Downloading Mobile Applications – Are Students Protecting Themselves?

Adnan A. Chawdhry
chawdhry_a@calu.edu
California University of Pennsylvania
California, PA

Karen Paullet
paullet@rmu.edu

David M. Douglas
douglas@rmu.edu

Robert Morris University
Moon Township, PA

Joseph Compimizzi
jcompomizzi@fau.edu
Florida Atlantic University
Boca Raton, FL

Abstract

Mobile applications (apps) are taking the world by storm. Currently, end users have downloaded over 225 billion apps on their mobile devices. Security concerns surrounding the downloading of apps are often overlooked. The apps on our smart phones can be accessed by the tip of our fingers or the sound of our voice. One must think about the interactive risks to our privacy and the security concerns that can affect our digital lives. This study explores awareness and security risks associated with downloading mobile apps. A total of 124 students were surveyed at two mid-Atlantic Universities. The study found that many students are downloading mobile apps without fully understanding the security risks associated with such action.

Keywords: Mobile security, mobile applications, apps, mobile device

1. INTRODUCTION

Mobile applications could be considered a scourge or savior to human interaction with our smart phones depending on who is asked. Each day many new or improved mobile applications are being created. These App creators can be found in all age groups, cultures and from all social economic backgrounds. Some are designed to make our life easier (location and directional) and less stressful (reminders and flashlight). It appears there is an App for all needs both real and perceived. According to Statistica (2016), there has been an upward trend in mobile app usage. In 2011, there were 22 billion free app downloads and 2.9 billion paid app downloads. As of June 2016, people have downloaded over 211 billion free apps and 13.49 billion paid apps showing the significant rise in mobile app usage.

These App creators, both young and old create for fun, profit, or perhaps most importantly to fill a "void" in the ever expanding catalogue of must have "apps." These apps, also known as mobile applications, are designed, or so they say, to improve our lives. Perhaps they do in some respect, but one of the unintended consequences is a more complacent and indolent mobile community especially in regards to cyber security and the oversharing of information both private and public.

However as with all things in life, there are unintended consequences. We live in a brave new world of the Internet of Things (IoT) and smart phones. The applications (Apps) on our smart phones are at the tip of our fingers or the sound of our voice. Knowing and unknowingly we often overshare many aspects of our personal information in cyberspace. Once shared, we can never retrieve or change this cyber data. The information is now beyond our grasp and control. One wrong click or one wrong tap of our finger on the wrong button or link can change a life instantly. This lapse of judgment or mistaken "click or send" can allow a miscreant hacker or rouge agency to gain access to financial and personal aspects of our digital lives. One must think about the interactive risks to our privacy and the security concerns that can affect our digital lives.

2. LITERATURE

Recent years have witnessed an explosion in the acquisition and use of mobile computing devices known as smart technology. According to the February 2013 Federal Trade Commission Report, 217 million smartphone were purchased in the fourth quarter of 2012 alone (Mobile Privacy Disclosures). Consumers of smart devices are using the technologies offered by these smart devices for a multitude of functions from waking up with alarm applications to lunch ordering and purchase to monitoring traffic for the commute home, not to mention the more mundane daily tasks of the texts, calls and emails completed through personal mobile devices.

As the functions of a mobile device become more complex, so too do their operating systems and development of their applications. And with this increased complexity of functionality, comes complexity with understanding: namely security and privacy understanding. Theoharidou, Mylonas, and Gritzalis (2012) explain that mobile apps are both an asset and threat for users. While the social, financial and business benefits of an app are numerous, they can act as a security attack access point for users. These security threats range from spoofing, to cloning, to unauthorized access, to disablement, to phishing to malware injection all related to permission access rights and authentication violations (Theoharidou, Mylonas, and Gritzalis, 2012).

One of the characteristics of how we conduct our mobile communication activities in 2016 is recognizing some of the more perilous aspects and unforgiving consequences of our more than casual acceptance of the "Terms of Service Agreement" before downloading any given application (APP). For many people, including some of the authors of this document, we are guilty of blindly checking "I accept" the terms of service for any given App without a hint of even reading the first sentence (Boyles, et.al, 2012).

This blind acceptance often permits the creator and/or carrier of the mobile application full access to many features of our mobile devices, including photos, contacts, and location to name just a few. Indeed, it is a frightening and somewhat unsophisticated Orwellian circumspection of our time and place in history. In short are we willing oversharing personal information about ourselves and those connected to and imbedded on our mobile devices.

We are at last finally comprehending just how much total and complete access to every aspect of our personal information we are blinding giving to a plethora unknown third parties to do with as they wish with our full and unequivocal consents. However, all is not lost as mobile device users are awakening to the fact that they do not want these third party terms of agreement unknowns to have control and access to their personal information. As our adoption of mobile technology cultivates and our acceptance of sharing our personal aspects of our life increases it would seem reasonable that we accept and welcome the apps that seemingly make our lives easier (Boyles, et.al, 2012).

Koved, Trewin, Swart, Singh, Cheng, Chari (2013) discussed the risks associated with the adoption of mobile devices regarding its authentication and authorization on network services. Their research especially focused when these devices were relied on to input or share sensitive information. Mobile devices such as smartphones, tablets, and other "mobile platforms" are now commonly used for banking and shopping. Accordingly they have identified

several risks. They include the possibility of that the user's action will be observed and allow an unauthorized authentication or "impersonation" on a different device. Understandably, when devices are stolen or lost the risks of exposing sensitive information is increased. "In particular, mobile device applications, including the web browsers, are caching authentication credentials, enabling an attacker to exploit them. Modern smartphones can enable multi-factor authentication by using sensors such as cameras and microphones to capture biometric data" (Koved, 2013).

Concerning third party applications commonly referred to as mobile apps, distribution marketplaces such as Apple's Appstore offer two types: paid apps and free apps. Understanding the difference between the two provides a foundation to pivot a discussion on security issues with mobile technology devices. Free apps, with no surprise, are more popular than paid apps. According to Petsas, Papadogiannakis, Polychronakis, Markatos and Karagiannis (2013), "paid apps usually have more advanced functionality and do not include advertisements" (p. 285). According to the study conducted by Compomizzi (2013), of the college student participants with iPads, 54.2% indicated that they paid for a few apps while 20.5% indicated that they didn't pay for any. Further, participants in this study indicated that the apps they purchased were related to academic uses specifically to complete study tasks like note-taking app's, for academic tools like calculator and dictionary apps, and for course requirements like e-book apps and video apps.

Given that free apps rely on advertisements, learning about the usage patterns by mobile device operators yields additional information that leads to a more thorough examination of the issue of security. In the study by Petsas, et al. (2013), 55,000 free apps from the Google Play Store were categorized, tracked and examined. The analysis of data collected in the study disclosed that the top 10 categories accounted for 60% of the apps. These app categories included tools, entertainment, brain apps like puzzles, lifestyle, business, books, travel, education and casual. Of the 55,000 apps examined, 46,000 as for the android permission to access the network. Further, of these 46,000 apps, 19,000 were connected to at least one advertisement library (Petsas, 2013).

As a result, skepticism and mistrust about the use of personal information by platform hosts, app developers and advertisers are increasing among smart device owners. A 2012 study by Boyles, Smith, and Madden revealed that"more than half of app users have uninstalled or decided to not install an app due to concerns about personal information". In fact, of the 2,254 participants in their study, Boyles, Smith and Madden reported that 49% of users between 18 and 29 indicated that they decided not to install an app based on personal information concerns; of those in the same age bracket, 29% report uninstalling an app due to concerns about personal information sharing. Interestingly, their study also revealed that "app users with at least some college experience are somewhat more likely than those with a high school education to choose not to install an app over privacy concerns (Boyles, Smith and Madden, 2012).

With this understanding of mobile technology, system operations, user behaviors, and app interfaces, Theoharidou, Mylonas, and Gritzalis (2012) explain the mobile apps are both an asset and threat for users. While the social, financial and business benefits of an app are numerous, the app itself may need protection and can act as a security attack access point for users. These security threats range from spoofing, to cloning, to unauthorized access, to disablement, to phishing to malware injection all related to permission access rights and authentication violations (Theoharidou, Mylonas, and Gritzalis, p. 450). As Koved, Trewin, Swart, Singh, Cheng, and Chari (2013) write, "In particular, mobile device applications, including the web browsers, are caching authentication credentials, enabling an attacker to exploit them" (p. 1).

The good news is that advances in mobile technology and user protection continue in development. Secure passwords are only the beginning. Mobile and smart technology are incorporating camera and voice detection sensors. Biometrics with fingerprinting and retinal recognition are also advancing to counteract privacy and security concerns. The bad news is that these additional security features are often in direct contrast to mobile operators' expectations of easy to use, fast, and on-the-go technology. Users often view these additional security steps as burdensome. In a study conducted with IT professionals who also teach at the college level by Compomizzi, D'Aurora, and Rota (2013), of 90 question responses received regarding security practices, 76 indicated regular practice of low tech methods of protection such as password authentication and using multiple browsers for different computing functions while

only 14 employed high tech methods of security protection like biometrics.

The literature concerning how mobile technology is perceived and used by operators is ever-growing. Interesting definitions of a mobile device continue to emerge. Likewise, the uses of mobile technology continue to grow, placing demand upon more flexible, available and integrated computing capabilities and mobile applications. With this expansion in mobile technology, security risks are also increasing. While software and hardware developers forge ahead with progressed security solutions, users may perceive them as burdensome; thereby opening the door to information invasion and attack.

3. METHODOLOGY

The study surveyed students from two small mid-Atlantic Universities from March to April 2016. For this study, the population chosen comprised of undergraduate and graduate students enrolled in on-campus or online programs. This population was chosen to ensure students surveyed would be 18 years or older. A total of 124 students completed the survey. The researchers utilized Survey Monkey, an online survey tool, to collect data, which were then imported into SPSS for organization and analysis. As part of the analysis, the researchers used a Chi-square analysis with a statistical significance at the .05 margin of error with a 95% confidence Level. The study addressed the following two research questions.

1. What actions are students taking to reduce privacy / security concerns when downloading applications on their mobile devices?

2. Is there a statistical significance among age, gender, and level of education with the actions student take to mitigate the risks of privacy / security with downloading applications?

The survey administered to students consisted of 22 closed-ended questions and one open-ended question for further understanding of the participants responses. The first three questions focused on student demographics to include age, gender, and level of education. The remaining questions focused on whether students were aware of security and privacy concerns that exist with downloading mobile applications. The questions primarily focused on responses of "Yes" and "No", while a few questions provided additional options for students to select the type of mobile device they use, applications they use on their phone, and how many apps they have downloaded.

4. RESULTS

The survey presented seven scenarios where it prompted the participant to respond with a "Yes" or "No" answer, one open ended question for further analysis, and a multiple choice question with predefined responses including an "Other" option to include additional responses. These questions were designed to understand what actions students take to reduce security and privacy concerns when downloading mobile applications. These questions included what the use of anti-malware software, backing up phone content, clearing browsing history, disabling location services, uninstalling an application and why, and choosing to uninstall / not install an application once they were aware of the security and privacy impacts. The summary of the Yes / No results are provided in Table 1. Additionally, the researchers thought it would be important to understand how many applications downloaded on average. The highest response rate was between 11-20 applications with 37.90% followed by 1-10 applications at 22.40%. The breakdown of these results can be seen in Table 2.

Table 1: Survey Questions

Scenario	Yes	No
Downloaded Mobile Apps	96.64%	3.36%
Disabled Location Services	84.48%	15.52%
Clear Browsing / Search History	74.14%	25.86%
Backup using 3rd Party Software	34.21%	65.79%
Installed Anti-Malware	29.31%	70.69%
Uninstalled / Not Installed App	94.71%	5.29%
Not Installed after discovering how much personal information is shared	77.00%	23.00%
Uninstalled after discovering how much personal information is shared	64.60%	35.40%

Table 2: Number of Downloaded Applications

Number of Mobile Apps Downloaded	Percent
0	1.70%
1-10	22.40%
11-20	37.90%
21-30	19.00%
31-40	5.20%
More than 40	13.80%

Additionally, the researchers were interested to further analyze the student responses on reading the terms of use for an application compared to their awareness that applications have access to their phone's content. Approximately 83.19% of the students were aware that mobile applications have access to their content while only 14% were unaware of this. Additionally, only 33.61% of students responded that they have read the terms of use before downloading an app. The highest percentage of 51.26% was found where students did not read the terms of use but were aware that applications have access to their phones content. The breakout of these results can be found in Table 3.

Table 3: Reading Terms of Use Vs Awareness

Read Terms of Use	Aware that Apps have access to Phone context		
	Yes	No	Total
Yes	32.76%	1.72%	34.48%
No	52.59%	12.93%	65.52%
Total	85.34%	14.66%	100.00%

While understanding the actions students took in regards to protecting their mobile devices from security and privacy concerns is important, knowing the reasons behind their decisions to uninstall an app, choose to not install an app, or disable location services may provide additional insights. The survey asked why students chose to uninstall a mobile application. The most common reason was because the application was collecting personal information with a response rate of 37.5%. The least common was security concerns. Table 4 below shows the breakdown of responses including an option to choose "Other".

Table 4: Reasons to Uninstall or not Install

Reasons to uninstall App	Percentage
Privacy Concerns	18.80%
Security Concerns	12.50%
Collecting personal Information	37.50%
Other	31.30%
Total	100.00%

The survey provided a supplemental question if students selected "other." Below are responses from those participants.

- Didn't use the app
- Either too large or didn't use it often
- Privacy and security concerns as well as collecting personal information
- The app is not useful for me anymore
- The app was not what I had thought it was.

While it was important to understand why they chose to uninstall an app, we thought it was also important to note the reasons they may have chosen to disable locations services for apps they decided not to uninstall. The responses included the following:

- Not necessary for the app to function
- Battery Life
- Told to disable it
- Tracking me
- Privacy / Security Concerns
- Don't trust it
- Used too much data
- Feeling insecure

Additionally, the participants were asked which applications they chose to disable location services for. Below is a summary of those responses.

- All applications
- Social Media Sites
- Banking
- Retail / Shopping
- Unpopular Apps
- Weather
- Maps
- Games
- News
- Calendar
- Photos

Lastly, you will find a chi-square analysis performed on these participant responses against age, gender, and level of education to understand any statistical correlation that may have existed. Only values of .05 or less were considered

statistically significant. These results can be found in Tables 5-7. Age had a statistical significance with clearing the browsing / search history, backing up the phone's content, and using anti-malware software. Gender was statistically significant with clearing the browsing / search history and using anti-malware software. Level of Education did not illustrate a statistical significance with any of the response.

Table 5: Chi-Square Analysis with Age

Action to Protect Security and Privacy	Age (df = 6)
Disabled Location Services	0.704
Clear browsing / search history	0.016
Backup phone contents with third party app	0.05
Use anti-malware	0.028
Read Terms of use / service	0.197
Uninstalled / Not Installed App	0.856
Not Installed after discovering how much personal information is shared	0.375
Not Installed after discovering how much personal information is shared	0.933

Table 6: Chi-Square Analysis with Gender

Action to Protect Security and Privacy	Gender (df = 1)
Disabled Location Services	0.362
Clear browsing / search history	0.035
Backup phone contents with third party app	0.925
Use anti-malware	0.002
Read Terms of use / service	0.201
Uninstalled / Not Installed App	0.771
Not Installed after discovering how much personal information is shared	0.26
Not Installed after discovering how much personal information is shared	0.191

Table 7: Chi-Square Analysis with Level of Education

Action to Protect Security and Privacy	Level of Education (df = 5)
Disabled Location Services	0.98
Clear browsing / search history	0.234
Backup phone contents with third party app	0.506
Use anti-malware	0.234
Read Terms of use / service	0.249
Uninstalled / Not Installed App	0.265
Not Installed after discovering how much personal information is shared	0.622
Not Installed after discovering how much personal information is shared	0.454

5. DISCUSSION

Mobile applications can access a good amount of information on your phone which can lead to security and privacy concerns. Most of this is outlined in the terms of use, but the question is how often do we really read it? Even more important was do we take action if we read it or do we choose to take action just knowing there are general concerns in terms of security or privacy. The survey revealed that 96.64% of the respondents have downloaded apps on their mobile devices. Additionally 84.48% have disabled location services on their device. These two numbers were interesting because it illustrated that while a high percentage do download apps, they took the first step of disabling location services to protect their privacy. Another important metric was that 94.71% of the participants have chosen to uninstall or not install an Application on their phone. A majority of the responses indicated a concern around privacy, security, or the application collecting too much data. However approximately 31% responded "other" with additional feedback that they no longer used the app or that the app did have the functionality they were looking for.

Another important piece to understand was if the participants took an action to uninstall or not install an application once they realized how much personal information may be shared. Of the

participants, 77% stated they chose to not install an application after discovering how much personal information was being shared. From the same sample, 64.6% stated they chose to uninstall the application once they realized the amount of personal information was being shared. These large response indicated that the participants were worried about security and privacy and they took an action after understanding the risks an application posed. However, the study also asked if the participants read the Terms of Use and only 35% responded that they have. This low response compared to the prior question indicate that either participants were informed of the risks through a different channel, possibly through general knowledge, another person informing them, or just a pop-up that asked permission for the application to access some content on their mobile device.

As mentioned earlier, 84.8% of the respondents chose to take an action of disabling location services on their phone to mitigate certain security and privacy concerns. The researchers assumed the majority of responses were related to security and privacy concerns but they asked two follow up questions to understand other reasons they may have done this and what applications they may have done this to. Some of the responses included extending battery life, they felt location services were not needed for the application, lack of trust and sharing too much data, and feeling of insecurity. Additionally, respondents stated they have turned location services off for applications in the categories of social media, banking, retail, weather, games, news, calendar, and photos. Given these results, it not only seems that users are taking general actions for protecting their privacy, but also that they have done so on specific applications that they felt impede on their security or privacy.

Lastly, the researchers wanted to understand if there existed a statistical significance among the three demographics (age, gender, and level of education) versus the actions taken to mitigate the security and privacy risks. Of the 8 scenarios, level of education did not have any statistical significance (a chi-square value of less than .05), while age had three and gender had two. For both Age and gender, the researchers found a statistical significance with clearing their browser / search history having chi-square values of .016 and .035, respectively. Using Anti-Malware software had a .028 chi-square value with age and a .002 chi-square value with gender. Additionally, age found another statistical significance with backing up the phone contents using a third party application while having a chi-square value of .05.

6. CONCLUSIONS

Mobile application can collect information from our mobile devices for a variety of reasons. While awareness is a key factor of ensuring that end users make informed decisions in order to stay safe while using their mobile devices, it is equally important to understand what actions these users take to protect their security and privacy. Using tools like anti-malware had a low response rate, participants illustrated that they were concerned about their security and privacy by their actions. Some had chosen to uninstall or not install an application once they learned of how much personal information would be shared. Others chose to keep the application but limit features like locations services to minimize the security and privacy risks. Given the low response rate for people who stated they read the terms of use, but the high response of some action being taken, it was clear that the participants were informed through another channel of the risks they pose. It was important to understand if users really cared about their security and privacy concerns and their actions certainly illustrate that they do. Since awareness is a key factor in protection, it would also be important to understand where they are getting their awareness from or if they are just generalizations about overall security.

7. REFERENCES

Boyles, J.L., Smith, A. and Madden, M. (2012). Privacy and data management on mobile devices. Retrieved 9/10/2016 from http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx

Canalys. (2011) Smart phones overtake client PCs in 2011. Retrieved 6/11/2016 from http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011

Compomizzi, J. (2013). The influence of iPad technology on the academic and social experiences of veteran and military students: Academic preparation, collaboration socialization, and information access. ROBERT MORRIS UNIVERSITY.

Compomizzi, J., D'Aurora, S., & Rota, D. P. (2013) Identity theft and preventive measures: the cost is all yours. Issues in Information Systems. Vol. 14, Iss. 1, pp. 162-168.

Federal Trade Commission. (February, 2013). Mobile privacy disclosures: Building trust through transparency. Retrieved September 10, 2016 from www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

Petsas, T., Papadogiannakis, A., Polychronakis, M., Markatos, E. P., & Karagiannis, T. (2013, October).

Rise of the planet of the apps: A systematic study of the mobile app ecosystem. In Proceedings of the 2013 conference on Internet measurement conference (pp. 277-290). ACM.

Salesforce. (2014). Mobile Behavior Report. Retrieved 6/9/2016 from http://www.marketingcloud.com/resource-center/digital-marketing/2014-mobile-behavior-report

Statistica, (2016). The Statistics Portal. Number of free and mobile app store downloads worldwide from 2011 to 2017 (in billions). Retrieved from www. Statistica.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A risk assessment method for smartphones. In Information security and privacy research (pp. 443-456). Springer Berlin Heidelberg.

Tongaonkar, A., Dai, S., Nucci, A., & Song, D. (2013, March). Understanding mobile app usage patterns using in-app advertisements. In Passive and Active Measurement (pp. 63-72). Springer Berlin Heidelberg.

