# Mobile Application Installation Influences: Have Mobile Device Users Become Desensitized to Excessive Permission Requests?

***Completed Research Paper***

**Mark A. Harris**
University of South Carolina
markaharris@sc.edu

**Robert Brookshire**
University of South Carolina
brookshire@sc.edu

**Karen P. Patten**
University of South Carolina
pattenk@sc.edu

**Elizabeth A. Regan**
University of South Carolina
earegan@mailbox.sc.edu

## Abstract

The purpose of this study was to investigate constructs that influence consumers before deciding to download and install mobile device applications. These constructs include market trust, risk perceptions, privacy concerns, and precautions. Through a survey, a prediction model was created that attempts to predict whether respondents would download applications asking for excessive permissions. The model results indicate those that take more precautions are less likely to download apps requesting excessive permissions. But the precautions taken by participants may be inadequate and may leave consumers with a false since of security. Another key finding is that some consumers may have become desensitized to excessive permissions. These consumers knowingly install apps requesting excessive permissions for reasons such as nothing bad has happened to them before or the app usually has a good reason for requesting questionable permissions. The security implications of permission desensitization and inadequate precautions are discussed.

**Keywords**

Mobile device security, permission requests, mobile apps, application installation, security precautions

## Introduction

Smart mobile devices, including smartphones and tablets, have been rapidly increasing in worldwide sales over the last few years. For the first time, smartphone sales surpassed feature phone sales, accounting for 57.6% of total sales in the fourth quarter of 2013 (Gartner 2014a). The expectations are even greater for 2014, with smartphone sales predicted to reach 1.9 billion units and tablet sales predicted to reach just over 250 million units and outsell PC's by 2015 (Gartner 2014c). Google's Android operating system remains the most popular and was utilized on 78.4% of all of the smartphones sold in 2013, compared to just 15.6% for Apple's iOS, 3.2% for Microsoft's Windows Mobile, and 1.9% for Blackberry (Gartner 2014a). In 2014, Android smartphone sales are predicted to approach one billion units (Gartner 2014c). Across all smart mobile device platforms, Google's Android operating system and Apple's iOS are the most popular.

The app markets associated with these two platforms are Google's Google Play market and Apple's App Store, with each containing over 1 million downloadable applications (Appthority 2014). Gartner predicts mobile application downloads will reach 139 billion in 2014, up from just 64 billion in 2012 (Gartner 2014b). The biggest risk to consumers that download and install mobile applications is malicious software, otherwise known as malware. Mobile device malware has been on the rise, especially with Android devices, which has seen a 600% increase in malware in 2013 compared to the year before (IBM 2013). In addition, 99% of all detected mobile malware in 2013 was written for Android and 98% of that malware targeted SMS text messaging (Cisco 2014). However, Apple applications are not without risk. In a recent report on Google Play's and Apple App Store's top 100 paid apps and top 100 free apps, iOS apps were found to be more risky than Android apps (Appthority 2014). In addition, the report highlighted that 95% of the top free Android and iOS apps and 80% of paid apps exhibited at least one risky behavior. Free apps are considered more risky and more likely to share data with ad networks, access user contact lists, and allow location tracking (Appthority 2014). In a different report from October 2013, it was reported that there was 1 million malware and high-risk applications in the wild (TrendMicro 2014). Seventy-five percent were of the malicious form and the other 25% ran dubious routines, such as utilizing adware.

When it comes to risk to consumers, malware is not the only thing to worry about. Consumers also need to be aware of exploitation from in-app-purchases (IAP) and the sharing of their personal data. For revenue, developers earn a percentage of the app's initial cost, which is nothing for free apps and insignificant for most paid apps, since most paid apps are relatively inexpensive. Therefore, many developers offer in-app-purchases (IAP), where a user downloads a free or inexpensive app, uses it, and then pays for additional app content if they like it. IAP is expected to account for nearly 50% of all app store revenue by 2017, with Apple achieving a higher percentage than other app stores (Gartner 2014b). However, IAP can exploit consumers in several ways. One is that the consumer can feel duped by purchasing an app only to find out it has very limited functionality without the need to pay more for additional content or features. At the time of initial purchase, it is not in the developer's best interest to disclose how much of the app is functional and how much additional functionality costs. Another way consumers can be exploited by IAP is when charges for purchases are made to the consumer's associated credit card without the consumer's knowledge. In a recent FTC settlement, Apple agreed to refund duped consumers $32.5 million for purchases made by children unbeknownst to parents (FTC 2014). Under the agreement, Apple agreed to change its billing practices and ensure it has obtained express, informed consent before charging consumers. With the predicted increase of IAP across all markets, consumers need to be given more information about app functionality and the cost structure of additional content before downloading.

Another way consumers can be exploited is from the legal sharing of their personal information with legitimate advertising networks and analytics companies (Appthority 2014). For example, an app may have permission to read the user's contacts, account names, phone number, GPS location, and more. Some of this information may be shared with 3rd parties, thus generating revenue for the developer. This legal way of sharing consumer's personal information is different than the before mentioned malware that might illegally obtain consumer's information for dubious purposes. However, there are legal constraints, such as disclosing the potential use of such data in user agreements or some other unavoidable disclosure method, as seen in a 2013 case where the FTC won judgment over an app developer for collecting GPS location and sharing it with a 3rd party (Hoffman 2013). Unavoidable disclosure means the consumer cannot avoid being told how their data will be used by the developer. Guidance from this FTC case suggests consumers agreeing to app permissions before app installation is not enough to justify unavoidable disclosure of information usage. Stated differently, agreeing to app permissions before installation does not tell the consumer enough about how their data will be used. Since this case is very recent at the time of this writing, it has yet to be seen if app developers will chose to display privacy messages in some form of unavoidable discloser or chose to hide them in lengthy user agreements, either of which would seem to satisfy the FTC.

Many mobile device users do not realize apps can legally collect personal data and are not considered malware and thus rejected from the app markets as such. If a user agrees to the apps user agreement and

data sharing is disclosed in said agreement, it is potentially legal for the developer to share the user's information for legitimate advertising and analytics. Users that do not take the time to read and understand app permission requests and user agreements may not realize how their personal information is being used by 3rd parties.

With the increase of malware, IAP, permission requests, and risky applications, users should take precautions when downloading and installing applications. The purpose of this study is investigate what influences consumers before deciding to download and install a mobile application. Several constructs are investigated, including market trust, risk perceptions, privacy concerns, and precautions.

The next section describes related work, followed by the survey description. The following analysis and results section includes the two prediction models. The last two sections are the discussion and conclusion.

## Precautions and Related Work

In this study, we investigate several actions consumers perceive as precautions they may take before downloading and installing a mobile application. One is to review and understand the permission requests, as recommended by researchers and government agencies (FCC 2014; Harris & Patten 2014; IC3 2012). While other platforms also use permissions, permission requests and malware are more prevalent on the Android platform. Every time a consumer downloads and begins installing an application, a list of permissions needed by the application are displayed for the consumer's consent. This list of permissions tells the consumer what services or data the app is requesting to function. However, it is important for the consumer to match each permission request with an actual feature of the app and determine if it is necessary. For example, if an app asks for GPS location, what feature in the app would use location and is it necessary? If it is a map app, then that makes sense. If it is a solitaire card game, then asking for GPS location is excessive and not warranted, even if the game has a reason for needing the feature. Apps with excessive features is one reason apps ask for excessive permissions. Consumers need to decide if excessive features and permissions is really necessary. Excessive permissions are defined as requested permissions beyond what is minimally necessary for the app to function. What is considered excessive changes from app to app. The apps intended purpose will influence what permissions are minimally necessary and excessive features can lead to excessive permissions. Consumers should also read the app's description, as some developers explain their permission requests. Carefully reading app permissions is important and research has shown that popular applications, free applications, and mature content applications request more permissions than average (Chia et al. 2012). While permissions are displayed to inform consumers, research has shown using app permissions as a precaution has not been an effective security measure because many consumers simply do not read them (Felt et al. 2012; Mylonas et al. 2013) or do not understand them (Benton et al. 2013; Kelley et al. 2012).

Another action consumers often take as a security precaution is to only install apps from trusted sources, as suggested by researchers and agencies (FCC 2014; Harris & Patten 2014; IC3 2012). While malware can be found on traditional markets, most malware is found on 3rd party markets (Juniper 2013). Traditional markets are defined as those affiliated with the device's operating system, like Google's Google Play and Apple's App Store, and third party markets are defined as any app market outside of the operating system's affiliated market. For Android users, accessing 3rd party markets is as easy as checking a security setting in the system settings. This freedom Android gives their users is one of the reasons malware is more prevalent on the Android platform. Apple users must jailbreak their devices in order to access 3rd party markets, which is a much more difficult process and one reason why Apple's iOS platform is considered safer than Android. When it comes to trusting traditional markets, research suggests that most consumers trust the official markets associated with their platform to deliver safe applications (Kelley et al. 2012; Mylonas et al. 2013). In this paper, we also investigate how much consumers trust the major platform markets as well as 3rd party markets.

Looking at the star ratings and reading reviews are other actions some consumers take to gauge security of the app. In one study, participants relied heavily on star ratings, full text reviews, and even word of mouth because they were better understood and trusted than permissions (Kelley et al. 2012). However, research has not shown these actions as reliable security methods, such as a 2012 study that concluded that community ratings used in app markets are not reliable indicators of app risks and ratings and are based on functional aspects like features and performance rather than risks (Chia et al. 2012).

Another recommended precaution is that consumers investigate and read reviews about the developers themselves (IC3, 2012). However, no research could be found that correlated developer reviews with the riskiness of the apps they develop. In this study, we ask participants if they research the developer before downloading an application.

Several theories may help explain what influences consumers before deciding to download and install mobile applications. In related information technology usage work, the Technology Acceptance Model (TAM) and Flow Theory were used to explain user's behaviors when visiting Web sites (Koufaris, 2002). The authors investigated the effects of emotional and cognitive responses when visiting Web sites and determined enjoyment and perceived usefulness predicted intention. In a more elaborate research study, Lee (2009) used TAM, the Theory of Planned Behavior, and Risk Theory to investigate the factors influencing the adoption of Internet banking. Lee's model integrated perceived benefit with five risk facets - financial, security/privacy, performance, social, and time risk. One result was that the intention to use the technology was adversely affected mainly by the security/privacy risk. In other research, shared values and social trust were shown to have a positive influence on perceived benefits and negative impact on perceived risks (Siegrist, et al. 2000). The author's results indicated that social trust was a key predictive factor of the perceived risks and benefits of a technology and supported the Salient Values Similarity Theory of Social Trust.

## Survey

To assess what influences consumers before downloading and installing mobile applications, a 34 question survey was given to in late 2013 and again in spring 2014. One hundred fifty-five subjects responded to the survey, as seen in Table 1. Their ages ranged from 17 to 55, with a mean of 23.57. One hundred eighteen were male and 34 were female, while three declined to give their gender. One hundred thirty-one of the respondents were or had been technology majors, studying information technology or computer science.

| | Male | Female | Declined | Total |
|---|---|---|---|---|
| Number of Participants | 118 | 34 | 3 | 155 |
| Studied Technology | 103 | 28 | 0 | 131 |

**Table 1. Descriptive Statistics**

## Analysis and Results

The respondents were asked to specify the operating system on their smartphone or tablet. Ninety reported currently using Apple's iOS, 65 reported currently using Google's Android, and six said they currently used both Android and iOS. Respondents were asked to report the number of applications they had downloaded. This ranged from none to 100, with a mean of 34.7.

Respondents were asked whether they had a rooted or jailbroken device, and 29 responded affirmatively, while 121 said they did not have such a device and five respondents did not know. There was no association

between having a rooted device and the operating system used, nor was there an association with the user's gender.

Slightly fewer than half, 77 respondents, reported having been a victim of mobile device malicious software (malware), including viruses or worms, with 78 saying they had not been victims. Once again, there was no association with being a victim of malware and the operating system used. However, those with rooted devices were more likely to be victims of malware (chi square=10.341, df=1, p=0.006), and female respondents were less likely report being malware victims (chi square=8.411, df=1, p=0.004).

We asked respondents to report which markets they had used to download applications. One hundred three said they had used Apple's App Store, while 73 said they had used Google's Google Play. Eighteen respondents had used Amazon's App Store, while only four had used the Windows Phone App Store. Nine respondents reported using other third-party markets. Among the Apple market customers, 17 were Android users and 89 were iOS users; among the Google market customers, 63 were Android users and 14 were iOS users. The Windows market customers were evenly divided between iOS and Android users, with two of each. Fifteen of the Amazon customers were Android users and eight were iOS users. Five of the third party market customers were Android users, and six were iOS users, which would indicate jailbroken devices.

### *Ratings of Application Markets*

We asked respondents to rate the five application markets in five different areas: protecting their personal information, such as credit card data; charging the correct amount for an application; limiting applications from asking for excessive permissions; selling applications that perform as advertised; and protecting the user from malware. The ratings were on a five-point scale, with 1 indicating "Not Trustworthy" and 5 indicating "Very Trustworthy." We then summed these evaluations to get an overall trust score for each market, ranging from 5 to 25.

In general, the markets were evaluated similarly. The Apple and Google markets had average trust ratings of 17.7 and 17.2, respectively. The Amazon market had an average rating of 17.1, while the Microsoft market's average rating was 16.4. Third party markets received an average trust rating of 12.95. Multivariate tests (F=31.194, df=4,148, p<0.001) show that the Apple, Amazon, and Google markets were trusted significantly more than the Microsoft market (p=0.001, 0.017, and 0.014, respectively), and that the third party markets were significantly less trusted than all the others (p<0.001 for all paired comparisons).

Users of Apple's iOS operating system evaluated third-party markets slightly higher than non-iOS users (t=2.131, df=150, p=0.035). Android users evaluated the Apple market lower than non-Android users (t=-2.142, df=150, p=0.034), and also evaluated third party markets lower (t=-2.953, df=150, p=0.004).

### *Risk and Precautions when Downloading Applications*

We were interested in gauging the subjects' perception of risk when downloading applications. Survey respondents indicated that they were concerned with applications obtaining their personal information, with 87% agreeing or strongly agreeing that they had this concern. The vast majority were also concerned about the possibility of malicious software in the applications they downloaded, with 82% agreeing or strongly agreeing that they had this concern.

Respondents also said they were not likely to put up with risk when downloading free applications. Only 27% agreed and 56% disagreed or strongly disagreed that they were willing to put up with some risk. They were more likely to put up with risk when downloading applications that met their needs, with 43% agreeing

or strongly agreeing with this statement, and 42% disagreeing or strongly disagreeing. Table 2 shows the responses to the questions we used to measure their perception of risk.

| | Strongly Disagree | Disagree | Neither Agree nor Disagree | Agree | Strongly Agree | No response |
|---|---|---|---|---|---|---|
| I am concerned with applications obtaining my personal information. | 0 | 6 | 13 | 77 | 56 | 3 |
| I am concerned about malicious software in downloaded applications. | 1 | 9 | 18 | 74 | 50 | 3 |
| I am willing to put up with some risk to get a free application. | 41 | 44 | 26 | 40 | 1 | 3 |
| I am willing to put up with some risk to get an application that meets my needs. | 27 | 37 | 23 | 61 | 4 | 3 |

**Table 2. Perceptions of Risk in Downloading Applications**

We asked survey respondents about the kinds of precautions they took when downloading applications, including whether they read the reviews of applications, if they investigate the application's developers, whether they read the permissions requested by the application, or whether they take other precautions. One hundred twenty-eight respondents said they read the application's reviews, 80 said they read the requested permissions, and 39 said they investigated the application's developer. Six said they take other precautions, including "common sense," "reading tech blogs," and "checking the number of downloads."

We counted the number of precautions each respondent took. Twenty-one took no precautions at all, while 47 took at one precaution. Fifty-five said they took two of the precautions, while 32 took three precautions. There was no association between the number of precautions taken and whether the respondent had a rooted device or was a victim of malware. IOS users were more likely than non-iOS users to take no precautions at all, with 19% taking no precautions (chi square=10.902, df=3, p=0.012, Somer's d=-.260). Android users were slightly more likely to take more precautions (chi square=13.855, df=3, p=0.002, Somer's d=0.319).

### *Applications Asking for Permissions*

We asked survey respondents if they were likely to abort the installation of an application that asked for excessive permissions, such as asking to access their contacts, track their locations, or sending icons or badges. Seventy-five percent of those responding to this question (n=152) said that they agreed or strongly agreed that they would abort the installation of this kind of application, while only eleven percent of respondents disagreed or strongly disagreed.

We asked respondents under what circumstances they would ignore an application asking for excessive permissions. Table 3 shows their responses to several scenarios they were presented. The circumstances under which a majority of respondents said they would ignore permission requests were if they trusted the

market, if the permission requests looked OK, and if they really wanted the application. They were less likely to ignore the permission requests if nothing bad had happened to them before, if they did not understand the requests, or if it took too long to read the requests. As Table 3 shows, however, sizeable minorities of respondents would ignore permission requests under these circumstances.

| | Strongly Disagree | Disagree | Neither Agree nor Disagree | Agree | Strongly Agree | No Response |
|---|---|---|---|---|---|---|
| I trust the market. | 4 | 28 | 32 | 68 | 20 | 3 |
| Nothing bad has happened to me before. | 7 | 41 | 25 | 65 | 14 | 3 |
| I do not understand the permission requests. | 17 | 57 | 35 | 38 | 5 | 3 |
| It takes too long to read them. | 16 | 38 | 34 | 53 | 11 | 3 |
| Whenever I read them, the always look OK. | 7 | 31 | 47 | 54 | 13 | 3 |
| I really want the application. | 9 | 30 | 38 | 61 | 14 | 3 |

**Table 3. Circumstances Under Which Respondents Ignore Permission Requests**

We asked survey respondents if they had ever installed an application that they believed asked for excessive permissions. Seventy-eight respondents (50%) said they had installed such applications anyway, while 74 (48%) said they had not; three respondents did not answer. There was no association between installing these applications and the respondent's gender, or whether the respondent had a rooted device, was a victim of malware, was an IOS user, or was an Android user.

For those respondents who had installed applications asking for excessive permissions, we asked further questions to see what would prompt them to do so. Of the 78 who installed such applications, 56 (72%) said they trusted the market from which they downloaded the application, and 49 (63%) said there was often a good reason for the application to request the permissions. Another 42 respondents (54%) said they just wanted the application and did not care about the permission requests, while 45 (58%) said that nothing bad had happened to them when they had installed such applications before.

## *Prediction Model*

In an effort to predict the behavior of survey respondents with their mobile applications, we constructed a prediction model designed to predict whether respondents would download applications asking for excessive permissions (0=yes, 1=no). A logistic regression model was used to estimate the model with this as the dependent variable. Independent variables entered in the preliminary model were the evaluations of the five markets, whether the respondent used IOS, the respondent's age and gender, the number of precautions taken, and whether the respondent was a technology major.

Using stepwise entry of the independent variables based on the likelihood ratio criterion, a model including only the number of precautions was significant. Table 4 shows the model statistics. The Hosmer and Lemeshow test indicated that there was no significant lack of fit between the model and the data (chi

square=1.687, df=2, p=0.430). The Nagelkerke R2 value was 0.068. The model shows those who take more precautions are somewhat less likely to download these applications than those who take fewer precautions. Each additional precaution that a respondent takes reduces the odd that he or she will install an application asking for excessive permissions by about 40%.

| Variable | B | Standard Error | Significance |
|---|---|---|---|
| Constant | .781 | 0.346 | 0.024 |
| # of Precautions | -0.502 | 0.183 | 0.006 |

**Table 4. Prediction Model 1 Logistic Regression Model**

Table 5 shows the predictive accuracy of the model. As shown in the table, the model classified 69.4% of the respondents correctly, with equal success in both the Yes and No conditions.

| Observed | | Predicted | | |
|---|---|---|---|---|
| | | Have you ever installed an application you believed asked for excessive permissions? | | Percentage Correct |
| | | Yes | No | |
| Have you ever installed an application you believed asked for excessive permissions? | Yes | 54 | 24 | 69.2 |
| | No | 33 | 41 | 55.4 |
| Overall Percentage | | | | 62.5 |

**Table 5. Prediction Model 1 Logistic Model Accuracy**

## Discussion

Participants in this study averaged over 34 downloads each, which establishes the sample as a group that has significant experience with mobile applications. Unlike worldwide and national averages, this group had more iOS representation than Android representation. Almost one in five of those surveyed rooted or jailbroke their devices, which made them more likely to be a victim of malware in this study. Rooting or jailbreaking a mobile device removes the built-in security restrictions, making the devices more vulnerable to malware. Thus, this result is expected and fits current research trends.

Participants in the study trusted the Apple App Store and the Google's Google Play markets significantly more than Microsoft's market, which was a little surprising considering Microsoft is a major market with their own platform. However, all three of these markets are seen as significantly more trustworthy than 3rd party markets, which fits current research that suggests most malware is present on 3rd party markets.

Half of those surveyed installed apps asking for excessive permissions. However, installing apps asking for excessive permission comes with major concerns based on the survey results. Eighty-six percent of

participants indicated they agree or strongly agree that they are very concerned with protecting their privacy. Also, 80% agree or strongly agree that they are concerned with malware.

Of those who installed apps with excessive permissions, 72% said it was because they trusted the market. However, our paper has already pointed out that all markets contain malware, ask for excessive permissions, and have major privacy concerns. The before mentioned (Appthority 2014) study indicated that Apple's App Store's top apps were more risky than Google Play's top apps and our survey participants trusted the Apple App Store the most. With 63% stating there is often a good reason for the application to request questionable permissions and 58% stating nothing bad had happened to them before, there is an indication of desensitization among consumers. When consumers no longer reject apps with excessive permissions because nothing has ever happened to them before and the belief that there is a good reason for the permission requests if they were to investigate, those consumers have become desensitized to excessive permission requests. Desensitization to permission requests puts the consumer at great risk and renders permission request lists even more inadequate. Consumer desensitization to excessive permission requests is also supported by the before mentioned (Benton et al. 2013) study that concluded permissions were ineffective even after adding additional text warnings to permission requests.

A prediction model was presented in this paper that attempts to predict whether participants will download applications asking for excessive permissions. Research demonstrates it is highly advisable to avoid apps with excessive permissions. But the model also suggests that those who downloaded apps with excessive permissions tended to take more precautions. While taking more precautions may seem like a good thing, this paper has already established that users most often fail to understand permission requests even if they read them and application star ratings and reviews are not related to risk. The other precaution, reviewing the developer, was only exercised by 26% of the participants. These precautions may be giving consumers a false sense of security, thus leading to the highly reported victimization from malware and the 34 app download average in this study.

## Conclusion

This study investigated the influences on consumers before downloading and installing mobile applications. A prediction model was created, and the study results indicate more work needs to be done to better inform consumers about potential security and privacy risks from permission requests. More work also needs to be done to inform consumers about the unreliability of common precautions, such as reviewing permissions and app reviews and ratings. New methods of explaining permission requests may not be enough if consumers have become desensitized.

This paper contributes in two primary ways. First, the paper creates a model to predict the installation of apps asking for excessive permissions. Second, the paper suggests changing the way permissions are displayed and explained to consumers may be ineffective if consumers have become desensitized to app permissions.

The primary limitation of this study is sample size. While the sample size of 155 participants is admittedly small, if generalizable at all, generalizability may be limited to other information technology students from the same institution. However, the results do support current trends reported in mobile device security research.

## References


Appthority 2014. "App Reputation Report," (Available online at https://www.appthority.com/learn/; Accessed March 10, 2015).

Benton, K., Camp, L. J., and Garg, V. 2013. "Studying the Effectiveness of Android Application Permissions Requests," in *Fifth International Workshop on Security and Social Networking 2013*: San Diego, CA.

Chia, P., Yamamoto, Y., and Asokan, N. 2012. "Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals," in *International World Wide Web Conference Committee*: Lyon, France.

Cisco 2014. "Cisco 2014 Annual Security Report," (Available online at http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html; Accessed March 10, 2015).

FCC 2014. "Ten Steps to Smartphone Security for Android," (Available online at http://www.fcc.gov/smartphone-security/Android; Accessed March 10, 2015).

Felt, A., Hay, E., Egelman, S., Haneyy, A., Chin, E., and Wagner, D. 2012. "Android Permissions: User Attention, Comprehension, and Behavior," in *Symposium on Usable Privacy and Security 2012*: Washington, DC, USA.

FTC 2014. "Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent," (Available online at https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million; Accessed March 10, 2015).

Gartner 2014a. "Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013," (Available online at http://www.gartner.com/newsroom/id/2665715; Accessed March 10, 2015).

Gartner 2014b. "Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013," (Available online at http://www.gartner.com/newsroom/id/2592315; Accessed March 10, 2015).

Gartner 2014c. "Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments On Pace to Grow 7.6 Percent in 2014," (Available online at http://www.gartner.com/newsroom/id/2645115; Accessed March 10, 2015).

Harris, M. A., and Patten, K. 2014. "Mobile device security considerations for small- and medium-sized enterprise business mobility," *Information Management & Computer Security* (22:1), pp. 97-114.

Hoffman, A. 2013. "FTC Settlement Provides Guidance Regarding an Apps Collection of Geolocation Data, When Data Collection and Sharing May Begin, and Privacy Representations in a License Agreement | InfoLawGroup," (Available online at http://www.infolawgroup.com/2013/12/articles/ftc/ftc-settlement-provides-guidance-regarding-an-apps-collection-of-geolocation-data-when-data-collection-and-sharing-may-begin-and-privacy-representations-in-a-license-agreement/; Accessed on March 10, 2015).

IBM 2013. "IBM X-Force: Ahead of the Threat – Overview," (Available online at http://www-03.ibm.com/security/xforce/downloads.html; Accessed March 10, 2015).

IC3 2012. "Smartphone Users Should Be Aware Of Malware Targeting Mobile Devices And Safety Measures To Help Avoid Compromise," (Available online at http://www.ic3.gov/media/2012/121012.aspx; Accessed March 10, 2015).

Juniper 2013. "Juniper Networks Third Annual Mobile Threats Report," (Available online at http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf; Accessed March 10, 2015).

Kelley, P., Consolvo, S., Cranor, L., Jung, J., Sadeh, N., and Wetherall, D. Year. "A Conundrum of Permissions: Installing Applications on an Android Smartphone," FC 2012 Workshops, Springer2012.

Koufaris, M. 2002. "Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior," *Information Systems Research* (13:2).

Lee, Ming-Chi, 2009. "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," *Electronic Commerce Research and Applications* (8), pp. 130–141.

Mylonas, A., Kastania, A., and Gritzalis, D. 2013. "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security* (34:0), pp. 47-66.

Siegrist, M., Cvetkovich, G., and Roth, C. 2000. "Salient Value Similarity, Social Trust, and Risk/Benefit Perception," *Risk Analysis* (20:3).

TrendMicro 2014. "Malicious apps, mobile malware reaches 1 million mark," (Available online at http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-high-risk-apps-hit-1m-mark/; Accessed March 10, 2015).