Mobile Applications: Exploring User Decisions Related to Passive and Exploitative Application Permissions

Early stage paper

Deanna House
University of Nebraska at Omaha
deannahouse@unomaha.edu

ABSTRACT

Research surrounding mobile applications and privacy has taken a variety of perspectives into consideration. However, research on mobile application permissions is continuously evolving as the permissions have evolved. The user is responsible for making permission selection decisions when installing an application. This is particularly impactful when considering mobile application trends over time, as is demonstrated and discussed in this research. First, permissions for top 50 free and top 50 paid applications were collected during three different points in time and three separate versions of Android OS in order to explore permission trends for free and paid applications. This research in progress paper aims to explore the effects that exploitative versus passive permissions and application category (free versus paid) have on a user's intention to install a mobile application. Additionally, the terms exploitative and passive permissions are defined, with a planned experiment and survey.

Keywords

Mobile application permissions, exploitative, passive, mobile application privacy, Android

INTRODUCTION

The emergence of Smartphones as useful and necessary devices is upon us. While the usefulness of Smartphones is an impactful area of study, the privacy concerns of Smartphone users are an area of study that needs to be explored as worldwide Smartphone saturation occurs. There are over 4.7 billion 4G mobile subscriptions and 570 million 5G mobile subscriptions in the world (Ericsson, 2022). In the US alone, smartphone penetration has reached 92% (Nielson, 2021). Mobile phones store private, highly sensitive information such as contacts, videos, notes, and photos (Nauman et al., 2015). Mobile applications are widely used, with 255 billion applications downloaded in 2022 (Statista, 2022) and the average number of apps installed by users at 40 with the 21-30 age group installing an average of 67 apps (Kataria, 2023). There are currently over 2.67 million apps on the Google Play Store (Statista, 2023). Mobile permissions have been previously been studied in various contexts such as mobile banking applications (Ferris, Stahle, & Baggili, 2014); risks (Chia, Yamamoto, & Asokan, 2012); and privacy concerns (Gu, Xu, Xu, Zhang, & Ling, 2017).

Mobile applications provide convenience, enjoyment, and time savings for users, but also open up a floodgate of potential violations to privacy. As mentioned by Riopel (2016) it is common for users to believe that if no private information is disclosed, they will remain anonymous. Concerns related to the disparity between the assumed level of mobile privacy and actual privacy are growing. The digital footprint created by mobile devices can be used to pinpoint user-level information. For example, a study by Welke et al. (2016) found that 99.67% of the 46,726 users/devices were not anonymous/had a unique app signature based on usage patterns of the top 500 most frequent apps. Research conducted in 2011 found that over 10% of applications request permissions that are unneeded (Felt et al., 2011). These unneeded permissions can put the user at risk of unintentionally or unknowingly disclosing personal information. In addition, any developer can write an Android application without being validated before it goes to the Google Play Store (Sokolova, 2017).

In prior versions of Android, granular permission selection was not a feature that was available (Licorish, MacDonell, & Clear, 2015). However, versions beyond Andriod 6.0, Marshmallow (beginning with limited release in May 2015) allow users to deselect some permissions at the time of installing the application and to see permissions at runtime. However, this process is overcomplicated. And while Android is mostly built using a permission restrictive access model, this requires users to grant or deny permissions on an app by app basis. This is further complicated by the fact that users frequently miss which permissions are being granted to applications entirely (Chennamaneni, & Gupta, 2022).

While giving users an option to have more control over permissions granted or denied was seen as a benefit, putting the onus of permission granting/denying on the user has also opened up additional vulnerabilities and the potential for abuse. Lack of understanding can be a key component in the success of an exploitation related to mobile permissions (Chia et al., 2012). In addition, lack of user-awareness of possible risks related to security and privacy in mobile applications is concerning (Ikram et al., 2017). Android systems are designed with a multi-layered security approach; which protects the Operating System and other functions but places a dependency on the user at the application permissions layer. This is the most external facing layer of security and creates a weak link in Android security (Kumar et al, 2018). Applications request access to personal information which is granted by users (consciously or unconsciously) (De Santo & Gaspoz, 2015). Also, of great concern, is the reliance on the users for security integrity; that they must know and understand what the permissions are using/accessing (Lane, 2012). In addition, users are asked to approve permissions prior to the installation of an application, which can result in prompt fatigue/ignoring the prompt (Roesner, 2017; Motiee et al., 2010).

Permissions within Android should provide a layer of security, however, as found by Sokolova et al., 2017, applications can abusively collect information that is not related to the application functionality. The user's concern related to device resource access varies greatly, with some user's using extreme caution for resource use and others having a more relaxed approach (Licorish, MacDonell, & Clear, 2015). As mentioned by De Santo & Gaspoz (2015) there is a need to study user decisions related to installing mobile applications and to prevent private information leakage.

LITERATURE REVIEW

Privacy

The concept of privacy is not new and has been studied extensively. One of the pivotal views is that of Warren & Brandeis, 1890. They discuss the "intensity and complexity of life" which makes the need for "solitude and privacy" becoming "more essential to the individual" pp. 196. Additionally, to keep things private that an individual prefers remain private (Warren & Brandeis, 1890). As technological advances have occurred beyond that of the 1800's, privacy terms have evolved to include *informational privacy*, which includes the scope of a person's information that is individually identifiable (Smith et al, 2011). Privacy is a very important piece of a person's identity (Shilton, 2009). Clarke (1999) discusses information privacy when possessed by another entity and places responsibility of control over data and its use on the third party, where applicable. Privacy can also be explored from a sense of a common value – to oneself, to the public, and as a collective – which can create challenges to protect one person's privacy versus the privacy of all

(Regan, 1995). However, privacy intrusions and disclosure can result in moral harms, so it is imperative that individuals be able to maintain information control (DeCew, 2016).

Privacy in the Context of Mobile Phones

Related to mobile technologies and privacy, there are concerns with the use of information that may have been gathered with consent, yet is anonymized (Rumbold & Wilson, 2019). On a troublesome note, prior research such as that by de Montjoye (2013) found that mobile data is very unique to an individual and is easily identifiable. When a mobile phone user is faced with a decision to install a mobile application, they are provided with permissions that are needed in order to use that application. The risks to privacy are fairly vague for users when making a decision to install, with some concern related to privacy among users if primed, but the effects are not long lasting (Rajivan & Camp 2016). This is further complicated by the individuality of privacy, it varies greatly from person to person. As mentioned by Lee et al. (2011), consumer privacy concerns can be broken into 1) privacy unconcerned – sharing willingly; 2) privacy pragmatist – sharing only when privacy protection is adopted; and 3) privacy fundamentalist – never sharing. In the context of mobile phones, users that are privacy pragmatists and privacy fundamentalists have to make a concerted effort to utilize mobile applications.

THEORETICAL PERSPECTIVES

Privacy Paradox

The disconnect between privacy attitudes and privacy behavior has been well-documented in online behavior related to social network sites (van Noort, Antheunis, & Verlegh, 2014; Hallam & Zanella, 2017), Internet use (Park et al., 2012), and digital services (Karwatzki, Dytynko, Trenz,

& Veit, 2017). The privacy paradox is interesting such that consumers can be very concerned with privacy yet provide personal information in a variety of circumstances (Smith et al., 2011). This creates a bit of a contradiction in the attitudes towards behavior versus the actual behavior, with a discount or something of value causing individuals to give up that privacy – particularly when there is a low value of perceived risk (Syverson, 2003; Acquisti, 2004). Organizations that ask for private information can actually stimulate positive responses and feelings from consumers towards a brand and purchasing behaviors (van Noort et al., 2014). A study by Sutanto et al. (2013) explored the personalization-privacy paradox, which encompassed the unbalanced state of data exploitation by marketers to provide personalized product information to consumers. While consumers were found to have an increased use of personalized content, privacy did not have an effect on usage but product messages that were privacy-safe were saved over messages that were not. Specific to mobile applications, permissions vary from application to application, which can vary the choices of an individual on a permission-level. For example, an individual may place higher value on certain permissions (such as location or contacts) or others (network information).

Privacy Calculus

According to Xu et al. (2009), the calculus of information privacy explores individual privacy from a personal information/benefit exchange. Individuals explore the perceived benefits and perceived risks prior to disclosing private information (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Anderson & Agarwal, 2011). If individuals believe that there is something to gain, such as a perceived award, from giving up private information, they are more likely to do so (Miltgen & Smith, 2015). Monetary incentives have been shown to influence the disclosure of information (Hui et al., 2007). Access to information or a personalized service may be a motivation behind disclosing personal information (Xu et al., 2009). This trade-off is not absolute, but rather will vary from individual to individual (Klopfer & Rubenstein, 1977).

It is mentioned by Ciocchetti (2007) that when utilizing services that are free, there may be a decision made by an individual that determines PII to be too intrusive and a move to a less invasive competitor can be made. Individuals try to control outgoing private information to other parties (Stanton, 2003; Stanton & Stam, 2003; Sutanto et al., 2013). However, just exactly what can be traded and which permissions are more concerning to individuals has not been explored. There is a need for research related to privacy practices from the individual's point of view and how these viewpoints differ among individuals (Bélanger & Crossler, 2011).

Value of Personal Data and Transactional Privacy

The concept of personal data markets that allows a consumer to receive payment for the use of private data would not only provide users with monetary benefits but also the potential for better product marketing or early diagnosis and treatment of diseases (Adar & Huberman, 2001). In a study by Staiano et al., (2014), mobile users overall rated location data as the most valuable personally identifiable information (PII). Research by Hann et al, (2007) found that monetary reward motivated individuals to accept secondary use of PII. However, research by Wang et al. (2016) determined that individuals value rewards over potential risks when using mobile applications and disclosing personal information.

All of the above mentioned theoretical perspectives make privacy and the sharing of private information a complicated process. Additional insights surrounding the complexity and changing nature of Android mobile application permissions are discussed and summarized in the next section.

PRELIMINARY RESEARCH SURROUNDING MOBILE PERMISSIONS ON ANDROID DEVICES

Users decide if an application can access sensitive information through permissions (Roesner, 2017). A requested permission is a demand from an app for control of the mobile device and a user's personal information (Gu, et al. 2017). Android has several permission categories that vary based on the level of risks to a user's privacy. Table 1 below shows the permissions categories.

Permission Category	**Description**
Install-time	Give app limited access to restricted data or to perform restricted actions
Normal	Very little risk to user's privacy
Signature	Utilizes a certificate/is more secure
Runtime/Dangerous	Involves user's private information; requires that a user grant the permission at the time of install and/or runtime; access private user data
Special	Extremely sensitive; requires user approval at the time of usage along with a manifest and management screen

Table 1: Android Permission Categories (Android, n.d.).

The structure of Android applications has evolved over time to provide users with more control at the time of installation. Prior to setting up the experiment, the researcher sought to learn more about the permissions during a longitudinal timeframe over three unique versions of Android OS. The goal for these data collections was to gain a better understanding of applications and the various permissions that existed across free and paid application categories. This information also provided further understanding and refinement surrounding what would be considered an exploitative permission versus what would be considered a passive permission.

Live data was collected from the Google Play Store (https://play.google.com/store/apps) during three periods in time: 2015, 2019, and 2022. While the top 50 lists of applications change fairly frequently, there are a number of similar applications during each of the time periods. In 2015, Messenger was the #1 application in the free list (and TikTok did not exist). In 2019, Messenger was the #3 application and TikTok was #6. In 2022, TikTok was #1 and Messenger was #2 in the top 50 free category.

There are, however, some differences, such as the 2019 collection, games were included in both the free and paid top 50, whereas in 2022, there became a separate game top 50 category. In 2015 and 2019, Minecraft was the #1 paid application and in 2022 Minecraft is #1 in the paid game category. However, not all games are in the 2022 top 50 games category, as several of the Toca Life series are listed.

During the data collection in 2015, Lollipop was the version of operating system in place. This OS version required that users install all permissions with no choice to de-select permissions. During the 2019 data collection Android Pie was the version of OS in place. During the 2022 data collection Android 12 was the version of OS in place. While there have been various privacy protecting features that have been implemented by Android during these collection periods, additional permissions such as "precise location" have been added.

A longitudinal comparison of the top 50 free and top 50 paid application permissions across three points in time is shown in Figures 1 and 2 below.

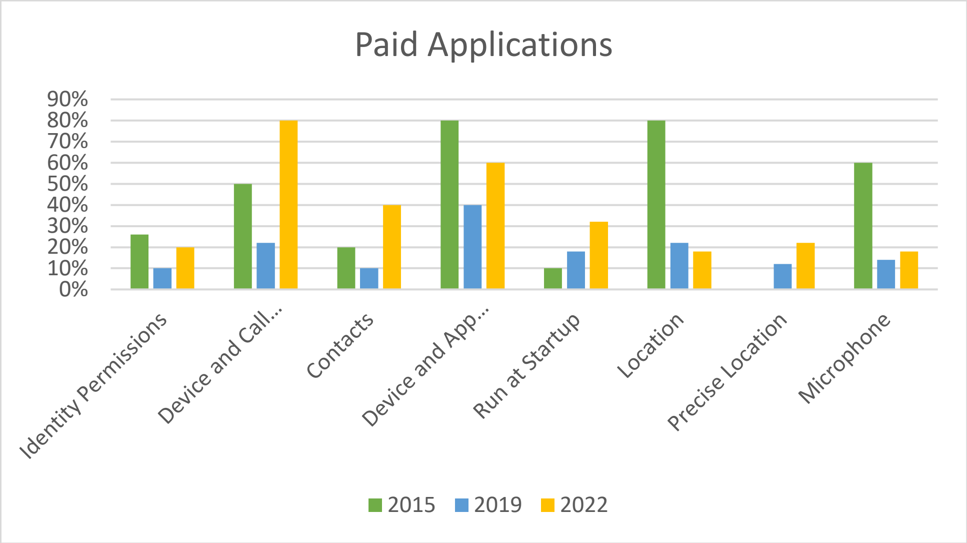

Figure 1: Top 50 Paid Application Selected Permissions, 2015, 2019, 2022

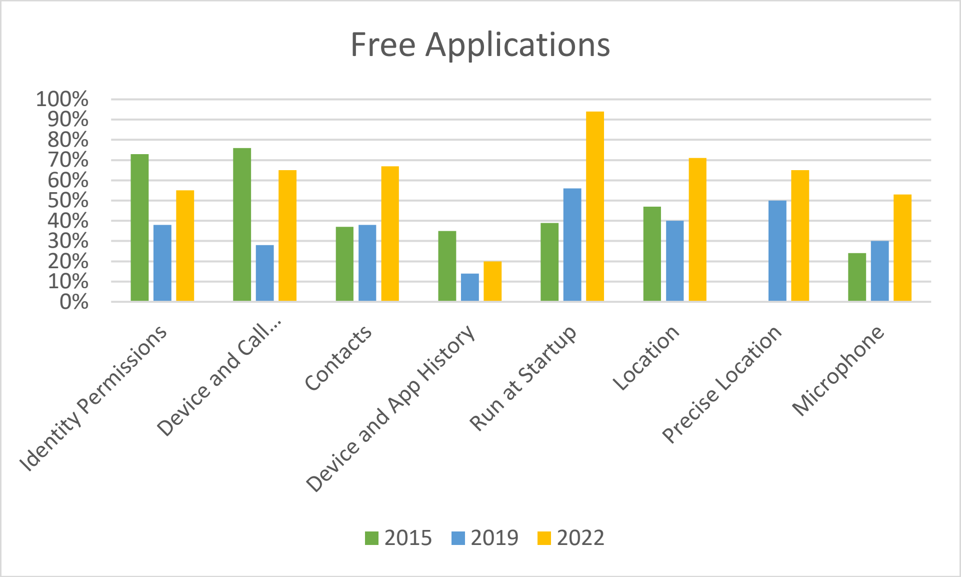

Figure 2: Top 50 Free Application Selected Permissions, 2015, 2019, 2022

This data shows that while some areas of application permissions have decreased over time for both the free and paid application categories, the more exploitative permissions such as location (and precise location) and microphone have increased on the free application side. The top 50 paid application data overall has a much smaller percentage of applications that use permissions, and frequently there is an application-specific reason for using the permission. This data helps provide a starting point to delve deeper into a research study that will explore behaviors related to mobile application installation intentions; particularly when an application is exploitative or on the opposite side, passive. The collected permission data also provides a detailed understanding of the types of permissions that are utilized by free or paid applications and will help inform the design of the experiment.

Exploitative versus Passive Permissions

While the terms exploitative and passive are terms that were developed by the author in this research, they have a very specific context in consideration of mobile applications. Exploitative applications are defined as those that ask for a wide range of PII (personally identifiable information) above and beyond the core functionality of the app. According to dictionary.com, exploitative is defined as "taking unfair or unethical advantage of a person, group, or situation for the purpose of profit, comfort, or advancement". On the opposite side, research surrounding passive technology can be seen as that which does not intrude upon the user (Laine & Nygren, 2016). Thus, passive applications are those that do not ask for PII above and beyond the core functionality of the app. This research will explore the influence that exploitative permissions and passive permissions may have on an individual's intention to install a mobile application.

This leads to the research questions for the study, as mentioned below.

RESEARCH QUESTIONS:

Do permissions that are exploitative affect a user's decision to install a mobile application?

Do permissions that are passive affect a user's decision to install a mobile application?

Does application category (free, paid) affect a user's decision to install a mobile application?

METHODOLOGY

The methodology for this research project will an experiment in addition to a questionnaire. While there have been numerous studies surrounding mobile application privacy as Smartphone use has increased, there is a need to find out more user's behavior related to the decision making that occurs surrounding permissions when installing a mobile app. This project will explore the installation intentions for mobile applications that are exploitative or passive with categories that are free or paid applications.

Participants will be shown example mobile application screens and mobile application terms of agreement/permissions screens. These application designs will be set up as a 2X2 with Permission Category (Passive, Exploitative) and Application Category (Free, Paid). In order to prevent bias, the application screens will be a fictitious yet realistic generic application. The treatments will be randomly assigned to each participant. Participants will be required to be 19+ years of age and current users of Android devices. The passive permission category will ask for permissions that do not go above and beyond the functionality of the application. The exploitative permission category will ask for permissions that go above and beyond the functionality of the application. Price and permissions will be manipulated in the design screens. The participants will then click on their intent to install these applications. Participants will then fill out survey questions related to privacy, mobile application behavior, perceived risk, and mobile application use.

Mobile Exploits

While providing permissions to mobile applications can seem innocuous to the average mobile application user, extensive research has been conducted on attacks and exploits. While this list is by no means exhaustive, there are a number of studies with concerning findings related to a user's privacy. Data leakage related to application permissions can initiate privacy exploiting events for users. For example, Ikram (2016) studied VPN apps and found a number of concerning practices such as tunneling without encryption, traffic forwarding through third parties, and abusive related to ad tracking and traffic redirection. Matte et al., 2015 found that geolocation on Android applications can launch a successful attack on a single device. Additional research by Archara et al. (2014) determined that ACCESS_WIFI_STATE and its related methods put users at serious risk of information leakage related to travel history, geolocation, and social networks. Location services can be utilized as a feature that is desirable to a user from a convenience perspective (Xu et al. 2010). However, one of the greatest threats to privacy is knowledge of location (Gambs et al., 2010). Location information by inference can be used to build a behavioral profile of a targeted individual (Gambs et al., 2010). If this information is shared with a third party, there is also a risk to a user's information privacy (Lane, 2012).

Additionally, anytime an update occurs, a privilege escalation attack can happen (Neisse et al., 2016). Lastly, this research has focused on application permissions at the time of install, runtime permissions are another method that require user decision making when the app is being used, which can create another vector for exploitation of a user's privacy (Wang et al. 2023).

CONTRIBUTIONS TO RESEARCH AND PRACTICE

This research will explore the perceptions of privacy related to free versus paid mobile applications. As mentioned in the privacy calculus, there is a trade-off when providing personally identifiable information. Ferris et al., (2014) discussed the need for permission-specific risk assessment research; particularly on the Android side where security categories are lacking related to reliability and specificity.

This research will also explore installation decisions related to application permissions that are related to the functionality of the application or *passive* and also installation decisions related to application permissions that go beyond the functionality or *exploitative*. As the number of users with access to mobile applications increases and becomes more available to the general public, the burden of user security and permissions is placed on the user. These users are frequently not technically savvy and are unable to make an informed decision related application permissions and installation. Providing information to a mobile application opens users up to security exploitations. Making users aware of these potential exploitations can help maintain a more secure environment overall.

Users with varying levels of security and privacy knowledge and proficiency are forced to make snap judgments about allowing mobile applications access to personal data. This research will help explore the different decisions related to installing a mobile application based on level of privacy and cost. As mobile application security changes, it is up to the user to determine which permissions are being used for an application and which are being used for purposes of profit.

LIMITATIONS AND CONCLUSION

While this study focuses on Android devices and Google Play Store applications to maintain a consistent privacy and permission framing, iOS devices are also at risk and future studies should explore the choices that are made by iPhone users. Traditionally, Apple has protected users from malware and dangerous apps due to a number of safety checks and balances. However, in recent years there have been a number of studies highlighting security and privacy vulnerabilities (Kundaliya, 2021; Seals, 2021; WSJ Pro, 2019).

This research study will utilize mobile permission data across multiple points in time to frame the data collection/methodology. As the burden of protecting one's privacy is placed on the user, it is important to conduct research such as this to understand more nuanced areas surrounding application permission decisions during installation.

KEY CHALLENGES

This paper has a challenging methodological setup and involves careful consideration for permissions that would be categorized as passive versus those that would be categorized as exploitative. It is important to ensure an adequate theoretical framework drives the data collection methods on the experimental and survey data collection sides. There is also still work that needs to be done to determine what a model might look like and that all key areas in prior work are covered before data collection begins.

ACKNOWLEDGEMENTS

The author would like to thank Carson Seaman and Sweetha Moorthi for their assistance with data gathering for permissions and screen design. This research was supported by grants from Ohio University MIS EY seed grant and the University of Tampa College of Business Dean's Course Release Research Award.

REFERENCES

Acquisti, A. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. In EC '04 Proceedings of the 5th ACM Conference on Electronic, USA, 21 – 29.

Andriod. (n.d.) Retrieved March 10, 2023 from https://developer.android.com/guide/topics/permissions/overview.

Archara, J.P., Cunche, M., Roca, V., & Francillion, A. 2014. WifiLeaks: Underestimated Privacy Implications of the access_wifi_state Android Permission. WiSec '14: Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks. 231-236.

Barth, S. & de Jong, M.D.T. 2017. The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. *Telematics and Informatics,* 34(7), 1038 – 1058.

Bélanger, F. & Crossler, R.E. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35(4), 1017 – 1041.

Chennamaneni, & Gupta, B. 2022. The Privacy Protection Behaviours of the Mobile App Users: Exploring the Role of Neuroticism and Protection Motivation Theory. *Behaviour & Information Technology*, *ahead-of-print*(ahead-of-print), 1–19.

Chia, P.H., Yamamoto, Y., & Asokan, N. 2012. Is This App Safe?: A Large Scale Study on Application Permissions and Risk Signals. In Proceedings of the 21st international conference on World Wide Web (WWW '12). ACM, New York, NY, USA, 311-320. DOI=http://dx.doi.org/10.1145/2187836.2187879.

Ciocchetti, C.A. 2007. E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. American Business Law Journal, 44(1), 55 – 126.

Culnan, M. J., & Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." Organization Science, (10:1), pp.104–115.

de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., & Blondel, V.D. 2013. Unique in the Crowd: The Privacy Bounds of Human Mobility. *Scientific Reports,* 3(1376), 1 – 5.

De Santo, A. & Gaspoz, C. 2015. Influence of Users' Privacy Risks Literacy on the Intention to Install a Mobile Application. New Contributions in Information Systems and Technologies. Rocha, A., Correia, A.M., Costanzo, S., & Reis, L.P. (eds.), pg. 329 – 341.

Dinev, T., & Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," Information Systems Research, (17:1), pp. 61–80.

Ericsson 2021. Ericsson Mobility Report. Retrieved February 20, 2020 from: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-subscriptions-outlook.

Felt, A.P., Greenwood, K., & Wagner, D. 2011. The Effectiveness of Application Permissions. In Proceedings of the 2nd USENIX conference on Web application development (WebApps'11). USENIX Association, Berkeley, CA, USA, 1-12.

Ferris, B., Stahle, J., & Baggili, I. 2014. Quantifying the Danger of Mobile Banking Applications on the Android Platform. *9th Annual Symposium on Information Assurance,* June 3-4, 2014, Albany, NY, 65 – 70.

Gambs, S., Killijian, M.O., & del Prado, M.N. (2010). Show Me How You Move and I Will Tell You Who You Are. SPRINGL '10, November 2, 2010, San Jose, CA.

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective. Decision Support Systems, 94, 19 – 28.

Hallam, C. & Zanella, G. (2017). Online Self-Disclosure: The Privacy Paradox Explained as a Temporally Discounted Balance Between Concerns and Rewards. *Computers in Human Behavior,* 68, 217 – 227

Ikram, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M.A., & Paxson, V. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps. Presented at ICM 2016, November 14 – 16, 2016, Santa Monica, CA, USA.

Kataria, M. 2023. App Usage Statistics 2022 that'll Surprise You (Updated). Retrieved February 25, 2023 from https://www.simform.com/blog/the-state-of-mobile-app-usage/.

Klopfer, P.H. & Rubenstein, D.I. 1977. The Concept Privacy and its Biological Basis. Journal of Social Issues, 33(3), 52 – 65.

Kumar, A., Kuppusamy, K.S., & Aghila, G. 2018. FAMOUS: Forensic Analysis of MObile Devices Using Scoring of Application Permissions. *Future Generation Computer Systems,* 83, 158-172.

Kundaliya. 2021. Computing - Incisive Media: Apple releases urgent security update to address critical spyware vulnerability. Computing.

Laine, & Nygren, E. 2016. Active and Passive Technology Integration: A Novel Approach for Managing Technology's Influence on Learning Experiences in Context-Aware Learning Spaces. *Technology, Pedagogy and Education*, *25*(1), 19–37.

Lane, M. (2012). Does the Android Permission System Provide Adequate Information Privacy Protection for End-Users of Mobile Apps? In Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, December 3 – 5, 2012.

Lee, D.J., Ahn, J.H., & Bang, Y. 2011. Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Quarterly,* 35(2), 423 – 444.

Licorish, S.A., MacDonell, S.G., & Clear, T. 2015. Analyzing Confidentiality and Privacy Concerns: Insights from Android Issue Logs. EASE 2015,Nanjing, China, April 27 – 29, 2015.

Lo Iacono, Gorski, P. L., Grosse, J., & Gruschka, N. 2017. Signaling Over-Privileged Mobile Applications Using Passive Security Indicators. *Journal of Information Security and Applications*, *34*, 27–33.

Matte, C., Achara, J.P., & Cunche, M. 2015. Short: Device-to-Identity Linking Attack Using Targeted Wi-Fi Geolocation Spoofing. *WiSec '15*, June 22-26, New York, NY.

Miltgen, C.L. & Smith, H.J. 2015. Exploring Information Privacy Regulation, Risks, Trust, and Behavior. Information & Management, 52(6), 741 – 759.

Motiee, S., Hawkey, K. & Beznosov, K. 2010. Do Windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices. Proceedings from the Symposium of Usable Privacy and Security (SOUPS), July 14 – 16, Redmond, WA.

Nauman, M., Khan, S., Othman, A.T., & Musa, S. 2015. Realization of a User-Centric, Privacy Preserving Permission Framework for Android. Security and Communications Networks, 8, 368 – 382.

Neisse, R., Steri, G. Geneiatakis, D., & Fovino, I.G. 2016. A Privacy Enforcing Framework for Android Applications. *Computers & Security,* 62, 257 – 277.

Nielsen. 2021. The Nielsen Total Audience Report 2021. Retrieved February 20, 2022 from: https://www.nielsen.com/us/en/insights/report/2021/total-audience-advertising-across-todays-media/

Rajivan, P. & Camp, J. 2016. Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices. Symposium on Usable Privacy and Security (SOUPS), June 22 – 24, Denver, CO.

Riopel, S.L. 2016. The Price of Free Mobile Apps Under the Video Privacy Protection Act. American University Business Law Review, 6(1), 115-136.

Roesner, F. 2017. Designing Application Permission Models that Meet User Expectations. IEEE Security & Privacy Magazine, (Jan/Feb), 75 – 79.

Seals. 2021. Apple Mail Zero-Click Security Vulnerability Allows Email Snooping. In Threatpost [Blog]. Newstex.

Shilton, K. 2009. Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection. *Communications of the ACM,* 52(11), 48 – 53.

Sokolova, K., Perez, C., & Lemercier, M. 2017. Android Application Classification and Anomaly Detection with Graph-Based Permission Patterns. Decision Support Systems, 93, 62 – 76.

Statista. 2023. Number of Mobile App Downloads Worldwide 2016-2022. Retrieved on February 25, 2023 from https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/.

Statista. 2023. Number of available applications in the Google Play Store from December 2009 to March 2023. Retrieved on March 11, 2023 from https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/.

Sutanto, J., Palme, Elia, Tan, C.H., & Phang, C.W. 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment of Smartphone Users. *MIS Quarterly,* 37(4), 1141 – 1164.

Sverson, P. 2003. The Paradoxical Value of Privacy. In 2nd Annual Workshop on Economics and Information Security – WEIS '03.

Wang, T., Duong, T.D., & Chen, C.C. 2016. Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective. *International Journal of Information Management,* 36, 531 – 542.

Wang, Y., Wang, Y., Wang, S., Liu, Y., Xu, C., Chueng, S.C., Yu, H., & Zhu, Z. 2023. Runtime Permission Issues in Android Apps: Taxonomy, Practices, and Ways Forward. *IEEE Transactions on Software Engineering,*49(1), 185-210.

Welke, P., Andone, I., Markowetz, A., & Blaszkiewicz, K. 2016. Differentiating Smartphone Users by App Usage. Presented at UBICOMP 2016, September 12-16, 2016 in Heidelberg, Germany.

WSJ Pro. 2019. Cyber Daily: Schools Are a Cybersecurity Battleground; Apple Re-Opens iOS Vulnerability; Hackers Attack U.S. Government Agencies.

www.dictionary.com. (n.d.) Exploitative. Retrieved March 10, 2023 from https://www.dictionary.com/browse/exploitative.

Xu, H., Teo, H., Tan, B.C.Y., & Agarwal, R. 2009. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. Journal of Management Information Systems, 26(3), 135 – 173.

Xu, F., He, J., Wright, M., & Xu, J. (2010). Privacy Protection in Location-Sharing Services. Proceedings of the International Conference on Computer Application and System Modeling, Taiyuan, China, October 22 – 24, 2010.