App Store, Google's Android Market, and Blackberry's App World all currently have measures in place to help address privacy concern issues.

When downloading an app through the Android marketplace, users are shown a list of permissions that the app asks for, ranging from "hardware controls," such as allowing the app to take pictures, to "your personal information," such as allowing the app to read the user's Internet browser history on their phone and the user's bookmarks (Gralla et al., 2011). This is all of the information that the developers need to provide to potential users currently. Lack of further disclosure puts the burden on the end user to take the time to read permissions, understand them, and make an informed decision about whether or not they are comfortable giving that information up (Gralla et al., 2011).

Blackberry's App World takes a different approach, as Blackberry is known for putting security first when it comes to adding applications on top of its operating system (Sacco, 2011).

Blackberry gives users the option to grant downloaded mobile applications the "Trusted Application Status" (Sacco, 2011). By having a "Trusted Application Status," the app has access to the three areas of security: Connections, Interactions, and User Data (Sacco, 2011). Connections refers to giving the app access to phone features like Bluetooth and Wi-Fi (Sacco, 2011). Interactions "dictate how applications can interact with device settings, and media and recording options," while User Data refers to the personal data stored on the phone that would be made available to the application if granted the "Trusted Application Status" (Sacco, 2011). If not granted a "Trusted Application Status," users of Blackberry can individually go through the three sections of security for each application, granting different security area access to each application. (Sacco, 2011).

Finally, Apple Inc.'s App Store functions in yet a different way. Unlike Android's Marketplace, apps that make their way onto the App Store are reviewed individually by Apple before they can be listed in the App Store (Gralla et al., 2011). Apple claims that it rejects any proposed apps that do not do what their description says, perform reliably, or respect the limitations Apple has provided in a broad "App Store Review Guidelines" that is constantly updated (App Store, 2015). Unbeknownst to many iOS users, applications that are approved for the App Store and subsequently downloaded are initially granted permission to Apple-provided apps and features, including the Camera, Contacts, Photos, and Music apps already installed on iPhones (Gralla et al., 2011). Again, similar to the other two major platforms, users have the ability to review application by application and deny specific permissions for apps, but the information that the app collects is not always readily accessible to users even if they are actively seeking that information. Although the security and privacy functionality is different in the App Store than on other platforms, the same issue is persistent as seen with Android apps and

Blackberry apps. Knowing what data is being collected and where that data is being sent depends on the end user to have knowledge of what permissions mean, as well as relying on the user to take the time to read permissions and make a decision as to whether or not they are comfortable giving personal information up voluntarily.

Recently, some regulatory bodies have taken a real interest in the privacy and security issues of free mobile applications. In 2012, the California attorney general Kamala D. Harris, reinforced a 2004 act entitled the California Online Privacy Protect Act, sending out letters to over 100 app developers whose applications were not in compliance with the act (Krasnow, 2013). The California Online Privacy Protection Act applies to any company that has customers download their app in the state of California. It protects the following information from being collected without explicitly stating that it does so in a conspicuously posted privacy policy: customer names, address, email, phone, social security number, or any identifier that permits physical or online contacting (Krasnow, 2013). Additionally, Harris, with six high profile tech companies created a Joint Statement of Principles document with five guidelines regarding information security and sharing that they plan to enforce in California. The statement focuses on making privacy policies more accessible, increasing transparency between developers and end users and implementing a reporting system to report infractions (Office of the Attorney General, 2012).

Overall, it appears as though one of the main pillars of this widespread issue comes down to consumer's privacy. Constantinos (2015) defines privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Laws and regulations are put in place to protect the privacy of users, but this is not always the case. With the mobile explosion in the world today, privacy

issues become more and more relevant. The discussion about what information can be collected, by whom it can be collected, and when it can be collected has shifted into "a gray legal area" (O'Brien, 2012). The existing consumer privacy protections in place have failed to keep up with the ever-evolving technology that is constantly transforming the world (O'Brien, 2012). Therefore, it is imperative that appropriate guidelines and rules be put in place that are easily understood and followed, as many online businesses consider the acquisition of customer personal data "the backbone of an ad-driven Internet," allowing the proliferation of free mobile app usage to continue (O'Brien, 2012).

PAST VIOLATORS

Due to a general lack of laws that would otherwise guide the providers of mobile apps, the misappropriation of consumer data is rampant. The Federal Trade Commission, (FTC), has on occasion successfully exposed companies that are misleading their consumers on what information is being taken when a consumer uses their app. For example, in February of 2013, the FTC brought charges against HTC America, a mobile device manufacturer (Hale, 2013). The free applications that were previously installed on HTC's devices posed severe privacy risks for consumers, and HTC had not done anything to warn their consumers. With the installation of these applications, consumers were vulnerable to the applications sending unwarranted text messages from their phones, and recording audio through the phone's microphone. Even information stored on the device such as financial account numbers or medical information could have been recorded and transmitted, all without the consumer's knowledge (Federal Trade Commission, 2013). Due to this blatant lack of security and subsequent misrepresentation by HTC that their customer's data was secure, the FTC filed a lawsuit against them alleging that HTC failed to take reasonable steps to secure the data. HTC ended up settling the charges with a

consent order, which required HTC to establish a security program and prohibiting HTC from "making any false or misleading statements about the security and privacy of consumers' data on HTC devices" (Hale, 2013).

The FTC also brought forth allegations against the popular free mobile app Snapchat. Snapchat told its users that the pictures taken and being sent to other users while using the app would disappear, yet it was proven that this was not true and that Snapchat was aware of the issue and could have easily taken steps to address the issue. Additionally, the FTC case also alleged that Snapchat was not truthful about how much of the consumers' personal data was being collected and disclosed. Concerning the nature of the disappearing pictures that Snapchat purported, the FTC rightfully claimed that Snapchat mislead consumers by saying that the pictures they took, or "snaps," would disappear forever after the designated time set by the original sender of the picture. It was shown that other users could easily gain access to these "snaps" even after the designated time through one of the following ways: use of a third-party app that could circumvent the security put in place by Snapchat to capture the original image, or by taking a screenshot of the image. If a screenshot was taken of their snap, a notification was only sent to the user if they had the most updated version of the phone's operating system at the time. If a third-party application was used then no notification would be sent. Beyond this misleading characteristic of the app, Snapchat also misrepresented its data collection practices. Snapchat collected geolocation information from users with Android operating systems, even though Snapchat explicitly stated otherwise in the privacy policy listed on the Android Marketplace. Additional charges were brought by the FTC because Snapchat collected personally identifiable data from its users that went beyond the scope of what they claimed to collect in the application's privacy policy. Specifically, Snapchat was supposed to only ask for

users' phone numbers through which it would collect their email address and Facebook ID, as laid out in the app's privacy notice. Instead, the application secretly collected all of the names and phone numbers from the user's contact list without consent. In May of 2014 Snapchat settled the claim with the FTC, resulting in a change to the app's privacy policy and data collection practices. The ruling prohibited Snapchat from misrepresenting "the extent to which it maintains the privacy, security, or confidentiality of users' information," and in addition Snapchat was required to implement a comprehensive privacy program which is planned to be monitored for the next 20 years (The Computer & Internet Lawyer, 2014).

Even though these sanctions imposed on both HTC and Snapchat may seem severe, the FTC is currently the only federal body taking action against mobile apps that violate consumers' privacy. While some states, such as California, are joining in, the regulatory power currently being wielded by controlling bodies in the United States is minimal. In Europe, the European Commission is making impressive headway with the "Right to be Forgotten," giving consumers the right to control how their personal data is consumed by companies vying for that data (Leslie, 2015).

USER EXPERIENCE & PERCEPTION

With the ever growing number of mobile devices and subsequent increases in mobile application downloads, another key area to investigate is how the users themselves perceive the consequences of data collection and privacy by mobile applications. Due to the widespread prevalence of smartphones and the ever increasing number of applications developed for them, there are countless services that the everyday user can access. This increased access has resulted in a considerably large volume of user data being gathered (Harris et al., 2014).Consequently,

with the influx of personal data being collected and shared come added privacy concerns for the end users.

There are multiple studies that suggest and support the idea that user age and other socio-demographic factors influence attitudes toward privacy, such as Sheehan's (1999) study on gender difference in online privacy concerns, and Graeff and Harmon's (2002) study that found that "privacy concerns vary by age, income, and gender." However, Hazari and Brown (2013) found that "most socio-demographic variables did not show significant effects on information privacy concerns." As such, the results are inconclusive as to whether socio-demographic factors affect privacy concerns. As Harris et al. (2014) study showed, the actual practice of secure habits is not discriminatory based on generation. In their 2014 study, Harris et al. looked at how data privacy knowledge and awareness translated into sound personal data practices for both undergraduate students who were about to enter the workforce as well as seasoned information technology professionals who actively worked in the IT fields. They found that there were no significant differences between the practices employed by undergraduate students and their information technology professional counterparts. From both populations of respondents they found that the groups had the ability and inclination to protect their privacy when using technology, but the actual practice of protecting their information was not existent. Furthermore, even the IT professionals were not able to demonstrate established levels of good privacy practices. These results suggested that commonly regarded safe data privacy practices "do not naturally come about as a result of longer-term experience" (Harris et al., 2014). Even the appropriate data security knowledge is not being put into practice. Slusky and Partow-Navid (2012) had come to the same conclusion in their study. They examined the correlation of students' practices and awareness of risks and countermeasures related to data through various

technological mediums. Their survey discovered that "the major problem with security awareness is not due to a lack of security knowledge, but in the way the students apply that knowledge in real-world situations" (Slusky & Partow-Navid, 2012). Overall, they found that "the compliance with information security awareness is lower than the understanding of it" (Slusky & Partow-Navid, 2012). The disconnect between privacy concern awareness and practice is concerning for the everyday user, especially when it comes to vast amount of personal data that is now being collected by smartphone applications.

The disconnect leads to the privacy paradox, in that users are uncomfortable with companies pulling personally identifiable information from them, especially without their knowledge, yet are willing to provide information despite acknowledging their concern for privacy issues (Acquisti & Grossklags, 2005; Barnes, 2006). Most of the information collected by companies through mobile applications is used to create customer profiles and send targeted advertisements, as the collected data represents a huge potential for marketers and companies to understand their customers better and address their needs more thoroughly. Marketers are interested in the more granular data because they want to be able to tailor advertising to the distinct consumer, and this personalization can only be done by having more complete knowledge of the customer's preferences and concerns (Chaney, 2009). Multiple studies have shown though that the "privacy paradox" is pervasive. A Pew Internet Research study (Purcell et al., 2012) found that the vast majority of online users disapprove of having their personal data and information collected for the purpose of targeted advertisements. Upon further inspection however, the personally identifiable information that is voluntarily posted by users suggests that "users are willing to give up information in return for customized information" (Purcell et al., 2012). Hazari and Brown (2013) found that customers are unwilling to have personal

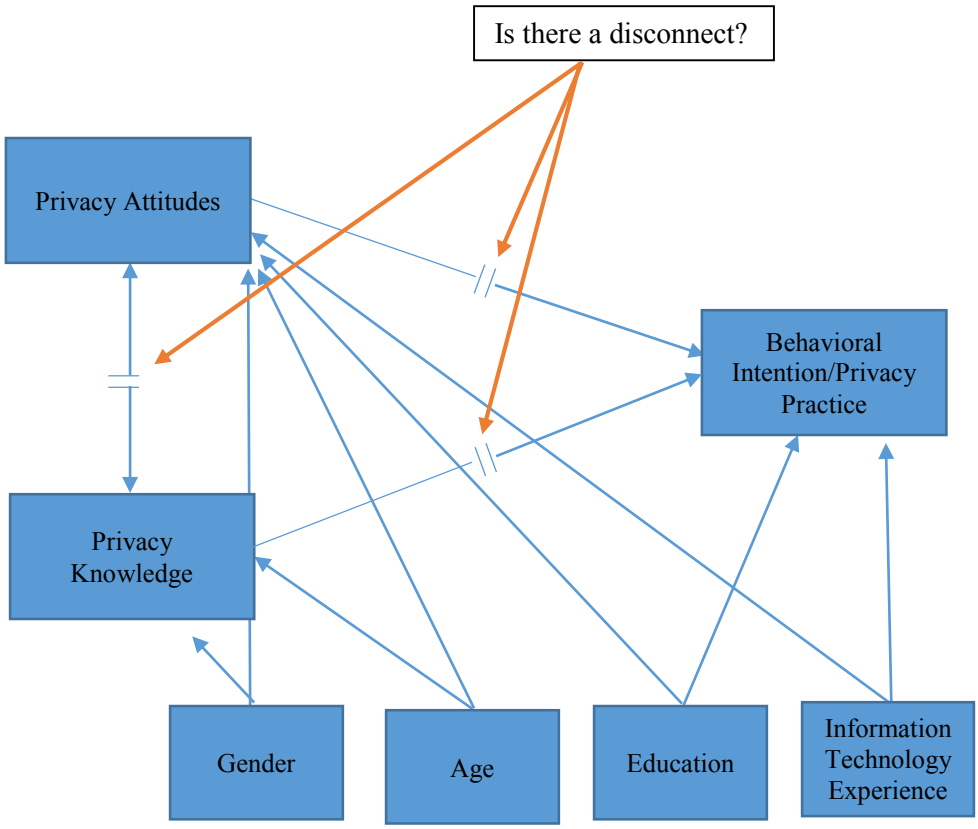
information collected for targeted advertising, specifically, information they put on social networking sites. Even though users are saying that they are uncomfortable with the collection practices employed by companies, their actions are contrary to their voiced sentiments. Shilton (2009) pointed out that most web browsers even have a 'do not track' button, but it is rarely activated. This shortfall could stem from a variety of reasons. As Shilton (2009) suggests, users are not aware that they can take easily accessible steps to anonyomize themselves against constant data collection. As Hazari and Brown (2013) postulated, most users expect that some form and level of tracking is employed by companies regardless of what the user does and they believe their personal data will always be at risk of exposure. Evidently though, users are both aware to some degree and concerned about current data sharing and privacy issues. Hazari and Brown (2013) stated this issue well, asserting that "Privacy has a technical as well as a behavioral component, but it is up to the user to be aware of the differences between these types of controls." As was found in a recent Pew Research study, privacy concerns are "case by case" rather than driven by broad principles, and this drives important questions to be asked concerning privacy concerns as they relate to users of downloaded mobile applications on smartphones (Dwoskin, 2016).

THEORETICAL BACKGROUND

Individuals that have a more positive attitude about how well protected their personal information is have been found to be more committed to using an online medium which they know to be potentially adverse to keeping their personal information secure. Generally, this acceptance behavior has been theorized to be influenced by a variety of individual differences including age, gender, and associated technical experience in addition to differences in individual's beliefs, attitudes, and situational influences (Agarwal, 2000). These conjectures are

founded on the Ajzen-Fishbein Theory of Reasoned Action, or TRA (Hazari & Brown, 2013). Subsequently, the Unified Theory of Acceptance and use of Technology (UTAUT) further considers influential factors for respondents' behaviors (Venkatesh et al., 2003). UTAUT offers a comprehensive review of the literature that studies age, experience and gender as influential socio-demographic factors that affect the relationship "between a system's expectations and behavior intention" (Venkatesh et al., 2003). The framework for the following study is founded on the conjunction of both the Theory of Reasoned Action and the Unified Theory of Acceptance and Use of Technology. Many of the studies previously mentioned in this paper have used one or both of these frameworks to study users through a variety of media, including social media sites and general online habits. Similarly, this study takes a similar approach and applies TRA and UTAUT to the use of downloaded applications on the user's smartphone device. Due to the relevancy of this issue and the fast-paced rate at which the mobile phone and mobile application fields evolve, there is a demonstrated need to study the general user's perception and the variables that affect the aspects of information privacy when it comes to mobile applications. Additionally, with the technology related to data collection expanding, research should be conducted on "how attitudes related to privacy have evolved as individuals get more comfortable and accepting of technology use" (Hazari & Brown, 2013). Figure 1 is a visual representation of the research model for the study and the research questions that follow.

Figure 1: Research Model



RESEARCH QUESTIONS

In order to examine the attitudes, knowledge, and practices of users of downloadable smartphone applications, this study poses seven research questions listed below.

Research Question 1: What are the attitudes of mobile app users regarding privacy on their mobile devices?

Research Question 2: Under what circumstances are users willing to give up privacy of personal information for free for more personalized functionality of their mobile apps?

Research Question 3: What are the attitudes of mobile app users regarding the current privacy protection policies established by the government and the mobile platform markets?

Research Question 4: What is the knowledge of mobile app users regarding privacy concerns on their mobile devices?

Research Question 5: What are the privacy practices of mobile app users on their mobile devices?

Research Question 6: How do socio-demographic factors (i.e., age, gender, and experience) of mobile app users affect attitude toward privacy, knowledge, or privacy practices, and their privacy-related behavior intentions on mobile devices?

Research Question 7: Is there a disconnect between the mobile app users' privacy attitudes, knowledge and their mobile app practices?

METHODOLOGY

This study surveys mobile application users across genders and generations about their attitudes, awareness, and practices in regards to personal data privacy in relation to mobile applications on smartphones. A copy of the survey can be found in the Appendix.

Participants

Data was gathered from a convenience sample of 385 adults living in the United States across various demographic variables, such as age, gender, education level, and IT-related experience. The participants were friends, family, and colleagues of the researchers. These participants are considered representative of the common user of downloaded mobile applications.

Procedure

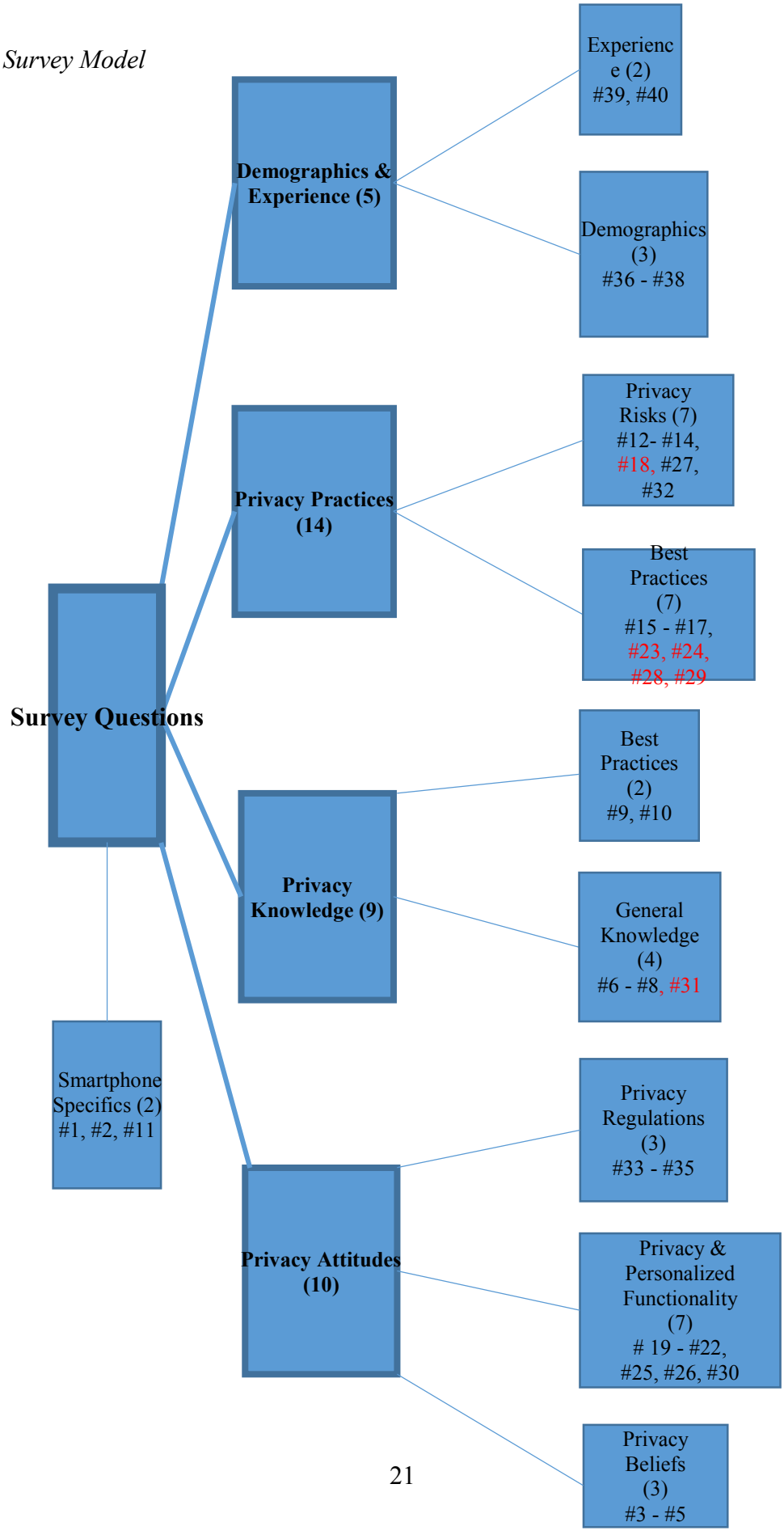
In order to study the attitudes, knowledge, and practices of mobile application users on smartphones, the investigators conducted a survey in which participants were asked to respond to questions that gauged their attitudes, as well as their knowledge and practices, towards current

privacy practices employed by downloadable mobile applications on smartphones. After completing a consent form and gathering demographic information, respondents answered questions regarding their smartphone mobile app privacy practices. The survey was distributed online via email and social media. The message associated with the survey contained a brief description of the purpose of the survey and a link to the survey itself. Completing the 40 question survey took no more than 15 minutes. Data was gathered during February and March of 2016, and the responses were organized using Qualtrics.

Measures

A majority of the questions asked in the survey used a five-point Likert scale to determine the degree with which each respondent agreed with the statement presented. The survey was pilot-tested with six individuals prior to administration. A figure mapping the survey is shown in Figure 2.

Figure 2: Survey Model



ANALYSIS

The collected survey results were reviewed for any incomplete responses and the incomplete data was removed, resulting in 385 sample size for the study. A summary of the significant findings from the analysis are presented below.

Demographics Data

There were a total of seven demographic questions in the survey designed to collect general information about the survey respondents. These questions included whether or not the respondent owned a smartphone, what type of smartphone they owned, their gender, their age, their education level completed, whether or not their education was/is in an IT related field, and the number of years they have worked in an IT related profession. Table 1 shows the demographic data, with the percentages out of 385 total respondents.

Demographics, Table 1

D#	Demographics Data							
D1	Own a smartphone	*Yes*	*No*					
		100.0%	0.0%					
D2	Type of smartphone	*Apple*	*Android*	*Other*				
		88.6%	9.6%	1.8%				
D36	Gender	*Male*	*Female*					
		42.6%	57.4%					
D37	Age	*Millennial*	*Non-Millennial*					
		69.1%	30.9%					
D38	Education Level	*High-school*	*Some College*	*Bachelors*	*Masters*	*Doctorate*		
		13.0%	51.9%	15.6%	9.1%	10.4%		
D39	IT Education Field	*Yes*	*No*					
		18.4%	81.6%					
D40	Years Worked in IT	*0*	*1-2*	*3-4*	*5-6*	*7-8*	*9-10*	*More than 10*
		71.9%	15.3%	3.6%	2.1%	0.0%	0.0%	7.0%

*D# - Demographic variables, with the number being the actual survey question number in the attached survey available in the Appendix.

The most common type of smartphone owned by respondents was an Apple iOS smartphone (88.6%). The majority of respondents (roughly 65%) have completed their high school education and/or some college education, with the vast majority (81.6%) not having an Information Technology related focus. Additionally, most respondents (71.9%) had no work-

related experience in an Information Technology field. Additionally, while a slight majority of the respondents were female (57.4%), there was a fairly even representation among genders. Finally, the majority of respondents came from the Millennial Generation (69.1%), those persons born between 1981 and 1997 (Fry, 2015).

Privacy Attitudes, Table 2

A#	Privacy Attitudes: Privacy Beliefs					
		Strongly Disagree	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***
A3	**Privacy...is important to me.**	1.8%	1.8%	7.5%	**57.9%**	**30.9%**
		Strongly Disagree	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A4	**I believe I am totally anonymous...**	**33.8%**	**51.4%**	9.6%	4.7%	0.5%
		Strongly Disagree	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A5	**I believe mobile app developers...**	5.7%	37.7%	37.7%	17.9%	1.0%
A#	**Privacy Attitudes: Privacy & Personalized Functionality**					
		Strongly Disagree	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A19	**I believe...if the app is free.**	**22.6%**	**42.6%**	19.5%	14.5%	0.8%
		Strongly Disagree	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A20	**I believe...share with third parties...**	**51.7%**	**31.4%**	9.6%	6.5%	0.8%
		Strongly Disagree	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A21	**Most of the time...**	2.3%	23.6%	20.3%	43.6%	10.1%
		Strongly Disagree	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A22	**I am willing...increased convenience...**	5.7%	20.3%	23.6%	46.0%	4.4%
	How concerned...privacy using "Google Maps"	*Not at all*	*Hardly*	*Neutral*	*Somewhat*	*A lot*
A25		14.0%	30.1%	32.2%	19.5%	4.2%
	How concerned...Location Tracking using "Google Maps"	*Not at all*	*Hardly*	*Neutral*	*Somewhat*	*A lot*
A26		14.3%	28.8%	25.7%	23.6%	7.5%
		Not at all	*Hardly*	*Neutral*	*Somewhat*	*A lot*
A30	**How concerned...using "Snapchat"**	17.1%	19.0%	30.1%	24.4%	9.4%
A#	**Privacy Attitudes: Privacy Regulations**					
		Strongly Disagree	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A33	**I believe the U.S. National Guidelines...**	**7.8%**	**47.0%**	28.1%	16.6%	0.5%
	I believe the Apple's App Store Guidelines...	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A34		2.9%	25.5%	31.2%	37.7%	2.9%
	I believe the Android's Android Marketplace Guidelines...	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*
A35		6.2%	31.4%	38.4%	22.3%	1.6%

Research Question 1: What are the attitudes of mobile app users regarding privacy on their mobile devices?

In order to address the first research question of the attitudes of mobile application users regarding privacy on their mobile devices three broad attitude questions were asked. It is apparent that privacy on respondents' smartphones is valued. Over 88% of respondents either

"Agreed" or "Strongly Agreed" with the statement that "Privacy, while using mobile applications on my personal smartphone, is important to me." At the same time, most respondents do not believe that they are anonymous while using applications on their smartphones (roughly 85%) and only 43% of respondents do not believe that mobile application developers provide necessary and adequate protection of their personal information.

Research Question 2: Under what circumstances are users willing to give up privacy of personal information for free for more personalized functionality of their mobile apps?

The other section of questions in the attitudes part of the survey dealt with privacy and personalized functionality, addressing research question number 2. The initial questions in this section, (A19, A20, A21, & A22), were intentionally broad-based questions to identify respondents' attitudes about how they believe personalized functionality from downloaded mobile applications should be attained. Most respondents (roughly 65%) are under the impression that it is not OK for free mobile applications to collect personally identifiable information from their users, nor should these free mobile applications collect and share users' personally identifiable information with third parties such as advertisers, app developers etc. (roughly 83% of respondents). A slight majority (roughly 53%) of respondents would be willing to pay money in order to remain anonymous while using the application. This shows that while a majority of respondents have the belief that mobile applications should not collect nor share their personally identifiable information, there is not a significant majority of respondents that would be willing to pay money in order to remain anonymous. Additionally, only a slight majority (just over 50%) responded that they would be willing to give up some of their personal data for increased convenience and functionality from their downloaded applications. It is important to

note that 46% of respondents did "Agree" with the statement that they would be willing to give up some of their personal data for increased functionality, as seen in table 2.

The remaining questions from the attitudes section introduced the case specific examples, dealing with the mobile applications "Google Maps" and "Snapchat." Even though "Google Maps" and "Snapchat" collect vastly different information from their users, respondents did not identify as having concerns about privacy while using either application. In both questions (A25 and A30), most respondents chose "Neutral" when asked if they were concerned about their privacy while using the application. Finally, most respondents noted that they were "Hardly" concerned about Location Tracking while using "Google Maps" (28.8%), while another 14.3% of respondents said that they were "Not at all" concerned about Location Tracking while using "Google Maps." These responses show that when initially asked about two applications that do collect personally identifiable information, one that collects much more information than the other, respondents are not very concerned about the collection of their personal information. This begs the question of whether or not respondents know that information is being collected from them and if they know what kind of information, as well as what practices these same users employ when it comes to privacy on their mobile applications.

> *Research Question 3:* What are the attitudes of mobile app users regarding the current privacy protection policies established by the government and the mobile platform markets?

The first question in the subsection on privacy regulation attitudes (K33) asked if the respondent believed the U.S. guidelines sufficiently protected mobile application user privacy. A very slight majority (roughly 55%) responded that the U.S. federal guidelines do not sufficiently protect user privacy. Out of the three policy questions, this was the only question that

respondents made a majority statement to either agree or disagree with. The following two questions (K34 and K35), which laid out the Apple App Store guidelines and the Android Android's Marketplace guidelines, did not garner a significant response. Respondents were split on whether or not the guidelines laid out by the two major players in the smartphone industry had requirements for their application developers that sufficiently protect user privacy. It should be noted that all three sets of regulations and guidelines, the U.S. federal regulations, the Apple App Store guidelines, and the Android Android's Marketplace guidelines were all simplified down into three bullet points with significant words bolded to make it quicker and easier for the survey respondents to read and understand. The actual rules and guidelines are multiple pages long, filled with legalese and verbiage that may prove difficult for a less well-versed end user to understand fully.

Privacy Knowledge, Table 3

K#	Privacy Knowledge: General Knowledge							
K6	I know what personally identifiable information...my mobile apps collects	***Strongly Disagree***	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*		
		12.7%	**57.1%**	14.8%	14.3%	1.0%		
K7	I know how to use privacy controls...	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***		
		3.9%	23.6%	14.5%	**53.5%**	**4.4%**		
K8	When I delete a mobile app...information collected by that app is also deleted.	***Strongly Disagree***	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*		
		17.9%	**55.6%**	15.3%	9.6%	1.6%		
K31	Do you believe Snapchat tracks...	*Contacts' info*	*Email*	*Name*	*Photos*	*Location*	*Web History*	*None*
		21.3%	17.5%	14.5%	15.9%	22.1%	5.6%	3.1%
K#	Privacy Knowledge: Best Practices							
K9	It is good practice...read the entirety of the privacy policy...	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***		
		2.6%	9.4%	23.9%	**54.8%**	**9.4%**		
K10	It is good practice...enable and disable Location Tracking...	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***		
		0.0%	3.1%	10.1%	**59.5%**	**27.3%**		

Research Question 4: What is the knowledge of mobile app users regarding privacy concerns on their mobile devices?

In regards to the respondents' general knowledge about privacy on mobile apps, there was again not always a strong consensus among all of the respondents as to what they knew or did not know. Surprisingly, roughly 70% of respondents answered that they did not know what personally identifiable information their mobile applications collected. Additionally, most respondents (73.5%) correctly said that they do not agree with the statement that "When I delete

a mobile application from my smartphone that I previously downloaded, the information collected by that application is also deleted." Roughly 58% of respondents replied that they did know how to use privacy controls on their downloaded mobile applications on their smartphones. Furthermore, only 10.9% of respondents (42 out of the 385) correctly recorded that Snapchat does track all six of those aspects of users' personally identifiable information. Of those respondents that have the application Snapchat downloaded and use it (answering "Yes" to both questions P28 and P29), 7.4% of respondents (17 out of the 232) correctly recorded that Snapchat does track all six of the personally identifiable information identified by Snapchat. Finally, most respondents (roughly 64%) said that they thought it was good practice to read the entirety of the downloaded applications' privacy policy, a practice that is commonly known as a best practice regarding user privacy on smartphones. When asked about whether or not it was good practice to enable and disable Location Tracking depending on the application, over 86% of respondents agreed that it was good practice to do so.

Privacy Practices, Table 4

P#	Privacy Practices: Best Practices							
		Strongly Disagree	***Disagree***	*Neither Agree nor Disagree*	*Agree*	*Strongly Agree*		
P15	Every time...read the privacy policy in its entirety.	**57.7%**	**36.6%**	3.9%	1.6%	0.3%		
	I enable and disable Location Tracking...depending on	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***		
P16	the mobile app	3.4%	11.9%	8.6%	**57.1%**	**19.0%**		
	I enable and disable privacy controls...depending on	*Strongly Disagree*	*Disagree*	*Neither Agree nor Disagree*	***Agree***	***Strongly Agree***		
P17	the mobile app	4.4%	17.9%	18.2%	**46.5%**	**13.0%**		
	Do you...Google Maps downloaded on your	*Yes*	*No*					
P23	smartphone	69.9%	30.1%					
		Yes	*No*					
P24	Do you use Google Maps on your smartphone	63.9%	36.1%					
		Yes	*No*					
P28	Do you...Snapchat downloaded on your smartphone	35.3%	64.7%					
		Yes	*No*					
P29	Do you use Snapchat on your smartphone	39.7%	60.3%					
P#	**Privacy Practices: Privacy Risks**							
		Last week	*Last month*	*Last year*	*Over a year*	*Never*		
P11	When was the last time you downloaded...	58.2%	34.8%	5.7%	0.8%	0.5%		
		Yes	***No***	*I don't know*				
P12	Have you ever jailbroken or rooted your smartphone...	14.3%	**82.1%**	3.6%				
		Yes	*No*	*I don't know*				
P13	Have you ever...Location Tracking on your smartphone	**90.4%**	6.5%	3.1%				
		Yes	*No*	*I don't know*				
P14	Have you ever...privacy controls on your smartphone	**71.2%**	15.1%	13.8%				
		Calendar Events	*Call Log*	*Contacts*	*Credit Card*	*Name*	*Email*	
	What personal information...using a free mobile app	7.1%	2.1%	8.2%	2.0%	18.1%	15.9%	
		Phone Number	*Photos*	*Location*	*SS#*	*Texts*	*Other*	*None*
P18		9.7%	7.8%	12.4%	0.1%	1.3%	1.0%	35.1%
		A lot less	*Less than before*	***No Change***	*More than before*	*A lot more*		
P27	Knowing that Google Maps...use this app in the future	3.6%	13.8%	**79.7%**	2.1%	0.8%		
	Which of the following...Snapchat tracks on your	*A lot less*	*Less than before*	***No Change***	*More than before*	*A lot more*		
P32	smartphone	17.9%	16.4%	**65.2%**	0.3%	0.3%		

Research Question 5: What are the privacy practices of mobile app users on their mobile devices?

In order to address the above research question, table 4 was created to show all of the questions from the survey that addressed the respondents' practices in regards to privacy.

The first section of questions from the privacy practices questions addressed best practices in regards to privacy. Most respondents, (roughly 60%), do enable and disable privacy controls depending on the mobile application. Furthermore, most respondents (over 70%) do enable and disable Location Tracking depending on the mobile application. Surprisingly though, over 94% of respondents answered that they do not read the entirety of the privacy policies of the downloaded mobile applications.

The second subset of questions regarding privacy practices addressed privacy risks. A large majority of respondents (82.1%) have not ever jailbroken or rooted their smartphones. Additionally, 71.2% of respondents have enabled or disabled privacy controls on their smartphones. An even higher percentage of respondents, (90.4%) have enabled or disabled Location Tracking on their smartphone at one point. Interestingly enough though, 35.1% of respondents answered that they would not be willing to give up any personal information while using a free mobile application.

Finally, questions P23, P24, P27 and P28, P29, and P32 address the two example mobile applications that respondents were questioned about in the survey. These questions asked survey respondents to answer how likely they were to use two applications, Google Maps and Snapchat, after learning what these applications collect from their users. P23 asked respondents, "Do you currently have the application 'Google Maps' downloaded on your smartphone?" and P24 followed by asking "Do you use 'Google Maps' on your smartphone?" while P28 asked "Do you

currently have the application 'Snapchat' downloaded on your smartphone?" and P29 asked "Do you use "'Snapchat' on your smartphone?" For respondents' use of both Google Maps and Snapchat, the majority of respondents answered that there would be no change in their use of the application (if they answered "Yes" to questions P23 and P24 or "Yes" to questions P28 and P29 for Google Maps and Snapchat respectively). 85.5% of those respondents answered "No Change" in regards to their use of Google Maps in the future after being told that it collects their location information. 79.3% answered "No Change" in regards to their use of Snapchat in the future after being told that it collects a variety of users' personal information.

Research Question 6: How do socio-demographic factors (i.e., age, gender, and experience) of mobile app users affect attitude toward privacy, knowledge, or privacy practices, and their privacy-related behavior intentions on mobile devices?

Tables 5, 6, 7, 8, 9, 10, and 11 show the results of correlations between demographic questions (D36, D37, D38, D39, and D40) and each of the seven subsets of questions identified in the Survey Model (Figure 2).

Attitudes – Privacy Beliefs, Table 5

Attitudes – Privacy Beliefs Correlations						
		D36	D37	D38	D39	D40
A3	Pearson Correlation	-.011	.047	.022	-.068	.047
	Sig. (2-tailed)	.835	.356	.671	.184	.362
A4	Pearson Correlation	.073	.037	-.055	.046	-.069
	Sig. (2-tailed)	.150	.469	.283	.363	.178
A5	Pearson Correlation	-.078	**-.225****	**-.176****	.018	-.091
	Sig. (2-tailed)	.129	.000	.001	.721	.076

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

As Table 5 shows, the only significant correlation between socio-demographic factors and respondents attitudes regarding privacy beliefs was evident in question A5. With a negative correlation of -0.225 at the 0.01 level, the conclusion can be drawn that the older the respondent to the survey was, the more strongly they disagreed with the statement that mobile application developers provide necessary and adequate protection of their personal data. Additionally, with a slightly negative correlation between A5 and D38, there is a negative correlation between education level completed and how respondents felt about the protection offered by mobile application developers. The less education completed by respondents, the more adequate they felt the protection was provided by mobile application developers.

Attitudes – Personalized Functionality, Table 6

Attitudes – Personalized Functionality Correlation						
		D36	D37	D38	D39	D40
A19	Pearson Correlation	**-.203****	**-.257****	**-.147****	-.040	-.070
	Sig. (2-tailed)	.000	.000	.004	.438	.173
A20	Pearson Correlation	**-.208****	**-.169****	-.098	.036	-.065
	Sig. (2-tailed)	.000	.001	.054	.482	.203
A21	Pearson Correlation	.043	**.165****	**.124***	-.057	.019
	Sig. (2-tailed)	.401	.001	.015	.263	.710
A22	Pearson Correlation	**-.131***	**-.181****	.002	-.024	-.015
	Sig. (2-tailed)	.010	.000	.973	.641	.772
A25	Pearson Correlation	**.154****	**.224****	.068	-.098	.091
	Sig. (2-tailed)	.002	.000	.185	.054	.075

A26	Pearson Correlation	**.159****	**.176****	.028	-.088	.066
	Sig. (2-tailed)	.002	.001	.585	.086	.195
A30	Pearson Correlation	.023	**-.165****	**-.148****	-.078	-.096
	Sig. (2-tailed)	.649	.001	.004	.126	.060

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 6 shows the rest of the attitudes-based questions in relation to the socio-demographic factors asked in the survey. Interestingly enough, there is a significant correlation between the gender of the respondent and their answers to questions A19, A20, A22, A25, and A26. A19, A20, and A22 asked respondents to rate on a five-point Likert scale how much they agreed with the statements, “I believe it is OK for a mobile application to collect personally identifiable information from its users, if the application is free." (A19), "I believe it is OK for a mobile application to collect and share with third parties (advertisers, application developers, etc.) personally identifiable information from their users, if the application is free.” (A20), and "I am willing to give up some privacy of my personal data in exchange for increased convenience and functionality from my downloaded mobile applications.” (A22). A25 and A26 also used a five-point Likert scale to ask respondents “How concerned are you about your privacy using ‘Google Maps’?” (A25) and “How concerned are you about Location Tracking using ‘Google Maps’?” (A26). Additionally, there was a slight negative correlation between A19 and D38, meaning that the more educated the respondent, the more strongly they disagreed with the statement that it is OK for a mobile application to collect personally identifiable information from their users if the application is free. Finally, there was a significant correlation between all of the attitudes questions dealing with personalized functionality and the subsequent age of the respondents. Specifically, questions A19, A20, A22, and A30 (A30 asked respondents “How

concerned are you about your privacy using 'Snapchat'?") all showed negative correlations, meaning the older the survey respondent was the more strongly they disagreed with the posed statements. For questions A21, A25, and A26 there was a statistically significant positive correlation all at the 0.01 level. A21, A25, and A26 asked respondents, using a five-point Likert scale to respond to the following statements: "Most of the time, I would be willing to pay money for a mobile application to remain anonymous while using the application." (A21), "How concerned are you about your privacy using 'Google Maps'?" (A25), and "How concerned are you about Location Tracking using 'Google Maps'?" (A26). In these cases, the older the survey respondent was, the more likely they were to agree with the posed statement. It is interesting to note that there were opposite correlations for questions A21 and A22. For A21, the older the respondent was the more willing they are to pay money for a mobile application in order to remain anonymous while using the application. For A22, The older the respondent was the less willing they would be to give up personal data in exchange for increased convenience and functionality from their downloaded mobile applications.

Attitudes – Privacy Regulations, Table 7

Knowledge – Privacy Regulations Correlations						
		D36	D37	D38	D39	D40
A33	Pearson Correlation	-.040	-.079	-.070	.024	-.047
	Sig. (2-tailed)	.432	.121	.169	.643	.353
A34	Pearson Correlation	-.040	-.055	-.006	-.039	-.063
	Sig. (2-tailed)	.435	.285	.907	.447	.217
A35	Pearson Correlation	-.007	**-.128***	**-.106***	.044	-.063
	Sig. (2-tailed)	.887	.012	.038	.391	.218

*. Correlation is significant at the 0.05 level (2-tailed).

Table 7 shows the correlations between the socio-demographic factors (D36, D37, D38, D39, and D40) and the Privacy Regulations questions (K33, K34, and K35). As the table shows, the only question that shows statistically significant correlations is question K35, which asked about respondent's knowledge regarding the Android's Android Marketplace Guidelines for application developers. Regarding both age and education level completed, there was a slightly negative correlation, meaning that the older the respondent was as well as the higher the education level of the respondent, the less likely they were to agree with the statement that Android's guidelines sufficiently protect mobile application user privacy.

Knowledge – Best Practices, Table 8

Knowledge – Best Practices Correlations						
		D36	D37	D38	D39	D40
K9	Pearson Correlation	**.207****	**.254****	**.127***	-.070	**.118***
	Sig. (2-tailed)	.000	.000	.013	.173	.021
K10	Pearson Correlation	-.038	**.210****	**.134****	**-.118***	**.120***
	Sig. (2-tailed)	.452	.000	.009	.021	.018

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 7 shows the relationship between socio-demographic factors (D36, D37, D38, D39, and D40) and questions K9 and K10 from the knowledge section of the survey model, specifically the Best Practices subsection of Figure 3. Both questions K9 and K10 had some statistically significant correlation with all but one of the demographic factors (whether or not the respondent's field of study was in Information Technology for question K9 and the respondent's gender for question K10). Regarding question K9, there was a positive correlation between gender and if the respondent agreed with the statement that it was good practice to read the

entirety of the privacy policy when downloading a mobile application. This means that female respondents were more likely to agree with the generally accepted best practice of reading the privacy policy when downloading a mobile application. Additionally, the older the respondent was, the more education they had completed, and the more number of years they had worked in an Information Technology related field, then the more likely they were to agree with the best practice of reading the entirety of the privacy policy when downloading a mobile application. Regarding question K10, if they respondent agreed with the statement that it is good practice to enable and disable Location Tracking on a smartphone depending on the mobile application, there was a positive correlation for increasing age, higher education level, and the more number of years worked in an Information Technology related field. There was a negative correlation between K10 and D39, meaning that if the respondent's field of study was not in Information Technology, then they were less likely to think that it is good practice to enable and disable Location Tracking depending on the mobile application.

Knowledge – General Knowledge, Table 9

Knowledge – General Knowledge Correlations						
		D36	D37	D38	D39	D40
K6	Pearson Correlation	**-.200****	**-.125***	**-.143****	-.081	-.033
	Sig. (2-tailed)	.000	.014	.005	.111	.521
K7	Pearson Correlation	**-.148****	**-.255****	-.097	-.067	-.076
	Sig. (2-tailed)	.004	.000	.058	.189	.138
K8	Pearson Correlation	.058	**.119***	**.132****	.038	.093
	Sig. (2-tailed)	.257	.019	.010	.456	.070

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 9 shows the correlation between the demographic questions (D36, D37, D38, D39, and D40) and knowledge questions K6, K7, and K8 from the General Knowledge subset of Figure 3. Regarding questions K6 and K7 (K6 which asked if respondents feel like they know "what personally identifiable information about me each of my mobile applications collects" and K7 which asked if respondents feel like they know "how to use privacy controls on my smartphone for my mobile applications."), there was a statistically significant negative correlation between gender and age for both K6 and K7, as well as a negative correlation regarding education level completed for question K6. These results demonstrate that males were more likely to agree with the statements "I know about what personally identifiable information about me each of my mobile applications collects" (K6) and "I know how to use privacy controls on my smartphone for my mobile applications," (K7) while females were more likely to disagree. Additionally, the older the respondent was the more likely they were to disagree with both statements. Finally, the higher the education level completed of the respondent, the more likely they were to disagree with the statement posed in K6. Finally, Table 8 also shows that there are two statistically significant positive correlations regarding question K8 and D37 and D38. These results show that the older the respondent was and the higher their education level, the more likely there were to incorrectly agree with the statement that "When I delete a mobile application from my smartphone that I previously downloaded, the information collected by that application is also deleted.

Practices – Best Practices, Table 10

Practices – Best Practices Correlation						
		D36	D37	D38	D39	D40
P15	Pearson Correlation	.041	**.205****	.063	-.054	**.110***
	Sig. (2-tailed)	.426	.000	.217	.292	.031
P16	Pearson Correlation	**-.146****	-.087	.003	**-.139****	.071
	Sig. (2-tailed)	.004	.089	.955	.006	.162
P17	Pearson Correlation	-.064	**-.154****	-.078	**-.129***	-.029
	Sig. (2-tailed)	.208	.002	.129	.011	.571

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 10 shows the correlations between the demographic questions and the practices questions from the Best Practices subset of Figure 3 (P15, P16, and P17). For question P15, there was a statistically significant positive correlation for both age (D37) and years worked in an Information Technology related field (D40) and if respondents agreed with the statement "Every time I download a mobile application, I read the privacy policy in its entirety" (P15). This means that the older the respondent was and the more years they had worked in an Information Technology related field, the more likely they were to employ the commonly accepted best practice of reading the privacy policies of their downloaded mobile applications. Question P16 showed a negative correlation for both gender and whether or not the respondent's field of study was in Information Technology. This means that more males were likely to agree with the statement "I enable and disable Location Tracking on my smartphone depending on the mobile application" (P16), and respondents whose field of study was not in Information Technology were also more likely to agree with the statement. Finally, there was a negative correlation for

both age and if the respondent's field of study was in Information Technology for question P17, which reads "I enable and disable privacy controls on my smartphone depending on the mobile application." As such, the older the respondent was and if their field of study was in Information Technology, then the more likely they were to disagree with the statement in question P17.

Practices – Privacy Risks, Table 11

Practices – Privacy Risks Correlations						
		D36	D37	D38	D39	D40
P12	Pearson Correlation	**.221****	**.164****	**.195****	**.187****	.072
	Sig. (2-tailed)	.000	.001	.000	.000	.157
P13	Pearson Correlation	-.057	**-.124***	-.040	-.056	.021
	Sig. (2-tailed)	.262	.015	.435	.273	.681
P14	Pearson Correlation	**-.119***	**-.125***	-.026	**-.155****	.023
	Sig. (2-tailed)	.019	.014	.614	.002	.656
P27	Pearson Correlation	**-.148****	**-.139****	.032	.093	**-.126***
	Sig. (2-tailed)	.004	.006	.531	.069	.013
P32	Pearson Correlation	**-.201****	**-.425****	**-.246****	.004	**-.235****
	Sig. (2-tailed)	.000	.000	.000	.936	.000

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 11 shows the correlations between the Privacy Risks questions (P12, P13, P14, P27, and P32) and the demographic questions from the survey (questions D36, D37, D38, D39, and D40). Question P12 resulted in positive significant correlations all at the 0.01 level for gender, age, education level, and if the respondent's education field is in Information Technology. As such, if the respondent was male, the older the respondent, the higher the respondent's level of education, and if their education field was in Information Technology, the

less likely they were to have "jailbroken" or "rooted" their smartphone. For question P13, the only statistically significant correlation was between age and whether or not the respondent had ever enabled or disabled Location Tracking. As the table shows, the older the respondent, the more likely there were to have not enabled or disabled Location Tracking. Question P14 asked if the respondent had ever enabled or disabled privacy controls on their smartphone before, to which a negative statistically significant correlation resulted for gender, age, and if the respondent's educational field was in Information Technology. As a result, male respondents were more likely to have enabled or disabled privacy controls than females. Additionally, the older the respondent was, the less likely they were to have enabled or disabled privacy controls. Finally, respondents whose field of study was not in Information Technology were more likely to have enabled or disabled privacy controls on their smartphones. Regarding question P27, which asked about the respondents willingness to use Google Maps in the future after learning that it collects location information, Table 11 shows three negative correlations from demographic factors. First is gender, in that female respondents were less likely to use Google Maps in the future. Second is age, in which the younger the respondent was the less likely they were to use Google Maps in the future. Finally, the fewer years of experience working in an Information Technology field the respondent had, the less likely they were to use Google Maps in the future after learning that it collects location information from users. The last question addressed in Table 11 is P32, which asked about the likelihood that respondents would use Snapchat in the future after learning the information that Snapchat has access to. There was a resulting statistically significant negative correlation for all socio-demographic factors except for whether or not the respondent's field of study was in Information Technology. Regarding gender, female respondents were less likely to use Snapchat in the future. As for age, the younger the respondent

the less likely they were to use Snapchat in the future. Regarding education level, the less education the respondent had completed the less likely they were to use Snapchat in the future. Finally, the less years of work experience in an Information Technology related field, the less likely the respondent was to use Snapchat in the future. It is possible that these results showcase that younger respondents with less education and less Information Technology exposure were made aware of the personal information collected from them by both Google Maps and Snapchat and felt more inclined to use these applications less moving forward.

Research Question 7: Is there a disconnect between the mobile app users' privacy attitudes, knowledge and their mobile app practices?

Tables 12, 13, 14, and 15 show the results of correlations between the attitudes, knowledge, and practice questions. Questions were selected to be compared to one another based on what would be expected to be common knowledge and common best practices in regards to privacy on mobile applications. As a result, the presence of a statistically significant correlation (or a lack thereof) was used to identify disconnects between respondents' attitudes, knowledge, and practices.

Table 12

A3 & Knowledge Disconnect Correlations

		K6	K7	K9
A3	Pearson Correlation	.024	**.107***	**.113***
	Sig. (2-tailed)	.643	.036	.027

*. Correlation is significant at the 0.05 level (2-tailed).

As Table 12 shows, there is a positive statistically significant correlation at the 0.05 level between questions A3 and K7 and K9. There is no correlation between A3 and K6. The correlations for K7, K9, and A3 mean that those who agreed with the statement that privacy

while using mobile applications is important to them (A3) also answered that they do know how to use privacy controls on their smartphone (K7) as well as knowing that it is good practice to read the entirety of the privacy policy when downloading mobile applications (K9). While these correlations should be expected, the fact that there was no positive statistically significant correlation between A3 and K6 can be identified as the possibility of a disconnect between users attitudes and knowledge. This means that those who see privacy as being important to them did not necessarily agree or disagree with the statement that they know what personally identifiable information about them each of their mobile apps collect.

Table 13

A3 & Practices Disconnect Correlations

		P12	P14	P15	P17
A3	Pearson Correlation	**.104***	-.002	-.013	**.126***
	Sig. (2-tailed)	.042	.968	.802	.014

*. Correlation is significant at the 0.05 level (2-tailed).

Table 13 addresses the possibility of disconnects between respondents' attitudes and practices. As Table 13 shows, question A3 also has significant correlations with question P12 and question P17. This means that those who said privacy is important to them while using mobile applications (A3) also tended to answer that they have not "jailbroken" or "rooted" their smartphone (P12). Additionally, those who said privacy is important to them while using mobile applications (A3) also would agree with the statement "I enable and disable privacy controls on my smartphone depending on the mobile application" (P17). Interestingly enough, there was no statistically significant correlation between question A3 and question P15, meaning that there was no relationship between respondents who said privacy is important to them while using

mobile applications and respondents who agreed with the statement “Every time I download a mobile application, I read the privacy policy in its entirety” (P15).

Table 14

K9 & P15 Disconnect Correlations

		P15
K9	Pearson Correlation	**.212****
	Sig. (2-tailed)	.000

**. Correlation is significant at the 0.01 level (2-tailed).

Table 14 shows the relationship between question K9 and P15, addressing the relationship between respondents knowledge and practices. As Table 14 shows, there is a positive statistically significant correlation between how respondents replied to “"It is good practice to read the entirety of the privacy policy when downloading a mobile application onto a smartphone." (K9) and "Every time I download a mobile application, I read the privacy policy in its entirety." (P15). This means that those who agreed with K9 would also agree with P15.

Table 15

K10, P13 & P16 Disconnect Correlations

		P13	P16
K10	Pearson Correlation	**.130***	**.331****
	Sig. (2-tailed)	.011	.000

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 15 shows the relationship between respondents’ knowledge and practices. There is a positive statistically significant correlation between K10 and P13 and P16. For the relationship

between K10 and P13, those who agreed with the statement “It is good practice to enable and disable Location Tracking on a smartphone depending on the mobile application.” (K10) also agreed with the statement “Have you ever enabled or disabled Location Tracking on your phone” (P13). Additionally, there was even a stronger positive correlation (0.331 at the 0.01 level) between K10 and P16. This means that those who agreed with the statement in question K10 also agreed with the statement “I enable and disable Location Tracking on my smartphone depending on the mobile application." (P16).

DISCUSSION

Looking at both Table 14 and Table 15, due to the statistically significant positive correlations between K9, K10, P13, P15, and P16 it can be concluded that there is no disconnect between respondents’ knowledge and practices. When looking to see if there is a disconnect between respondents’ attitudes and practices, the only possible disconnect is between A3 (“privacy, while using mobile applications, is important to me”) and P15 (“Every time I download a mobile application, I read the privacy policy in its entirety.”) It would follow that there would be a positive correlation between these two, yet the lack of a positive correlation shows that further research should be conducted to see if there is a disconnect. Finally, there is possibly a disconnect between respondents attitudes and knowledge for questions A3 and K6 (K6, which asked if respondents felt like they knew “what personally identifiable information about me each of my mobile applications collects”) due to the lack of a statistically significant positive correlation. This is again an instance where further research could be conducted to verify that the disconnect exists. With a lower-than-recommended 0.70 Cronbach’s Alpha for the scales’ reliability measures, comprehensive statements about smartphone mobile application users’ privacy attitudes, knowledge, and practices cannot be made. But when addressed at an

individual question level, there are multiple noteworthy disconnects that are evident between users' attitudes, knowledge, and practices.

LIMITATIONS

The study has a few limitations associated with the results worthy of noting. The first limitation is the population that was used for the study. While the population was diverse in age, gender, and education level completed, 88.6% of respondents had Apple smartphones. Implicit in owning an Apple smartphone and downloading Apple mobile applications comes the trust that Apple has pre-screened all of its applications that are available on the Apple App Store. This may lead to many users being less concerned about their privacy compared to those that are not downloading Apple App Store applications. Another limitation worth noting is that personal political attitudes on the issue of privacy may have impacted how respondents answered survey questions. Depending on how the respondent views the importance of privacy and issues such as government surveillance of citizen's data, this may have affected how respondents answered the survey questions. It is worth noting though that 88.8% of respondents still agreed with the statement "Privacy, while using mobile applications on my personal smartphone, is important to me." Respondent's personal political views may have played more of a role in how they answered questions regarding their future use of an application after learning what personal information they give up when using the application, such as the results seen with the application "Snapchat." If the respondent had the belief that their personal information is accessible regardless of what steps they take as an end-user, or the respondent did not mind if their personal information was kept private or not, these attitudes may have impacted how they answered the survey questions.

IMPLICATIONS

For Businesses

Beyond what these results mean for the end user, there are implications of this study that can be drawn pertaining to the entities collecting and utilizing the data as well. App developers, data analytics companies, and even the smartphone companies themselves (Apple, Google, and Blackberry) should be looking to capitalize on the plethora of app users willing to give up personal data. The collection and usage of that personal data should be conducted in a secure and legal way, but the possibilities for what can be done with this customer data are boundless. If users are made aware and consent to giving up their personal data, complete customer profiles can be created that allow companies to learn the purchasing habits of their customers. Targeted advertisements and promotions can be sent to those who will actually see some tangible benefit in using the promotions, rather than having a company waste money on customers that will not adopt their products. Even more so, companies can offer direct benefits to their customers as well through the appropriate use of data. Making applications more accessible and convenient for the end user in exchange for their personal data creates shared value for both parties, and can lead to the creation of a loyal customer base.

All of the data privacy practices by companies must be carried out legally and without any adverse intentions towards the end user. One of the first steps in reaching a conducive environment where the end user feels comfortable giving up personal data is to simplify the process. Application developers should make it explicit to end users what their application is asking access to, and what it will do with the data it collects. This information should be presented in a clear and concise manner in conjunction with the end user downloading the application. Similar to Blackberry's approach to keeping their end users secure and more privacy aware, the practice of complete transparency will be necessary to build the end-users' trust. As

the study results show, 90.4% of respondents do not read the privacy policy in its entirety when they download an application. With this knowledge, it is naïve of companies to be under the impression that the users of their application are fully aware of what the application is doing. The need for shorter, less legalese filled privacy policies with a clear explanation of the app's collection practices and the usage and sharing components of the collected data should be the new standard for mobile applications.

For Individuals

As mobile applications draw almost 90% of all time spent on smartphones, a multitude of implications arise from what this study means to the everyday user (Rudolph, 2015).One of the main concerns is if there are specific applications or groups of applications that the everyday end user should avoid downloading if they wish to keep their personal information private. Unfortunately for those looking for a catch-all answer, these considerations must be done on an individual basis, both by the user as well as by the individual application they are downloading. At the current state of how mobile application platforms present to the end user what personal information they are giving up when they download specific mobile applications, the burden is still on the end user to know what information they are giving up. The end users must become more knowledgeable and aware of the type of personal information they are willing to give up. There are no specific applications to avoid downloading, but the end users must be aware of what the applications do on the back-end. Commonly accepted best practices regarding maintaining privacy when downloading mobile applications must be followed. The first step is to have more end users read the entirety of the privacy policies of the mobile applications they download. From this survey, 94.3% of respondents said they do not read the entire privacy policy every time they download an application. This has significant negative implications for the more

privacy conscious user, as they are using applications without even having read and been made aware of the access they are giving to the app. Additionally, more users should take it upon themselves to discriminately enable and disable privacy controls depending on the app on a regular basis. By taking the time to look at what information each of their applications is requesting access to and, in most cases, having the ability to either allow or deny the app's access to this data, users can become more privacy conscious and privacy literate. Much of this could be accomplished with a basic smartphone data privacy crash course, similar to what Slusky and Patrow-Navid (2012) suggested. A smartphone personal information privacy course could be integrated into high school education or even at the university level. The course should include topics such as what the common best practices are regarding privacy on smartphones, where to find the privacy controls on the users' smartphone, how to use those privacy controls, as well as explanations of common collection practices employed by mobile app developers. In addition to using the curriculum to make users more privacy aware, education should also focus on why mobile application developers are trying to collect their users' personal data in the first place. The education of end users will help create a more comprehensive understanding of why privacy is important, as well as what the consequences are for both the users and the parties collecting the data.

FUTURE RESEARCH

The implications of this study are interesting for the rapidly expanding smartphone mobile application field. Due to the low Cronbach's Alpha reliability measures of the privacy subscale comprehensive statements about the inter-related disconnects between users' privacy attitudes, knowledge, and practices as well as the connections between various socio-demographic variables and users' privacy attitudes, knowledge, and practices could not be made.

While relationships could be addressed between individual questions, further research should continue to look at the attitude, knowledge, and privacy constructs as a whole. The evidence is there to imply that there may be disconnects, but more studies will help solidify the conjecture.

Another area of the study from which further research should be conducted is about the current privacy regulations put in place by the FTC, Apple, and Android. Regarding the Knowledge Privacy Regulations questions, there were essentially no correlations among the 5 demographic variables (only -0.128 and -0.106 negative correlations at the 0.05 level for Age and Education Level for Android's Guidelines). There was no consensus either agreeing or disagreeing with the statements that the U.S. Federal Guidelines, the Apple App Store Guidelines, nor the Android's Android Marketplace Guidelines sufficiently protected mobile app user privacy. What does this say about those regulations then? Research should be conducted to see why respondents did not have significant reactions to these regulations. Is it possible that most respondents are apathetic towards what regulations these bodies put in place? Or is it possible that users do not fully understand the regulations, either due to their complex legal nature or even the fundamental reason why there are regulations in the first place? Finally, should the people in charge of creating and maintaining these regulations look to what the European Union is pushing for with the "Right to be Forgotten" and how this concept can apply to mobile apps as well? Overall there is a need to have more concrete data regarding users' attitudes and knowledge of the regulations that are currently governing the enormous smartphone application industry.

APPENDIX

Mobile Apps: Survey

CONSENT STATEMENT

This research project is being conducted by Brien Twomey (Undergraduate Honors Student; Business Information Systems; Texas Christian University; Study Investigator) and Beata M. Jones, Ph.D. (Honors Faculty Fellow and Professor of Business Information Systems; Neeley School of Business; Texas Christian University; Principal Investigator). You are invited to participate in this research project concerning mobile application privacy.

Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. Should you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalized.

This procedure involves filling out an online 40-question survey that will take no more than 15 minutes to complete. Your responses will be confidential and we do not collect identifying information such as your name or IP address. Beyond some fundamental demographic questions, the survey asks questions about your use of mobile applications, your knowledge of general data collection practices employed by commonly downloaded mobile applications, and your perceptions of those practices.

We will keep all information confidential. All data will be stored in a password protected electronic format. The results of this study will be used for scholarly and research purposes.
If you have any questions about the research study, please contact:
1. Brien Twomey by phone at (512) 431-1822 or via email at brien.twomey@tcu.edu
2. Beata M. Jones by phone at (817) 257-6948 or via email at b.jones@tcu.edu

By agreeing to participate in this study, you agree to the following:

- You are free to withdraw from the study at any time without penalty.
- You have read and understand all of the above material.

❍ Yes, I agree to consent and participate
❍ No, I disagree and do not consent to participate

1) Do you have a personal smartphone? (A "smartphone" is a mobile phone that allows its users to download mobile applications and browse the Internet.)

- ❍ Yes
- ❍ No

2) What type of personal smartphone do you have?

- ❍ Apple iOS Phone
- ❍ Android Phone
- ❍ Other _____

Please respond to the following statements with how you are feeling at this moment.

3) "Privacy, while using mobile applications on my personal smartphone, is important to me."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

4) "I believe I am totally anonymous using mobile applications on my smartphone."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

5) "I believe mobile application developers provide necessary and adequate protection of my personal data."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

Please respond to the following statements with how you are feeling at this moment.

6) "I know what personally identifiable information about me each of my mobile applications collects."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

7) "I know how to use privacy controls on my smartphone for my mobile applications."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

8) "When I delete a mobile application from my smartphone that I previously downloaded, the information collected by that application is also deleted."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

9) "It is good practice to read the entirety of the privacy policy when downloading a mobile application onto a smartphone."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

10) "It is good practice to enable and disable Location Tracking on a smartphone depending on the mobile application."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

11) When was the last time you downloaded a mobile application?

❍ Within the last week ❍ Within the last month ❍ Within the last year ❍ Over a year ago ❍ I have never downloaded a mobile application

12) Have you ever "jailbroken" or "rooted" your smartphone? (i.e., removed software restrictions imposed by the smartphone's operating system)

❍ Yes ❍ No ❍ I don't know

13) Have you ever enabled or disabled Location Tracking on your phone?

❍ Yes ❍ No ❍ I don't know

14) Have you ever enabled or disabled privacy controls on your smartphone?

❍ Yes ❍ No ❍ I don't know

Please respond to the following statements with how you are feeling at this moment.

15) "Every time I download a mobile application, I read the privacy policy in its entirety."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

16) "I enable and disable Location Tracking on my smartphone depending on the mobile application."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

17) "I enable and disable privacy controls on my smartphone depending on the mobile application."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

18) What personal information would you be willing to share while using a free mobile application? Please check all that apply.

- ❑ Calendar events
- ❑ Call log
- ❑ Contacts on your phone
- ❑ Credit Card information
- ❑ Full name
- ❑ Personal Email
- ❑ Personal Phone Number
- ❑ Photos on your phone
- ❑ Physical Location
- ❑ Social Security Number
- ❑ Text messages
- ❑ Other ID information
- ❑ None of the above

Please respond to the following statements with how you are feeling at this moment.

19) "I believe it is OK for a mobile application to collect personally identifiable information from its users, if the application is free."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

20) "I believe it is OK for a mobile application to collect and share with third parties (advertisers, application developers, etc.) personally identifiable information from their users, if the application is free."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

21) "Most of the time, I would be willing to pay money for a mobile application to remain anonymous while using the application."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

22) "I am willing to give up some privacy of my personal data in exchange for increased convenience and functionality from my downloaded mobile applications."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

23) Do you currently have the application "Google Maps" downloaded on your smartphone?

- ❍ Yes
- ❍ No

24) Do you use "Google Maps" on your smartphone?

- ❍ Yes
- ❍ No

Please respond to the following statements with how you are feeling at this moment.

25) How concerned are you about your privacy using "Google Maps"?

❍ Not at all ❍ Hardly ❍ Neutral ❍ Somewhat ❍ A lot

26) How concerned are you about Location Tracking using "Google Maps"?

❍ Not at all ❍ Hardly ❍ Neutral ❍ Somewhat ❍ A lot

Please respond to the following statement with how you are feeling at this moment.

27) Knowing that "Google Maps" uses Location Tracking, how likely are you to use this application in the future?

❍ A lot less ❍ Less than before ❍ No change ❍ More than before ❍ A lot more

28) Do you currently have the application "Snapchat" downloaded on your smartphone?

❍ Yes
❍ No

29) Do you use "Snapchat" on your smartphone?

❍ Yes
❍ No

Please respond to the following statement with how you are feeling at this moment.

30) How concerned are you about your privacy using "Snapchat"?

❍ Not at all ❍ Hardly ❍ Neutral ❍ Somewhat ❍ A lot

31) Which of the following do you believe "Snapchat" tracks on your smartphone? Please check all that apply.

❑ Your contact's information in your phone's contact list
❑ Your email address
❑ Your legal name
❑ Your photos on your smartphone
❑ Your physical location
❑ Your web browsing history
❑ None of the above

Please respond to the following statements with how you are feeling at this moment.

32) Knowing that "Snapchat" collects email address, web browsing history, physical location, photos on your smartphone, your legal name, names as well as contact information for everyone in your phone's contact list, how likely are you to use "Snapchat" in the future?

❍ A lot less ❍ Less than before ❍ No change ❍ More than before ❍ A lot more

Please respond to the following statements with how you are feeling at this moment.

33) Under U.S. National Guidelines, application developers must provide:

- A description of the **types of personal information** kept by the application developer
- **The process** by which a consumer may request a change to how their personal information is stored, if available
- A notification when the **privacy policy is updated**

After reading these guidelines, how would you respond to the following statement? "I believe the U.S. National Guidelines sufficiently protect mobile application user privacy."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

34) Under Apple's App Store Guidelines, application developers must provide:

- Clear and complete information to users regarding **collection, use and disclosure of user data**
- Steps taken to protect users' personal data from **unauthorized use** or disclosure
- A way to **cease the collection of personal data** from the user if the user ceases to consent or affirmatively revokes consent for the application's collection or disclosure of the user's personal data
- A **link to the privacy policy** on the App Store

After reading these guidelines, how would you respond to the following statement? "I believe the Apple's App Store Guidelines sufficiently protect mobile application user privacy."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

35) Under Android's Android Marketplace Guidelines, application developers must:

- Protect the **privacy** and **legal rights** of users
- Make the user aware if the application accesses or **captures users' personal information**
- Provide a **legally adequate** privacy notice to users

After reading these guidelines, how would you respond to the following statement? "I believe the Android's Android Marketplace Guidelines sufficiently protect mobile application user privacy."

❍ Strongly Disagree ❍ Disagree ❍ Neither Agree nor Disagree ❍ Agree ❍ Strongly Agree

Demographic Questions:

36) What is your gender?

❍ Male
❍ Female

37) What is your age?

❍ Under 18	❍ 18	❍ 19	❍ 20	❍ 21	❍ 22
❍ 23	❍ 24	❍ 25	❍ 26	❍ 27	❍ 28
❍ 29	❍ 30	❍ 31	❍ 32	❍ 33	❍ 34
❍ 35	❍ 36	❍ 37	❍ 38	❍ 39	❍ 40
❍ 41	❍ 42	❍ 43	❍ 44	❍ 45	❍ 46
❍ 47	❍ 48	❍ 49	❍ 50	❍ 51	❍ 52
❍ 53	❍ 54	❍ 55	❍ 56	❍ 57	❍ 58
❍ 59	❍ 60	❍ 61	❍ 62	❍ 63	❍ 64
❍ 65	❍ 66	❍ 67	❍ 68	❍ 69	❍ 70
❍ 71	❍ 72	❍ 73	❍ 74	❍ 75	❍ 76
❍ 77	❍ 78	❍ 79	❍ 80	❍ 81	❍ 82
❍ 83	❍ 84	❍ 85	❍ Over 85		

38) What is the highest level of education you have completed?

❍ High-School ❍ Some college ❍ Bachelor Degree ❍ Master Degree ❍ Doctoral Degree

39) Is your college education in an Information Technology or Computer Science-related field?

❍ Yes
❍ No

40) How many years of Information Technology-related work experience do you have?

❍ 0
❍ 1-2
❍ 3-4
❍ 5-6
❍ 7-8
❍ 9-10
❍ More than 10

Thank you for completing the survey!

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1), 26-33.

Agarwal, B. (2000). Conceptualising Environmental Collective Action: Why Gender Matters. *Cambridge Journal of Economics*, 24, 283-310.

AndroLib (2014) *Distribution of free and paid apps in Android market.* Retrieved October 26, 2015, from http://www.androlib.com/appstatsfreepaid.aspx

App Store, (2015). *App Store Review Guidelines.* Retrieved November 21, 2015, from https://developer.apple.com/app-store/review/guidelines/#apple-pay

Appthority (2014), *Appthority Summer 2014 Reputation Report.* Retrieved November 21, 201, from http://www.nomasis.ch/fileadmin/user_upload/flyer/produkte/Appthority/App_reputation_report.pdf

Barnes, S. B. (2006, September 4). A Privacy Paradox: Social Networking in the United States. *First Monday*, 11(9). Retrieved from http://firstmonday.org/article/view/1394/1312_2

Chaney, P. (2009). *The Digital Handshake: Seven Proven Strategies to Grow Your Business Using Social Media*. New Jersey: John Wiley & Son.

Constantinos, A. (2015, April 1). *The Value of Privacy: Evidence From the Use of Mobile Devices for Traveler Information Systems*, Journal of Intelligent Transportation Systems (ISSN: 1547-2450), Vol. 19 No. 2

Dwoskin, E. (2016, January 14). *New Study Highlights Privacy Gap Between Consumers and Tech Vendors*. Retrieved from Wall Street Journal: http://blogs.wsj.com/digits/2016/01/14/new-study-highlights-privacy-gap-between-consumers-and-tech-vendors/

eMarketer (2014, December 11). *2 Billion Consumers Worldwide to Get Smart(phones) by 2016.* Retrieved November 21, 2015, from http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

Ericsson (2015, June). *Ericsson Mobility Report: On the Pulse of the Networked Society* Retrieved November 21, 2015, from http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf

European Commission (2012, June 10). *Why do we need an EU Data Protection Reform?* Retrieved November 1, 2015, from http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

Federal Trade Commission (2013, February 22) *HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers* [Press Release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile

Frenkel, K. A. (2014). Free and Paid Apps Pose Risks for the Enterprise. *CIO Insight*, 1.

Friedman, M. (1975). *There's No Such Thing As a Free Lunch.* LaSalle, Illinois: Open Court.

Fry, R. (2015, January 16). *This year, Millennials will overtake Baby Boomers*. Retrieved from Pew Research Center: http://www.pewresearch.org/fact-tank/2015/01/16/this-year-millennials-will-overtake-baby-boomers/

Graeff, T. R., & Harmon, S. (2002). Collecting and Using Personal Data: Consumers' Awareness and Concerns. *Journal of Consumer Marketing*, 19(4/5), 302-318.

Gralla, P., Sacco, A., & Faas, R. (2011, July 11). *Smartphone apps: Is your privacy protected?* Retrieved September 28, 2015, from http://www.computerworld.com/article/2509878/data-privacy/smartphone-apps--is-your-privacy-protected-.html

Hale II, R.V. (2013). *Recent Developments in Mobile Privacy Law and Regulation.* Business Lawyer, vol. 69, no. 1, pg. 237-243.

Harris, M. A., Furnell, S., & Patten, K. (2014). Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals. *Journal of Information Privacy and Security*, 186-202.

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy & Security*, 31.

Kang M, Wu L, and Yang S, (2015, April) *What Makes Users Buy Paid Smartphone Applications? Examining App, Personal, and Social Influences*, Journal of Internet Banking and Commerce, vol. 20, no. 1

Krasnow, M. J. (2013). *Mobile Application and Website Privacy Policies - It's Not Just About California*. Financial Executive, vol. 29, no. 2, pg. 65-66.

Krugman, P. R., and R. Wells. (2012). *Microeconomics,* 3rd ed. New York: Worth Publishers.

Leslie R (2015, September 26). *As Privacy Fades, Your Identify is the New Money* Retrieved from http://m.livescience.com/52315-your-online-identity-has-value-but-who-profits-from-it.html?utm_source=dlvr.it&utm_medium=twitter

Llamas, R., Reith, R., & Nagamine, K. (2016). *Smartphone OS Market Share, 2015 Q2*. Retrieved from International Data Corporation (IDC): http://www.idc.com/prodserv/smartphone-os-market-share.jsp

McCarthy, N. (2014, October 29*). Mobile App Usage By The Numbers*. Retrieved October 19, 2015. http://www.forbes.com/sites/niallmccarthy/2014/10/29/mobile-app-usage-by-the-numbers-infographic/

Melson, B (2015, July). *Protecting Privacy and Security in Software and Mobile Apps.* Wireless Design & Development. Retrieved September 14, 2015. vol. 23, no. 4, pg. 20-21.

Nielson (2014, July 1) *Smartphones: So Many Apps, So Much Time*. Retrieved November 1, 2015, from http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html

O'Brien, K. (2012, October 28). *Data-Gathering via Apps Presents a Gray Legal Area*. Retrieved November 21, 2015, from http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?_r=0

Office of The Attorney General. (2012). *Joint Statement of Principles*. Sacramento, California: State of California Office of The Attorney General.

Plangger K and Watson R (2015) *Balancing customer privacy, secrets, and surveillance: Insights and management* Business Horizons, Kelley School of Business Indiana University, vol. 58, p. 625-633

Purcell, K., Brenner, J., & Rainie, L. (2012, March 9). *Search Engine Use 2012*. Retrieved from Pew Research Center: http://www.pewinternet.org/2012/03/09/search-engine-use-2012/

Ranger, S. (2014) *Apple's App Store downloads top $10bn: battle for developers' hearts and minds heats up.* Retrieved October 26, 2014, from http://www.zdnet.com/apples-app-storedownloads-top-10bn-battle-for-developers-hearts-and-minds-heats-up-7000024884/

Robertson, J. (2014, January 29). *Leaked docs: NSA uses 'Candy Crush,' 'Angry Birds' to Spy.* Retrieved from SF Gate - San Francisco Chronicle: http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php

Rudolph, S. (2015, June 15*). Mobile Apps Usage – Statistics and Trends [Infographic]*. Retrieved November 1, 2015, from http://www.business2community.com/infographics/mobile-apps-usage-statistics-trends-infographic-01248837#P8P46im6hEDbADmr.97

Sacco, A. (2011, June 13). *How to Manage BlackBerry Application Permissions*. Retrieved November 1, 2015, from http://www.cio.com/article/2407222/mobile/how-to-manage-blackberry-application-permissions.html

Sheehan, K. B. (1999). An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors. *Journal Of Interactive Marketing*, 13(4), 24-38.

Shilton, K. (2009, November). Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 52(11), 48-53.

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security*, 3.

Strain, M. (2015, February 13). *1983 to Today: A History of Mobile Apps*. Retrieved November 1, 2015, from http://www.theguardian.com/media-network/2015/feb/13/history-mobile-apps-future-interactive-timeline

Summerfield, J. (2015). *Mobile Website vs. Mobile App (Application) – Which is Best for Your Organization?* Retrieved November 21, 2015, from http://www.hswsolutions.com/services/mobile-web-development/mobile-website-vs-apps/

The Computer & Internet Lawyer (2014, August). *Snapchat Settles FTC Complaint that It Deceived Customers*. vol 31, no. 8, pg. 23-24.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003, September). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478.