What's "Appening" to our Privacy? A Student's Perspective on Downloading Mobile Apps

Karen Paullet
paullet@rmu.edu
Robert Morris University
Moon Township, PA 15108

Adnan A. Chawdhry
Chawdhry_a@calu.edu
California University of Pennsylvania
California, PA 15419

David M. Douglas
douglas@rmu.edu
Robert Morris University
Moon Township, PA 15108

Joseph Compimizzi
jcompomizzi@fau.edu
Florida Atlantic University
Boca Raton, FL 33431

Abstract

Smartphones and mobile device sales continue to grow allowing mobile applications (apps) to develop in variety and usage. Mobile device users have downloaded over 225 billion apps and this number continues to grow. While there is an inherent benefit to our daily lives of having applications that are available at our fingertips or by the sound of our voice, they come with an associated and undiscussed cost of security and privacy issues. One must consider these risks, how they may impact our lives, and the best alternative of mitigating the risk with the balance of convenience. This study explores specific apps downloaded by end-users, the number of apps they download, and how they correlate to their awareness of mobile app security and privacy concerns. A total of 124 undergraduate and graduate students were surveyed at two mid-Atlantic Universities in both traditional and online programs. The study concluded that students download apps regardless of the security or privacy risks that are being exposed.

Keywords: mobile security, mobile applications, apps, mobile device, application privacy

1. INTRODUCTION

With the increased use of smartphones and mobile devices, mobile applications have become an integral part of our everyday lives. Numerous applications are being developed daily and are created by developers of different ages, cultures, and social / economic backgrounds.

These applications strive to provide users with an easier life and less stress by supplementing manual activities with application driven ones. With the extensive library of applications available to use, it appears these applications have filled our present and perceived needs. According to Statistica (2016), there has been an upward trend in mobile application usage. In 2011, users had downloaded 22 billion free and another 2.9 billion paid applications. However, as of June 2016, these numbers have significantly increased to 211 billion free and 13.49 billion paid applications. The variance between these two numbers illustrates that people download more because its free.

Mobile technology is significantly impacting the way people interact with each other, organizations, and with technology itself. Mobile applications, or apps as commonly called, promote communications, information retrieval and exchange, and any other number of tasks users need to complete at a literal touch of a screen. These third party interfacing platforms offer users ease. Mobile apps, though, also offer security and privacy threats to such audiences as undergraduate and graduate level university students.

Developers are creating applications for various reasons including fun, profit, or possibly to fill a gap in the growing library of "must have" applications. In some respects, apps certainly provide us clear advantages, however, they also come at a cost of a more complacent and indolent mobile community in regards to cyber security and oversharing of information.

As with any technological advancement, there are always unintended consequences that must be balanced against its perceived benefits. These applications are at the tip of our fingers on our smart phone and in some cases, usable by the sound of our voice. Knowingly and unknowingly, we tend to overshare private information in cyberspace about our personal lives. Unfortunately, once this information is released in cyberspace, it can be difficult, if not impossible, to retrieve or change it. The information is now in the public domain and beyond our grasp or control. Our carelessness can open the gateways for a hacker or rouge agency to digitally access our financial data and other aspects of our lives. Before divulging too much, one must carefully consider the risks to ourselves and our privacy plus any security concerns to our digital lives.

2. RELATED LITERATURE

In the article "The Mobile Application Preferences of Undergraduate University Students: A Longitudinal Study" Potgieter indicates her study revealed that "even though users were aware of security threats associated with downloading apps, this knowledge did not deter them from continuing to download apps" (2015, p. 1). A study conducted by Chawdhry, Paullet, Douglas, and Compomizzi confirmed similar results in that students downloaded mobile apps without fully understanding the security risks associated with such action (2017, p. 35). In their study, while 96.64% of students indicated that they download mobile apps, only 70.69% did not install any type of anti-malware on their devices. Interestingly, in this same study 64.60% of students surveyed disclosed that they also uninstalled an app after discovering how much personal information was shared.

Why students download mobile applications in spite of security risks gives insight to their motivations. As studies by Potgieter reveal, "In 2013, 48% of respondents indicated that they searched for an app when they 'need information on a brand, its product or its services, whereas the most popular reason in 2014 for searching for an app was that respondents 'wanted to be entertained'" (2015, p. 3). Other reasons indicated by students in the research studies by Potgieter as to why they downloaded a mobile application included family or friend recommendation of the app, curiosity about the app, reference to the app on regularly used websites, or the desire to purpose a product or service. Researchers like Baily (2016), maintain that consumers of mobile applications conduct a cost-benefit analysis and conclude that the convenience is worth more than privacy (p. 5). Other researchers such as Soukup (2015) present that mobile technology platforms call "attention to personal presence, personal choices, and the social forces that shape both" (p. 5). Soukup's observations advocate that these devices and platforms promote social cohesion.

Given these motivations, the number and types of mobile apps employed by college students provide insight to the presence of security risks as well. In a study conducted by Compomizzi (2013) regarding social use of mobile technology, 21.3% of study participants indicated that they downloaded 41 or more apps. Of these apps, 12.0% indicated that half of the apps downloaded were related to

academic tasks. Regarding social use of mobile applications in this study, "Facebook was the social media app listed most frequently by participants with Twitter following as the second most frequently accessed social media app" (p. 128). The study by Potgieter (2015) found similar results: "Facebook was a clear favorite with 75% of respondents indicating that they had this app on their smartphone, whereas in 2014, WhatsApp had been installed by 73% of respondents" (p. 5).

Advanced mobile operating systems implement a "sandbox" permission system whose function is to provide security and privacy policy for third-party apps. "To provide better services to users and gain more downloads of Apps, mobile App developers try to request more and more data access permissions, which can help to implement the intelligent applications, such as social sharing services. However, these services may result in potential security and privacy risks" (Zhu, Xiong, Yong, Chen, p. 2-3).

A July 9, 2017 Wall Street journal article by Fritz and Mickle stated that according to estimates by Bernstein Research: "iTunes videos, music, book and magazine sales last year accounted for an estimated $4.1 billion in revenue, making it the second-largest services business behind App Store sales, which were nearly twice as large …" (Fritz, et.al. 2017).

Baily sheds some light on the impacts of technological interface with application users. In the article "Why Consumers Opt Out of Privacy by Buying into the Internet of Things" from the Texas Law Review (2016), Baily describes a possible effect that is applied to app users called unrealistic optimism or over optimism. She asserts that with unrealistic optimism, a "user may be subject to the above average effect because they may believe that they are less likely than the average person to experience harm from data loss" (p. 1029). Drawing on the research of Miyazaki and Fernandez, Baily emphasized, "Moreover, the more Internet experience a person has, the lower his perceived risk toward risky online behaviors" (p. 1029).

Koved, et al. (2013) discussed four increased risks associated with authentication and authorization regarding interaction with the mobile platforms of smartphones and tablet devices. These risks include (a) user action observation by others who may than impersonate (authenticate) on another device. (b) stolen or lost devices could expose sensitive or personal information to unauthorized persons (c) "man in the middle attacks" which would allow attackers to "capture authentication credentials and perform actions" as the device owner (d) multiple passwords saved on mobile devices may save time but increase risk of unauthorized access and authentication (p,1). Moreover, Koved, et al. (2013) suggests that to guard against these perceived and actual security risks it is essential to have a trusted authentication strategy and communications systems that are secure. Part of the solution they argue, is various authentication methods are part of the solution. Since passwords can be observed it is not considered a single or reliable approach (p. 1). "In particular, mobile device applications, including their web browsers, are caching authentication credentials, enabling an attacker to exploit them" (Koved, et al., p.1. 2013).

Although current smartphone and tablet devices can capture biometric data via cameras and microphones which offers a potential and partial security solution, some users most likely would consider it an added burden. As user interaction with their mobile devices is generally brief, it is perceived they do not want to bother with the distraction of a lengthy or complex authentication process. This is especially true if they do not understand the reasons or importance for authentication. "Little is known about peoples' awareness of these mobile device authentication risks" (Koved, et al., p.1. 2013).

The use of biometrics is now being utilized in mobile applications. "In 2015, Citigroup began testing an ATM that would scan a customer's iris and make four-digit access codes obsolete" (Demos, T., p, B4, 2017). Two years have passed and Citi has all but abandoned the project. Reason one, cost and complexity. Collecting and managing a database of millions of customer biometric data would be enormous. Reason two, a biometric database and genetic template of this magnitude and value would be an alluring target for a legion of hackers from lone wolves to international gangsters. (Demos, T., p, B4). Passwords can be easily replaced, but biometric authentication such as fingerprints and irises obviously cannot.

Wells Fargo, J.P. Morgan, and Bank of America have begun to utilize ATM's that can link biometric data to the smartphone devices of customers. Instead of the financial institution storing customer biometric information, it is the customer's responsibility to store and safeguard

their biometric authentication. One method uses the customers fingerprint to sign in via their mobile device which would transmit a code to the ATM (Demos, T., p, B4). According to banking-technology start-up HYPR Corporation there are "about two billion units globally can use fingerprints, pictures of eyes and faces, and voice recognition … "and are already used for mobile banking applications (Demos, T., p, B4).

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 which comprised of a total of 124 students completing 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 approach with a statistical significance level of .05 margin of error and a 95% confidence Level. The study addressed the following two research questions.

1. Does the use of specific mobile applications impact the level of mobile security and privacy awareness?

2. How does the number of applications installed on a mobile device impact the user's actions to prevent security and privacy issues?

The survey administered to students consisted of 22 closed-ended questions and one open-ended question for further understanding of the participant's responses. The questions focused on whether students were aware of security and privacy concerns that exist with downloading mobile applications. Additionally, participants were asked to identify the applications they are using and the number of applications they have downloaded. 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 began with various foundational / demographic questions about the participants. For this study, the first question of primary importance was to understand which apps were being downloaded and used. The question allowed the users to select as many as needed that were applicable to their personal use. The apps included Facebook, Twitter, Instagram, Snapchat, Accessing Email, Playing Games, Listening to Music, Reading Books, and Searching for Information. Additionally, the users were asked how many applications they have downloaded with the response categorized as 1-10, 11-20, 21-30, 31-40, and 40+. A summary illustrating the percentage of participants who responded to each question can be found in Table 1 and 2.

Table 1: Summary of Applications downloaded by Users.

Application Downloaded	Uninstalled After Learning About App
Facebook	70.20%
Twitter	50.00%
Instagram	56.50%
Snapchat	62.10%
Accessing Email	91.10%
Playing games	56.50%
Listening to music	81.50%
Reading books	31.50%
Searching for information	84.70%

Table 2: Number of Apps Downloaded

Number of Apps Downloaded	Percentage of Respondents
1-10	28.30%
11-20	35.50%
21-30	17.70%
31-40	4.80%
40+	13.70%

From the findings, more than half of the respondents have used each of the applications mentioned with the exception of "Reading

Books" which only illustrated 31.5% of the respondents. Additionally, the majority, 63.8%, of respondents have downloaded 20 apps or less. The largest responses suggested that the users downloaded between 11-20 apps on their mobile device.

Table 4: Chi-square Analysis of Security / Privacy Activity vs Number of Applications Downloaded

Security / Privacy Activity	Number of Applications Downloaded
Disabled Location Services	0.866
Clear Browsing History	0.89
Have Anti-Malware Software	0.048
Read Terms of Use	0.137
Uninstalled / Not installed an App	0.687
Uninstalled / Not Installed an App	0.684
Uninstalled / Not installed an App	0.727
Not Installed After Learning About App	0.775
Uninstalled After Learning About App	0.517

A second component to this study's analysis was to analyze the data using Chi-square. The objective was to determine the statistical significance between two variables using a .05 margin of error and a 95% confidence interval. The results are illustrated in Table 3 and Table 4. Table 3 (in appendix) illustrates the application downloaded assessed against a number of activities illustrating the users were aware of a potential security and privacy concern. Only one application illustrated a statistical significance given the .05 margin of error. Facebook had a value of .05. Instagram had significance with having Ant-Malware installed and a value of .021. Instagram also had statistical significance with Reading the Terms of Use with a value of .04. Lastly, Snapchat had a statistical significance with Having Anti-Malware Software having a value of .049.

Additionally, the researchers compared various security and privacy activities with the number of applications downloaded. Only one activity, Having Anti-Malware Software, had a statistical significance of .048 with the number of applications downloaded. Further details are provided in Table 4.

It was also important to see how many participants undertook security and privacy risk mitigation activities and how it correlated to the applications they downloaded. The activities included disabling location services, clearing browsing history, backing up their phone, having anti-malware software installed, another person accessing their phone, and reading the terms of use. Over 50% of the users who downloaded Facebook, Instagram, Snapchat, Email, Music, and Searching for Music applications stated they disabled location services. Additionally, over 50% of users who downloaded Facebook, Email, Music, and Searching for Information stated they cleared their browsing history. Lastly, over 50% of the users of Facebook, Snapchat, Email, Music, and Searching for Information reported that another person has access their phone. All other areas reported less than a 50% response rate. The details of this analysis can be found in Table 5 in the Appendix.

Similarly, the researchers did an analysis of various security and privacy risk mitigation activities and compared it against how many applications were downloaded. The activities included disabling location services, clearing browsing history, installing anti-malware software, another person accessing their phone, reading terms of use, uninstalling / not install an app, not installing an app after learning about it, and uninstalling an app after learning about it. For each activity, the largest response was either in the 1-10 or the 11 – 20 categories. In most cases, over one third of the respondents fell in the 11-20 category. Further details of this analysis are available in Table 6 in the Appendix.

5. DISCUSSION

Mobile Application Impact

Based upon the chi-square analysis of the applications users download and the activities to mitigate the security and privacy risk, the researchers found three applications that had some level of statistical significance. The first

research question sought to find out if the use of specific mobile applications impacts the level of mobile security and privacy awareness. These applications included Facebook with disabling location services, Instagram and Snapchat with installing anti-malware software, and Snapchat with reading the terms of use. The interesting part of this analysis is that all three of these applications are categorized as social media sites. In addition to these, accessing email, listening to music, and searching for information also had large response rates (over 50%) for the same activities in addition to clearing your browsing history. However, it is important to note that clearing your browsing history was not statistically significant.

From this analysis one could assume that certain applications like Facebook, Instagram, and Snapchat do affect the level of security and privacy awareness given that their users were more likely to act to protect themselves. Further extrapolation lead the researchers to believe that the respondents may consider social media applications risky in relation to security and privacy issues and therefore act to mitigate this risk. However, Twitter, another social media site, was not statistically significant and less than 50% of the respondents stated they undertook an activity to protect themselves. One assumption could be that this social media is used less than the other social media applications. Another thought is that users do not perceive Twitter as risky in comparison to Facebook, Instagram, and Snapchat.

Number of Applications

The second research question determined if the number of applications installed on a mobile device impact the user's actions to prevent security and privacy issues. When reviewing the number of applications downloaded, the largest category was 35.5% of the respondents saying that they downloaded 11-20 apps. Second to that were 28.3% of the participants stating they downloaded 1-10 applications. Most participants downloaded less than 20 applications. Lastly, 17.7% of the participants stated they downloaded 21-30 apps. Given these numbers, it was important to note that the researchers had a good variety of participants from ones who download few applications to those who download many applications.

One form of assessments was to review the chi-square values when comparing the number of apps downloaded with the various security and privacy risk mitigation activities. Of each of the values, only reading the terms of use showed a statistical correlation. There is a trend with the number of apps downloaded and reading the terms of use. Essentially one could interpret this as users are reading the terms of use more as they are downloading more apps. This could be because of being more familiar with the apps and the risks they possess. Therefore, users are reading the terms of use more frequently. Another notion is that users who have downloaded less apps have read the terms of use and realized that the risk associated with the apps is not worth it. And by doing so they chose not to download other apps.

Many of the other activities did not have a statistical correlation with the number of applications downloaded. One of great importance was disabling location services. Although we could not see a correlation with the number of applications, it was seen that users were still disabling location services. Lastly, it was important to note that there was consistency of whether users uninstalled / not installed an application before and after they learned about it. This consistency was across all the categories for the number of applications downloaded. Therefore, it is difficult to assess the impact of learning about the application had on their choices in relation to security and privacy concerns.

6. CONCLUSIONS

With the advent of the concepts of big data and the Internet of Things, research regarding the use of mobile applications, user practices, and user sense of security growing. Studying the needs and preferences of users, yields understanding to the practices and appreciation of privacy users demonstrate, especially college students. Although statistical significance was not prevalent throughout this study it is apparent that at least half of the student populations download apps without completely understanding the potential security risks to their data and privacy. This study was important because it illustrated regardless of security risks, it is becoming a trend that students are ignoring concerns that can risk their privacy and security.

Mobile applications are here to stay. It is apparent that convenience to some outweighs the risks associated with downloading some apps. Below are a list of tips to help keep our data and privacy secure:

1. Install apps from trusted sources such as an app store
2. Install anti-malware or security software on mobile devices
3. Read the terms of use and information regarding privacy and what the app can actually access on the mobile device
4. Review permissions when an app sends a notice to update
5. Enable app security features such as a password
6. Always keep the latest update on the mobile device. The updates can assist with catching viruses
7. Remove applications that are not necessary
8. Turn off connecting automatically to Wi-Fi or Bluetooth

7. REFERENCES

Bailey, M. (2015). Seduction by technology: why consumers opt out or privacy by buying into the Internet of Things. Texas Law Review, Austin, TX pp. 1023-1054

Chawdhry, A., Paullet, K., Douglas, D. & Compomizzi, J. (2017). Downloading mobile applications: Are students protecting themselves? *Journal of Information Systems Applied Research.* Vol 10, Issue 2, pp. 35-42

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* (Doctoral Dissertation). Retrieved on 7/6/2016 from Proquest 3565603.

Demos, T. (2017, July 9). Why your phone will be the key to ATMs of the future. The Wall Street Journal, P. B4. Retrieved on July 10, 2017 from https://www.wsj.com/articles/why-your-phone-will-be-the-key-to-atms-of-the-future-1499598001

Fritz, B., Mickle, T. (2017, July 9). Apple loses ground in the digital-movie battle. The Wall Street Journal, P. B1, B2. Retrieved on July 10, 2017 from https://www.wsj.com/articles/apples-itunes-falls-short-in-battle-for-video-viewers-1499601601

Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P., and Chari, S. (2013). Perceived security risks in mobile interaction. Symposium on Usable Privacy and Security (SOUPS) 2013, July 24-26, 2013, Newcastle, UK

Potgieter, A. (September 18, 2015). The application preferences of undergraduate university students: A longitudinal study', *South African Journal of Information Management* 17 (1). Art. #650, 6 pages. Retrieved on July 1, 2017 from http://dx.doi.org/10.4102/sajim.v17i1.650

Soukup, P.A., SJ. (2015). Smartphones. Communication Research Trends. Vol. 24, No. 4 pp 1-39.

Statistica, (2016). The statistics portal. Number of free and mobile app store downloads worldwide from 2011 to 2017 (in billions). Retrieved on July14, 2017 from www. Statistica.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Zhu, H., Xiong, H., Yong, G., Chen, E. (2014). Mobile App recommendations with security and privacy awareness. University of Science and Technology of China, Rutgers University, UNC Charlotte. Retrieved from http://dx.doi.org/10.1145/2623330.2623705

ISSN: 2167-1508
v10 n4525

Appendices and Annexures

Table 3: Chi-Square Analysis of Applications Downloaded Versus Security and Privacy Awareness

Application	Disabled Location Services	Clear Browsing History	Have Anti-Malware Software	Read Terms of Use
Facebook	0.05	0.548	0.135	0.296
Twitter	0.405	0.66	0.195	0.351
Instagram	0.134	0.179	0.021	0.04
Snapchat	0.29	0.682	0.049	0.06
Accessing Email	0.936	0.166	0.485	0.951
Playing Games	0.942	0.632	0.829	0.65
Listening to Music	0.7	0.252	0.438	0.16
Reading Books	0.607	0.626	0.267	0.291
Searching for information	0.468	0.943	0.729	0.93

Table 5: Participants Undertaking Security / Privacy Activities Based upon Applications Downloaded

Application Downloaded	Location Services Disabled	Browsing History Cleared	Phone Backed up	Anti-Malware Installed	Another Person Access Your Phone	Read Terms of Use
Facebook	61.29%	52.42%	26.61%	17.74%	61.29%	25.81%
Twitter	43.55%	37.90%	21.77%	15.32%	42.74%	15.32%
Instagram	50.00%	44.35%	21.77%	12.10%	49.19%	15.32%
Snapchat	54.03%	46.77%	24.19%	14.52%	54.03%	17.74%
Accessing Email	75.00%	66.94%	29.03%	26.61%	75.00%	30.65%
Playing games	47.58%	42.74%	20.16%	16.13%	48.39%	18.55%
Listening to music	68.55%	61.29%	25.81%	22.58%	70.16%	25.81%
Reading books	25.81%	24.19%	12.10%	11.29%	26.61%	12.90%
Searching for information	70.16%	62.10%	29.03%	25.00%	71.77%	29.03%

Table 6: Participants Undertaking Security / Privacy Activities Based upon Number of Applications Downloaded

Number of Apps Downloaded	Location Services Disabled	Browsing History Cleared	Anti-Malware Installed	Another Person Access Your Phone	Read Terms of Use	Uninstalled / Not installed an App	Not Installed After Learning About App	Uninstalled After Learning About App
1-10	22.68%	23.53%	38.24%	25.32%	17.50%	29.31%	22.09%	27.78%
11-20	39.18%	35.29%	20.59%	37.97%	37.50%	34.48%	38.37%	36.11%
21-30	19.59%	20.00%	20.59%	22.78%	15.00%	18.10%	18.60%	16.67%
31-40	4.12%	5.88%	8.82%	6.33%	12.50%	4.31%	6.98%	5.56%
40+	14.43%	15.29%	11.76%	7.59%	17.50%	13.79%	13.95%	13.89%
Total	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%