2014-11-01

A Privacy Risk Scoring Framework for Mobile

Jedidiah Spencer Montgomery
Brigham Young University - Provo

A Privacy Risk Scoring Framework for Mobile Applications and Platforms

Jedidiah Spencer Montgomery

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Barry M. Lunt
Richard Helps

School of Technology

Brigham Young University

November 2014

ABSTRACT

A Privacy Risk Scoring Framework for Mobile Applications and Platforms

Jedidiah Spencer Montgomery
School of Technology, BYU
Master of Science

Protecting personal privacy has become an increasingly important issue as computers become a more integral part of everyday life. As people begin to trust more personal information to be contained in computers they will question if that information is safe from unwanted intrusion and access. With the rise of mobile devices (e.g., smartphones, tablets, wearable technology) users have enjoyed the convenience and availability of stored personal information in mobile devices, both in the operating system and within applications.

For a mobile application to function correctly it needs permission or privileges to access and control various resources and controls on the mobile device. These permissions can range from location and account information to access to all storage on the mobile device. A single permission, or a combination of permissions, could lead to a high risk of potential privacy invasion. This privacy invasion risk can be amplified specifically for security applications when compared to non-security applications due to the administrative privileges that security applications frequently need to moderate and protect information on a mobile device. Currently there is no defined matrix or framework for analyzing privacy risks for any mobile platform, including the main mobile platforms of Android, iOS and Windows mobile.

The purpose of this research is to create a framework for analyzing mobile application permissions and identify potentially invading permission. The framework produces a Privacy Invasion Profile (also known as a PIP) for each application, which can be used to compare the risk of privacy invasion for a specific application.

Keywords: mobile, smartphone, tablet, privacy, invasion, security, application, risk, framework

ACKNOWLEDGEMENTS

I am so thankful for my wonderful wife, Katie, for all of the support that she gave me throughout my education, especially during my graduate studies. I would also like to thank the faculty in the School of Technology for all of the guidance, help, and feedback they gave to me throughout the entire thesis research process. Lastly, I would like to thank my family and friends for all of the support and help that they have given me over the years.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This research builds a framework for analyzing the potential for privacy invasion on mobile devices. Analyzing a select set of applications across the main mobile platforms demonstrates that the framework correctly evaluates permissions requested by mobile applications. This framework is intended to provide a means to evaluate privacy information about mobile applications in a format that is easy for the typical end-user to read and understand.

1.1 Working Definition of Privacy

There are many different definitions of privacy (discussed in Chapter 2). To avoid confusion, the following is used as a definition through the remainder of this thesis:

Privacy – The ability to control, manage and withhold information about oneself and information specific to an individual from outside parties, including; individuals, groups, companies and other entities. Private information is specific information about who someone is (e.g., location information including current, historical and recurring), what someone has (e.g., phone number, email address, social security number, credit card information, contact information) and what someone knows (e.g., shopping, web browser, preferences). The more personal or private the information the greater the expectation of privacy: for example, information such as phone number, location information, and address will be more protected and private than information such as browser preferences.

Throughout the remainder of this thesis, the above definition is referred to as the Working Privacy Definition, or WPD.

1.2 Nature of the Problem

Privacy-invasion risks are frequently overlooked and underestimated when installing and using an application on a mobile device, such as a smartphone or tablet. Information privacy is an important topic for both individuals and corporations. Privacy has become even more prominent as information availability and dissemination have increased with mobile devices and personal computers.

This research focuses on the risk of privacy invasion for mobile devices, including, but not limited to, smartphones, tablets, PDAs, e-readers, and other similar devices. Hereafter, a mobile device is referred to as a MobDev. MobDevs store and manage more personal information, than ever before, including, but not limited to a wide range of account credentials, banking information, personal information, application information and usage, personal contact information, and GPS location information. The information requested by these features and applications results in the threat of privacy invasion, especially when an application requests a combination of permissions and privileges.

Are the trade-offs between the risk of privacy invasion and information accessibility in mobile applications acceptable? Can users have any expectation or perception of privacy when these mobile applications could have access to a wide variety of personal information? How can the risk of privacy invasion be measured and analyzed?

1.3 Purpose of the Research

The purpose of this research includes the following actions and research:

1. Develop a framework for mobile application privacy analysis that is suitable for the following:
    a. Use the framework developed to score mobile applications such that it conveys information risks in the context of privacy. A scoring matrix has been designed for the benefit of a general audience as opposed to a technical or security-based audience.
    b. Compare and contrast permissions, risks, and classifications across multiple mobile platforms and between various popular mobile applications. This comparison and contrast is used to verify that the framework functions.

1.4 Justification

As of the beginning of this research, no previous work has been done to create a cross-platform scoring and analysis framework for providing a comparison between various mobile platforms. Extensive research has been done into how the various platforms have analyzed how personal information could be shared or lost from a mobile device. However, no type of analysis framework has been created to assist in risk classification for applications and the likelihood that the permissions provided to that application could invade the personal privacy of the owner of that mobile device.

1.5 Project Approach

The focus of this research is to design a simple and easy-to-evaluate framework for analyzing mobile privacy. Categorizing and classifying mobile applications according to their potential for privacy invasion provides detailed information about what is being put at risk by installing and agreeing to various permission and privilege requests by mobile applications. This categorization is based on the permissions requested by an application.

The evaluation of this framework is limited to tablets and phones from the three major mobile platforms (Android, iOS, and Windows Phone) and concentrates on privacy risks for mobile applications on these devices. The framework creates a scoring matrix for mobile applications. To demonstrate that the framework functions correctly, a variety of applications and mobile operating systems are evaluated then scored based on the framework's scoring matrix developed as part of this research. The framework analyzes all permissions requested by an application, assuming that no permissions have been disabled by permission management applications or settings by the owner and user of the MobDev. With those permissions, a Privacy Invasion Profile (PIP) based on criteria defined and applied throughout this research is created for each application and compared with the PIPs created for other applications on the same and other mobile platforms.

1.6 Research Questions and Hypotheses

The following questions and hypotheses are addressed by this research:

- **Question 1 (Q1):** What are the risks to information privacy on MobDevs and how are these currently represented by application permissions?

- **Hypothesis 1 (H1):** A framework for mobile applications permissions analysis across platforms can robustly reveal privacy risks for MobDevs.
- **Hypothesis 2 (H2):** The framework demonstrates through an analysis of current applications across multiple platforms that it is effective in identifying privacy concerns and risks.
- **Question 2 (Q2):** Are the permissions requested by security applications (e.g. mobile antivirus programs) greater than those requested by other applications and does this increase the risk to information confidentiality?

1.7 Definitions

- MobDev – A mobile device such as a smartphone, tablet, PDA, e-reader, biosensors, Google Glasses, smart watch, or other similar small personal computer. In this research, a MobDev specifically refers to smartphones and tablets.
- Mobile App (or App) – Software installed on a MobDev. These applications can range from mobile adaptations of social websites, such as Facebook, LinkedIn, or Twitter, to mobile versions of desktop software, such as Evernote, OneNote, or Pandora, to mobile specific security applications, including Norton Security antivirus, Avira Antivirus Security, and McAfee Antivirus & Security ("App Store Downloads on iTunes" 2014; "Android Store (Google Play Store)" 2014).
- Privacy or Working Privacy Definition (WPD) – A working definition of privacy is defined in section 1.1 of this thesis and applies as a working definition throughout the remainder of this document.

- Privacy Invasion Profile (PIP) – A profile created based on the permissions and combination of permissions that a mobile application requests.
- Create, Read, Update and Delete (CRUD) – Basic data manipulation and management term. Most mobile applications' permission-grant CRUD access to the feature that is accessed; however, some only have "read" access. Read access is the only permission needed to invade privacy and is the only factor contributing to the PIPs being developed in this thesis. Hereafter, create, read, update, and delete access is referred to as CRUD access.
- Mobile Platform – Mobile platforms include such devices as e-readers, smartphones, feature phones, tablets, smart watches, Google Glasses®, and other similar devices. This thesis focuses specifically on applications developed for and deployed on smartphones and tablets. All mobile operating systems are used in their original form as the company intended for the mobile platform to implement the operating system. This includes not jailbreaking, rooting, or otherwise modifying a mobile platform's operating system. When a mobile platform is referenced in this thesis it refers specifically to the following three platforms:
    1) Android tablets/phones as produced by Google, Inc. No custom ROMs or rooted devices were used in this research.
    2) iPhone/iPad as produced by Apple Inc. No jailbroken devices were used as part of this research.
    3) Windows Phone as produced by Microsoft.

1.8 Limitations on Framework Evaluation

Limitations of the evaluation of the framework include the following specifications:

1. The only mobile devices that were tested were tablets and phones running Android, iOS, and Windows Phone. Despite these limitations, the scoring matrix contains elements that are applicable to other mobile devices and mobile platforms. The specific versions of tablets that were used throughout this thesis are listed in Table 1-1:

Table 1-1: Selected Mobile Devices and Device Specifications

Device	Platform	Device Specifications
Nexus 5	Android	2013 T-Mobile version. Technical Specifications include 16 GB of internal storage, 2GB of RAM running Android 4.2.2 to 4.4.4
Nexus 10	Android	2012 Wi-Fi only version. Technical specifications include 32 GB of internal storage, 2GB of RAM running Android 4.2.2 to 4.4.4
Nexus 7	Android	2012 Wi-Fi only version. Technical specifications include 16GB of internal storage, 2GB of RAM running Android 4.2.2 to 4.4.4.
iPad Mini	iOS	2012 Wi-Fi only version. Technical specifications include 16GB of internal storage, dual core A5 processor running iOS 7.1.1 to 7.2.1.
Nokia 521	Windows Phone	2013 T-Mobile version. Technical specifications include 512MB of RAM, 8GB of internal storage running Windows Phone version 8.0.10517.150

2. The potential for cost-inferring permissions (e.g. in-app purchases, costs money, premium rate SMS/MMS/phone calls etc.) are not considered privacy-invading permissions. Due to the fact that no personal information is gathered or transmitted, cost-inferring permissions are not considered privacy invading and are therefore not within the scope of this research. This research focuses specifically on the gathering and dissemination of personal information, preferences, and actions.

3. Analysis of permissions is limited to permissions requested by an application. Monitoring of network connections and traffic to identify, decrypt, and analyze breaches in privacy not indicated by granted permissions are out of scope.
4. Government regulations, laws, and other similar literature supporting this research were limited to documents based in the United States, following US expectations and policies.
5. Any updates or patches provided by the MobDev manufacturer or developer were applied. This provides the most current and accurate picture of mobile platforms' privacy management and definitions while still allowing the framework to provide insight to the privacy implications of mobile operating systems and mobile applications.

2 LITERATURE REVIEW

This chapter reviews privacy research (current and historical), digital privacy, and practical implementations of privacy features for each of the primary mobile platforms (Android, iOS, and Windows Phone).

2.1 Current and Historical Digital Privacy Expectations

Throughout history, many people, groups, and other entities have attempted to define privacy, especially in relation to digital communications. Thomson stated that "the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is" (Thomson 1975) With nobody having a clear sense of privacy, Westin attempted to provide a groundwork for the definition of digital privacy in this statement: "With the rise of communication equipment and computing systems, the notion of information privacy has emerged, which has been initially defined as 'the claim of individuals . . . to determine for themselves when, how and to what extent information about them is communicated to others'" (Christin et al. 2011; Westin 1968). Privacy as a term in and of itself is hard to define, as it is more of a concept, idea, or principle, not a soundly defined expression.

The foundation of modern policies relating to digital and personal privacy comes from our non-digital history and is based on unalienable rights as defined in the Bill of Rights.

> Much of our modem conception of privacy is grounded in the Fourth Amendment's mandate that individuals 'shall be secure in their person, houses, papers and effects' from unreasonable government intrusion. Though it may sound like a blanket grant of protection, the scope of the Fourth Amendment is actually limited. Katz vs. United States, a wiretap case, established that people are protected from unwarranted government intrusion only in situations where: (1) they have a subjective expectation of privacy; and (2) that expectation is one society is prepared to recognize as 'reasonable.' Since only 'reasonable' expectations of privacy will be honored, for information to receive protection it must meet this threshold. (Levis 2011).

While the Fourth Amendment may be the basis for digital statutes and concepts it does little to define how digital privacy is defined today. This gap in privacy definition was further displayed by Levis when he stated:

> Because the Court has failed to nail down a clear objective standard to measure society's expectations, particularly within the digital context, judging what society is willing to recognize as reasonable has become a very flexible standard. This flexibility might be seen as a virtue that allows certain societal interests in security, such as airline security, to trump an individual's desire for privacy. However, it is also concerning that an individual's interest in privacy hinges "on whether 'society'—e.g., some unspecified group of other individuals—approves of such protection." This is even more concerning when it becomes one step removed and a judge is deciding what society is willing to recognize as reasonable. (Crowther 2012)

Lipton further detailed this lack of clarity in digital privacy definitions and the subsequent risk in his statement:

> By contrast, the United States has never been particularly focused on protecting individual privacy. To the extent that American law has dealt with privacy at all, the protections have largely been restricted to government intrusions into privacy. Setting aside the limited development of the four privacy torts, there has not been much of an effort to protect individual privacy against private intrusions. (Lipton 2010)

Privacy standards and statutes exist, including FERPA and HIPPA. These standards do not deal with consumer information, neither are they tied to non-payment-based personal information, which separates HIPPA and FERPA from defining digital privacy in a format needed to evaluate mobile device privacy. Levis further validated this lack of a digital privacy

standard when he stated, “Currently their no statute[s] specifically regulating access to user data. Instead this information is governed by statutes regulating electronic communication such as the Electronic Communication Privacy Act [also known as the ECPA]” (Levis 2011). The ECPA focuses almost exclusively on wiretaps for telephones as opposed to other digital communication and limits law enforcement and government entities, not third party or corporate bodies (Tuerkheimer 1993). This statement on digital privacy helps to clarify why there are so many ambiguous laws, laws that force government and corporate entities to enact policies that help to manage and govern privacy. Most laws and policies take a long time to be debated, worded and enforced, much longer than technology takes to develop, change and advance. These differences become a larger problem as the world moves more towards MobDevs and away from traditional computers as their main computing platform. This move comes as MobDev technology is being advanced and replaced far more rapidly than traditional computers. An example of this can be found in the average length of life for MobDevs and MobDev contracts (typically between 12 and 24 months) when compared to the average life or warranty of a laptop or desktop computer (as little as 1year, but typically between 2 and 5 years).

What does privacy encapsulate? One paper breaks it down to four sub-categories:

1. Privacy of person.
2. Personal behavior privacy
3. Personal communication data.
4. Personal data privacy (Bélanger and Crossler 2011).

Another definition of digital privacy states:

> Privacy is defined as a process of anonymity preservation and so it is strongly connected with control over information about the self. In online environments, people who perceive higher threats to privacy are less disposed to disclosing information about the self because they perceive themselves as less able to control information and protect themselves too (Taddei and Contena 2013).

What role does this online trust play in MobDevs and their applications? Applications cannot be easily installed without an Internet connection and many apps actively pull data from Internet sources (e.g., email, news blogs). Do users put the same trust in Internet-using applications that they do in browsing the Internet or using web-based applications and resources? To further add to the ambiguous nature of privacy, Levis adds "It is not clear if authorization is required from the actual end user (Levis 2011).

While the definition of privacy is in flux with current laws, statutes, and policies, it can be very difficult to know what is or is not in a gray area in relation to the public's expectation for digital privacy. Information and digital privacy "are [a] myriad and [of] a varied nature" (Bélanger and Crossler 2011) making it difficult for the public and developers to know what to expect and where a line can be drawn; how much privacy can and should be sacrificed?

2.2 **Contributions to Privacy Definitions**

Warren and Brandeis argued that privacy laws should conclude that "the individual shall have full protection in person and property" and that it "is a principle as old as the common law" (Warren and Brandeis 1890). The idea that privacy includes the right to control our property and our own person (including information about oneself) was further expounded on by Thomson when she stated, "For if we have fairly stringent rights over our property [for example the Fourth

Amendment and similar laws and policies] we have very much more stringent rights over our own persons" (Thomson 1975).

Similarly, Hann, Hui, and Lee described privacy as "the ability to control the acquisition and use of one's personal information" (Hann et al. 2002) which follows writings by Alan Westin (Westin 1968). Hann continued the definition by saying "That control over information is a key dimension of privacy[,] has been stressed by researchers in diverse disciplines including law, information systems, marketing, organizational and social sciences, and psychology."

Additional definitions came from Duri and Gruteser who define privacy using the following definition:

> In a general sense, privacy may be defined as the ability of individuals to decide when, what, and how information about them is disclosed to others. Privacy principles demand that systems minimize personal data collection, for example through anonymization. Before personal data can be collected, consent from the data subject needs to be obtained by notifying [them] about the nature and purpose of their data collection and offering policy choices (Duri et al. 2002).

Duri and Gruteser went on to state that "privacy principles require notifying users and obtaining consent." One of the main complaints about obtaining consent comes from the fact that many applications state their privacy policy in a Terms and Agreements style; a style which is often ignored by the users who simply click to agree.

Seriot further stated: "According to Merriam-Webster's dictionary, privacy is the quality or state of being apart from . . . observation. In the context of spyware applications, we consider privacy more narrowly as personal data confidentiality" (Seriot 2010). While spyware is not directly part of this research, privacy-invading applications are within the scope of research; it plays a very important role in the ongoing debate about what is included or excluded from a person's digital privacy.

Other concepts, factors, and ideas that contribute to privacy and a working definition include:

1. Big Brother governments watching every digital move you make. (Hong et al. 2004)
2. Parents keeping close tabs on their children. (Hong et al. 2004)
3. Overzealous telemarketers and the protection of generic personal information. (Hong et al. 2004)
4. Is privacy a moral or legal right? (Bélanger and Crossler 2011)
5. Information privacy is a subset of the overall concept of privacy. Do principles that apply to one set of rights always apply to the other set of rights, or are they partially exclusive? (Bélanger and Crossler 2011)
6. Four dimensions of privacy, including collection, unauthorized secondary use, improper access, and errors. (Bélanger and Crossler 2011)
7. The privacy paradox, which states that a person's intentions to disclose their information is not the same as a person's observed behavior when actually sharing their personal information. (Bélanger and Crossler 2011)
8. Personal location privacy and how an individual controls that information. (Khosla 2004b)
9. Identity privacy. (Liang et al. 2012)
10. The advent and advancement of technology have created problems and challenges with consistent application of the reasonable expectation of the privacy standard and threatens digital privacy. (Crowther 2012)

11. How much privacy can the Fourth Amendment guarantee to Internet and other digital communication media? (Crowther 2012) This research primarily uses definitions, laws, and policies based in the United States, but can generally be applied internationally as digital boundaries between countries are less defined than geo-political boundaries. Examples of this include international technology companies such as Adobe, Microsoft, and Apple that run various parts of their company in different countries, requiring them to comply with multiple privacy laws and statutes depending on how data is handled and transmitted between data centers across country lines. A company having its headquarters in one country can further complicate this and data centers in multiple other countries, potentially leading to the question of which country's (or countries') privacy laws and statues should be applied to data being stored by that country.

The above factors were used in creating a working definition of privacy, which is found in section 1.1 of this thesis and used throughout this document.

2.3 Potential Data Sharing and Privacy Intrusion

All peripheral parts of a MobDev, including the camera, GPS, gyroscope, accelerometers, and proximity sensors (NFC, Bluetooth, wireless cards, etc.) can be used to learn about a person, their habits, and their activities, amongst other information (Christin et al. 2011). Among these data-gathering mechanisms, location information and specific personal information (e.g. usernames, password, social security number, phone number, email address) can be the most highly invading information collected, especially considering that some of this information can

be readily found and obtained via social media like Facebook, LinkedIn, Google+, and other such web applications. For personal location information, the "privacy of mobile users is not completely under their own control since the system administration [from mobile providers] maintains a central server where the location information of mobile users is stored (Khosla 2004a).

To further illustrate the potential data loss to mobile applications, Christian Levis described the permissions that mobile applications need as follows:

> Each app a user chooses to install on his smartphone can access different information stored on that device. This access, however, is never unlimited. The level of access granted to each application is determined by a set of controls called 'permissions.' Applications do not have access to any user information by default, and can only access whatever the 'permissions' allow them to. These restraints can be defined either at the installation of the application by a traditional 'clickwrap' license, or later on throughout the use of the application by user prompts (Levis 2011).

The clickwrap method is used by the Android platform for application permission and privileges while the prompt method is used by the iOS platform. Both of these methods include the concept that an application has only the permission that it is granted by the MobDev owner, from completely disallowing the application, to potentially granting only some features of the application permission to function. Thus, a user literally chooses to sacrifice their privacy for security and usability, depending on the function of the mobile application.

MobDevs lead to more sharing and storing of private personal information than other computing devices have historically. One author stated that:

> Mobile phones are so tightly coupled with our personal sphere, sharing information through them raise[s] privacy concerns, including the fact that people might be leaving private information traces they are not even aware of. This increased public awareness of privacy and several research studies present convincing data that such concerns have an impact on people's acceptability and adoption of these new technologies (Tschersich et al. 2011).

The best summary of the current definition of the changing definition of digital privacy can be found in Skehin and Chung's statement: "In today's evolving mobile privacy landscape, new technologies and products are constantly sparking new privacy questions even as they reshape consumers' expectations and desires" (Skehin and Chung 2011).

2.4 **Mobile Applications Permissions**

For most mobile applications to correctly function, they need permission to access resources on the MobDev, from access to the memory/storage to save information, to access to the Internet (3G/4G/Wi-Fi) to access information, to GPS location. For each platform, denying these permissions can "negatively impact the user experience, the system, or other applications installed on the device"(Barrera et al. 2010; Levis 2011). Many of these permissions may be essential for the application to correctly function, but are the permissions requested by the application actually being used by the application as part of the service the application provides, or are those permissions being used to access and collect private personal information without unnecessarily? Excessive permissions might be requested by an application without a user knowing.

Application permissions have already been discussed in depth by a variety of different papers and articles. One paper points out that "[one] problem with the permissions system [is] the difficulty of interpreting the meaning of the plethora of permissions requested, as well as the lack of a way to convey that certain combinations of permissions are far more dangerous than the individual permissions in isolation" (Au et al. 2011). This article further categorizes permissions into three types, or groups, with those groups being defined as follows:

Control: This indicates how much control the permission system gives the user over applications. An example of control is whether permissions can be individually enabled and disabled.

Information: We also categorize permission systems by how much information they convey to the user. Permission systems can convey two types of information — what resources (and thus permissions) the application developer believes their application will access (a priori) and what resources the application actually accesses at run time.

Interactivity: Finally we indicate how much of a burden the permission system is on the user by indicating how much interaction is required to use the system. Some permission systems require a lot of interaction because they prompt the user frequently, while others take measures to reduce the amount of interaction (Au et al. 2011).

Taking permissions a step further, if an application requests more access and privileges than a user is comfortable permitting the application, the user may go so far as to define that application as malicious software, due to the information access it has, or its use of requested information (Peng et al. 2012).

2.5 Android Privacy Research

Research into Android privacy and permissions has been done extensively (Shin et al. 2009; Jeon et al. 2012; Jeon et al. 2011; Portokalidis et al. 2010; Felt et al. 2012; Sarma et al. 2012; Enck et al. 2010), specifically researching into permission creep, excessive permissions, and permission consistency on Android applications purchased on the Android market.

In addition to this research, a variety of tools have been purposed and initial development has started that would allow for fine-grained permission control (Jeon et al. 2012), separation of library permissions and application permissions (Pearce et al. 2012; Shekhar, Dietz, and Wallach 2012), provide mock information to an application requesting personal information (Beresford et al. 2011), and the checking of permissions included in an Android application (Vidas, Christin, and Cranor 2011).

Also, rooting an Android device exposes additional potential attack vectors that can be used to access private information and compromise the MobDev user's privacy.

2.6 **iOS Privacy Research**

While iOS is often considered a secure mobile platform there is an extensive history of privacy-attacking exploits, including libtiff exploits, SMS fuzzing, Aurora Feint, MogoRoad, Storm8 complaint, Pinch Media, Ikee, Dutch 5 ransom, Privacy.A, and Ikee.B (Seriot 2010). There are many other reports of remote exploit being created and executed on an iPhone (Portokalidis et al. 2010). Additionally, there have been extensive research and reports on a unique identifier used by iPhones called UDID. These UDIDs were gathered by a variety of iPhone applications and websites (Smith 2010). While these are not particular examples of privacy invasion via iPhone applications, they are examples of how exploits and vulnerabilities in the iPhone architecture and design could be exploited by permissions in an application or introduce a new weakness in iPhone software. This can be found in the recent iCloud attack gathering private pictures from multiple celebrities.

Similar to Android applications, iPhone applications often suffer from over-requested permissions, which in turn provide access to a wealth of private personal information. This could

cause concern for potential privacy invasion and the exfiltration of personal information (Beresford et al. 2011). Additionally, by jailbreaking an iPhone, additional exploits and vulnerabilities could be introduced (Seriot 2010; Vidas, Christin, and Cranor 2011).

2.7 Windows Mobile Privacy Research

Due to the similarities between Windows Phone and the full version of Windows Desktop there is essentially no available research on privacy specifically for the Windows Phone mobile operating system. As far as is known, this thesis presents the first research that addresses privacy issues on Windows Phone.

2.8 Cross-Platform Comparison of Privacy, Security and Applications

Many articles have been written about security and privacy for both Android and iOS devices, since both platforms have been active on the mobile scene since 2007 ("Apple Unveils iPhone | Macworld" 2014; "Industry Leaders Announce Open Platform for Mobile Devices | Open Handset Alliance" 2014). Literature detailing privacy and security concerns for Windows mobile devices was not found that specifically referenced windows phone privacy, due to the relative newness (2010) of its current mobile platform iteration. Because of the recent release of Windows mobile devices and the lack of academic articles, these devices are not being directly covered or referenced in the remainder of this chapter.

The differences between privacy management on Android, iOS, and Windows Phone are provided here. Android and Windows Phone provide a complete list of required permissions an application requests to users before installation, while iOS only requests access permissions when an application requests the permissions to execute a specific action. Additionally,

"Android's privilege notification has some security advantages, but it pushes the most important security checking work to its end users who might not have expertise in security and may not even read or understand those privileges listed during application installation" (Han et al. 2013). iOS privacy security is thought to be the most secure and most effective privacy-protecting platform because of the controlled and limited environment, both on the device and through the iTunes App store (Han et al. 2013).

To further establish similarities and differences between Android and iOS, in May 2012 there were more than 312,000 apps on Google Play, over 478,000 applications on the iTunes store, and over 20,000 applications were shared between platforms. This overlap means that approximately "12.2% (about one in eight) of applications on Android have a counterpart application on iOS" (Han et al. 2013). One major difference between Android apps and iOS apps is that each Android app comes with a file titled Android Manifest.xml ("App Manifest | Android Developers" 2014) which details all of the permissions requested by that app. This list is displayed to a user before the application can be downloaded from the Google Play store onto an Android device. On the other hand, iOS devices have no "official documentation specifying what privileges are allowed for third-party applications" (Han et al. 2013).

Another comparison of Android and iOS discovered that there were 20 security sensitive API (SS-API) types that covered access rights to the most common resources/services on a MobDev, including the calendar, contacts, Bluetooth, Wi-Fi state, camera, and vibrator (Han et al. 2013). One of the interesting facts discovered by Han and his associates is that many of those SS-API permission requests were not coming from the application itself but from third-party libraries such as GoogleAds, MillennialMedia and Mobclix, which are inserted into the application for revenue purposes (Han et al. 2013).

2.9 **Current Industry Standards for Mobile Privacy**

At the writing of this thesis (May 2014 to October 2014), there are no published industry standards for privacy on mobile devices. Such organizations, groups, and standards as RFC, ISO and NIST have not been created nor published. It is important to note that at this time, NIST is working on a draft of Technical Considerations for Vetting 3rd Party Applications (Voas et al.), but this document is still under review and open for comment and critic. Furthermore, the NIST document only briefly mentions privacy standards without providing much information for categorizing and critiquing third-party applications. The main mention about privacy in relation to mobile applications is found in the paragraph:

> Privacy considerations, such as revealing traditional [Personally Identifiable Information] also include mobile-specific personal information like location data, pictures taken by onboard cameras, both still and video, as well as the broadcast ID of the device. This needs to be dealt with in the User Interface (UI) as well as in the portions of the apps that manipulate this data. For example, a tester can verify that the app complies with privacy standards by masking characters of any sensitive data within the page display, but they should also review audit logs, when possible, for appropriate handling of this type of information. Examples of traditional types of sensitive data include financial data (e.g., credit card number), personal data (e.g., social security number), or login credentials (e.g., password). The login page should limit the number of failed authentication attempts and not provide the ability to save a password for automatic login if the app contains sensitive data. Another important privacy consideration is that sensitive data should not be disclosed without prior notification to the user by a prompt or a license agreement (Voas et al.).

In addition to this loose definition of mobile digital privacy, the draft by NIST includes brief statements about insufficient data protection, malicious functionality built into a mobile application, and excessive permissions, which often stem from code copying or lack of knowledge by developers as to what personal information a permission might be able to access on a MobDev.

While this may provide the beginning of a definition for digital privacy, particularly in relation to mobile devices, it is far from a complete and comprehensive statement as to what personally identifiable information could be gathered using a MobDev.

3 METHODOLOGY

This chapter outlines the plans for study and research for this thesis. Also included in this chapter is the methodology used for answering the questions and proving the hypotheses as defined in section 1.6 Research Questions and Hypotheses as follows:

- **Question 1 (Q1):** What are the risks to information privacy on MobDevs (specifically in relation to mobile applications) and how are these currently represented by application permissions?
- **Hypothesis 1 (H1):** A framework for mobile application permissions analysis across multiple platforms can robustly reveal privacy risks for mobile devices.
- **Hypothesis 2 (H2):** The framework demonstrates through an analysis of current applications across multiple platforms that it is effective in identifying privacy concerns and risks.
- **Question 2 (Q2)**: Are the permissions requested by security applications (e.g. mobile antivirus programs) greater than those requested by other applications and does this pose a greater risk to information confidentiality?

3.1 Privacy Risks for Mobile Platforms (Q1)

The purpose of this research is to provide insight into the privacy-invading potential for mobile applications. As part of defining that insight, a working definition of digital privacy, with

respect to MobDevs, has been developed and used throughout this research. Research into historical privacy laws and statutes (before and after the introduction of MobDevs) was done to define what precedents set by judicial statement and review, specifically in relation to privacy and digital privacy. Literature review included judicial statements from court cases, law reviews, academic articles, and other similar publications that referenced digital privacy.

As part of the working definition of mobile application privacy risks, a list of recorded methods of privacy invasion as well as potential methods of privacy invasion for mobile devices was compiled. Privacy invasion between multiple applications is addressed and discussed later, but additional research on this topic and research on the potential for cross-application privacy invasion is creating a PIP are not within scope for this thesis. An example of potential information sharing could be found with the Facebook app and the Facebook Messenger app. The combined permissions request by these two applications and the information gathered by these applications have access to could provide detailed information about an individual.

3.1.1 Identify Potential Privacy-Invading Permissions

A method was established that compiled a list of available permissions and privileges for each mobile platform. No special considerations were taken into account for permissions and privileges that are only available on any one of the three platforms in the design of the framework. The framework should be flexible enough to analyze any mobile application or browser extension, regardless of the platform or architecture. Mapping privileges between the various platforms were incorporated into the framework, adding to its versatility and ability to create a PIP for every application on each platform. Additional attention and consideration were

given to combinations of permissions and how those combinations of permissions might allow for additional privacy invasion.

3.2 **Framework Reveals Privacy Risks (H1)**

A framework was created for risk classification and scoring. A framework that uses a point-based system was created to evaluate the permissions requested by mobile applications. Based on the points an app receives, it is awarded a risk score and risk classification. A Privacy Invasion Profile (PIP) is developed that takes into account the following factors for each application analyzed:

1. Requested permissions.
2. What information and data each permission has access to create, read, update, and delete.
3. Combinations of requested permissions.
4. A "need to know" factor of the permission (e.g., why does the application need access to the information?).

In addition to the above factors, an additional factor that was addressed (but not included as part of the framework at this time) is how a mobile application publisher handles information, specifically how it handles data in the following three phases:

1. Stored Data
2. Data Processing
3. Data in Transmission

Protection of information gathered by a mobile application was addressed, but it was not a focus, nor was it considered within the framework as part of an application's PIP.

The framework is flexible enough to accommodate permissions across multiple platforms (Android, iOS, and Windows Phone) and takes into consideration how in-app purchases affect an application's permissions. Additionally, the framework is flexible enough to be extended to web applications or browser extensions. While the framework should be flexible enough to accommodate web apps and browser extensions, a demonstration of this functionality is not within the scope of the framework for this research.

Lastly, the framework also takes into consideration combinations of certain permissions. This is done to accurately reflect the permissions requested by a mobile application and how a combination of permissions could affect the PIP, depending on the particular permissions requested.

3.3 **Cross-Platform Analysis of Applications (H2)**

As part of the demonstration process, the framework was used to evaluate several mobile applications from each of the pre-defined mobile platforms. The following sub-sections define the criteria used to select all applications, including criteria such as platform specific applications, cross-platform applications, and security applications.

For this research all permissions were enabled for each application analyzed. No permissions were modified or disabled to ensure that an accurate representation of permissions for each was application was collected. Due to having all permissions enabled, the PIP that was produced for each application is a reflection of the highest possible risk potential for privacy invasion.

3.3.1 Cross-Platform Application Selection Criteria

Applications were selected using the following criteria, being applied in this order:

1. Thirty (30) applications in total were selected.
2. The top 10 applications for each platform (Android, iOS, and Windows Phone) were selected. Top 10 applications are defined as the top 10 applications as ranked by each platform's respective application store (Google Play, iTunes and Windows Phone store). The app stores define top, or popular, applications by overall downloads or downloads over a period of time, as well as composite user ratings of an application as presented by each respective app store. There is currently no way to validate these lists of top applications as defined by each application store.
3. For each platform, 5 of these top 10 applications must be available on at least two of the three platforms. If an application does not have a cross-platform counterpart in the top 10 of a second platform, then the next most popular application that is available on two devices is selected. For example, if Android does not share any of its top 10 applications with a comparable application on Windows Phone or iOS, then the 11^{th} application is selected from each platform and compared to other top applications on the other platforms. This process continues until an application is selected that is available on at least two of the three platforms. This is part of the demonstration process for the framework as it provides a similar application to compare application permissions between each platform.
4. At least 2 of the top 10 applications for each platform are security related applications (antivirus and firewall, etc.). A similar process as described in #3 above is used,

proceeding down the list of top applications until an application is selected that is considered a security application.

In summary, 30 applications were evaluated, 5 applications on each platform need to be cross-tested on at least one other platform and 2 applications on each platform must be a security related application. Updates and packages that are pre-installed as applications on a MobDev (e.g., Google Play Services on Android devices) were not be considered as one of the top 10 applications installed because they come pre-installed (meaning there is no user choice to download this application) or they are required to run another application. However, if that same application is available on a different platform (e.g. Gmail on iOS devices) that application is eligible for selection as one of the applications used for testing and verification of the privacy framework.

Additionally, if a list of "Top 10" applications cannot be found using the criteria above, other websites were used to supplement the application selection process based on the following factors:

1. The number of times an application has been downloaded.
2. The number of ratings given for an application.

3.3.2 Android Application Selection Criteria

All Android applications were selected from Google Play ("Android Store (Google Play Store)" 2014). Other third-party application stores such as Amazon App store("Amazon.com: Apps for Android" 2014), Get Jar ("Getjar" 2014), and other similar third-party application stores("Best Android App Store Alternatives (if You're Tired of Google Play) | Digital Trends" 2014) were not considered for this research.

3.3.3 iOS Application Selection Criteria

All iOS applications were selected from the iTunes website and application ("App Store Downloads on iTunes" 2014). Third-party apps from stores such as "Cydia" ("Cydia" 2014) were not considered for this research.

3.3.4 Windows Phone Application Selection Criteria

Windows Phone applications were selected from the Windows store built into Windows phones. These same applications can be found online ("Apps for Windows - Microsoft Windows" 2014). No considerations were made for jailbreaking, installing third-party applications, or otherwise modifying the Windows Phone or tablet or installing applications from any third-party stores on this platform.

3.4 Requested Permissions and Information Confidentiality (Q2)

The classifications and risk profiles that are developed in chapter 4 and chapter 5 provide information for continued analysis of security and non-security applications, single platform applications, and cross-platform applications. PIPs are created by the framework in such a way that the PIPs cover and detail all permissions that have the potential to invade privacy and create a profile that is easy to understand not just for the security professional or the technology enthusiast, but also for the technology layman. Structuring the PIP in this way helps all MobDev users to better understand what personal information is being gathered and stored, or what personal information *could* be gathered and stored, based on the permissions requested by the MobDev applications.

3.4.1 Operating System Baseline

By design, each mobile platform provides different permissions to a mobile application without the application requesting any permission. These unrequested permissions grant minimum access to MobDev resources for an application to utilize. Unrequested, or baseline, permissions were analyzed by the framework to create an operating system factor which was included as part of the PIP for each application. This operating system factor was included as a separate element from the other permissions and permission combinations requested by an application.

3.4.2 Security Application Selection

Security applications were selected following the process and methodology defined in section 3.3 and its underlying sub-sections. In addition to meeting the conditions defined in section 3.3, security applications could include the following types of apps:

1. Antivirus applications
2. Firewall applications
3. Anti-malware applications
4. Find and recover applications. These applications are used in the situation where a MobDev has been lost or stolen and the owner of the device can remotely lock and wipe data from the mobile device as well as turn on the GPS and locate the device.
5. Other similar applications that provide some type of security, protection, or monitoring service.

Due to the differences between platform operating systems, finding security applications across platforms may not be possible. While difficult, it was still attempted to provide a useful

comparison of security applications across multiple platforms. However, cross-platform security applications, created by the same company or group for each mobile platform, were not a requirement during the selection of applications, but an optional bonus if achievable.

3.4.3 Non-Security Application Selection

Non-security applications were selected following the process and methodology outlined in section 3.3 and underlying sub-sections. When possible, the applications selected for cross-platform analysis and comparison were cross-platform applications. However, having a security application be available cross-platform is not a hard requirement during application selection, but an extra, which, if not fulfilled, would not change the scope, purpose, and outcome of this research.

3.4.4 Comparison Between Security and Non-Security Applications

A comparison of PIPs generated by the framework between security applications and non-security applications was conducted to provide a more in-depth analysis of application permissions for evaluation. Security software and applications have an implied trust from users, to protect computers and MobDevs from malicious software that attempts to exploit computing power and personal information. Due to this inherent trust, most users do not question the high number of permissions and privileges often requested and required to monitor files, processes, and uses of other MobDev resources to protect the MobDev user's information. However, due to un-vetted application permissions this may not be the case. Non-security applications may request similar (or more) permissions than security applications, which could present a much higher privacy invasion risk. This would also demonstrate that mobile application permissions

are not monitored nearly as rigorously as each application store claims. It also means that personal information might be collected and exploited (sold, used, posted on the Internet, etc.) without the user being aware of the information exfiltration occurring.

To extend this comparison, if excessive permissions and potential privacy invasion were discovered in a security application, its PIP may be significantly higher than a non-security application's, placing it on the same security level with a PIP similar to a virus, malware or other malicious code that invades personal privacy. If this is the case, this analysis could demonstrate that an application is closer to malicious code that invades privacy and collects personal information.

4 FRAMEWORK DEVELOPMENT

This framework consists of the following primary components:

1. Categorizing individual application permissions according to their potential to access, gather, and exfiltrate the data stored on a MobDev.
2. Categorizing groups of application permissions according to their potential to access, gather, and exfiltrate data on a MobDev.
3. Create a privacy invasion profile (PIP) that can help users to understand the potential for their privacy to be invaded and exploited.

This chapter contains details considered during the categorizing of permissions, selecting applications as a demonstration that the framework functions as desired.

The privacy classifications are general enough to be used across all mobile platforms used in this research, while also being flexible enough that a PIP might be adaptable enough to also create a profile for browser extensions, plugins, and other similar browser applications.

4.1 Developer Considerations

As mentioned in chapter 3, there are three items that need to be addressed in relation to how a developer handles data after it is collected, including:

1. How are data and privacy protected during data storage?
2. How are data and privacy being protected while data is being processed?

3. How are data and privacy being protected while data is being transmitted between locations?

While these are important issues to address, they are nearly impossible to incorporate into an analysis framework, especially where there is little to no standard for how data is stored, processed, and transmitted for mobile applications.

4.1.1 Challenge of an Application's Need to Know

The considerations listed in section 3.2 include a "need to know" factor. Ambiguity in who defines and how they define a "need to know" makes this a challenge that is impossible to answer. Does the research define this term? If yes, there will be challenges by developers as to why they need various permissions. If the developers define "need to know", then there will be disagreement between those developers, researchers, and MobDev users. Due to these challenges, the "need to know" factor will be excluded from this version of the framework.

4.2 User Profile Considerations

Privacy is a perceived and subjective concept that cannot be defined for everyone using a single use case. For this research the main user profile in the development and analysis of the framework is that of the writer of this thesis. The background and education of this user profile include a bachelor's degree in information technology from an accredited four-year university, including experience in information security. While using a user profile does not directly address the target users (non-technical users) it provides a baseline to create the framework.

4.3 **Privacy-Invading Profile Categorization**

Category labels are given to each type of permission. The naming and abbreviation scheme includes the following elements:

1. The permission is individual (I) or a combination of permissions (C).
2. The risk level is for the permission: Extreme (E), High (H), Medium (M), Low (L), or No Risk (NR).
3. An index number that allows for uniquely identifying a specific category of permissions. Indices start at 1 and go as high as needed for all elements within that section.

An example of this would be the following: a permission category named "Individual High 2" would have the abbreviation IH2. A second example is a category named "Combination Medium 3," which has the abbreviation of CM3. These abbreviations are found in the first column of each table from Table 4-2 to Table 4-7.

An additional factor that is considered in building a PIP is a severity factor to help explain the severity of permissions. The following severity factor is applied to the specified category level, whether the category is an individual permission category or a combination of permissions category:

Table 4-1: PIP Risk Factor Classification

Category Level	**Severity Factor**
Extreme	Multiply by 4
High	Multiply by 3
Medium	Multiply by 2
Low	Multiply by 1

For example, an application has the following permission categories:

- No Operating System Factor for this application
- 1 extreme combination permission
- 2 high individual permissions
- 1 medium combination permission
- 1 medium individual permission
- 3 low individual permissions

The raw categories for the example application are 1 extreme permission, 2 high permissions, 2 medium permissions and 3 low permissions. After applying the severity factor to the PIP for the application the raw PIP points would be:

- No Operating System Factor for this application
- 4 points of extreme invasion potential
- 6 points of high invasion potential
- 4 points of medium invasion potential
- 3 points of low invasion potential.

This example application would have a raw PIP of 17, which details the individual part of the PIP for that application. Figure 4-1 provides a graphical representation of how this example application compares to platform PIP averages as well as an overall PIP average for all mobile applications analyzed by the framework in this thesis. Note: The averages used in this example graph are from actual results defined in later chapters.

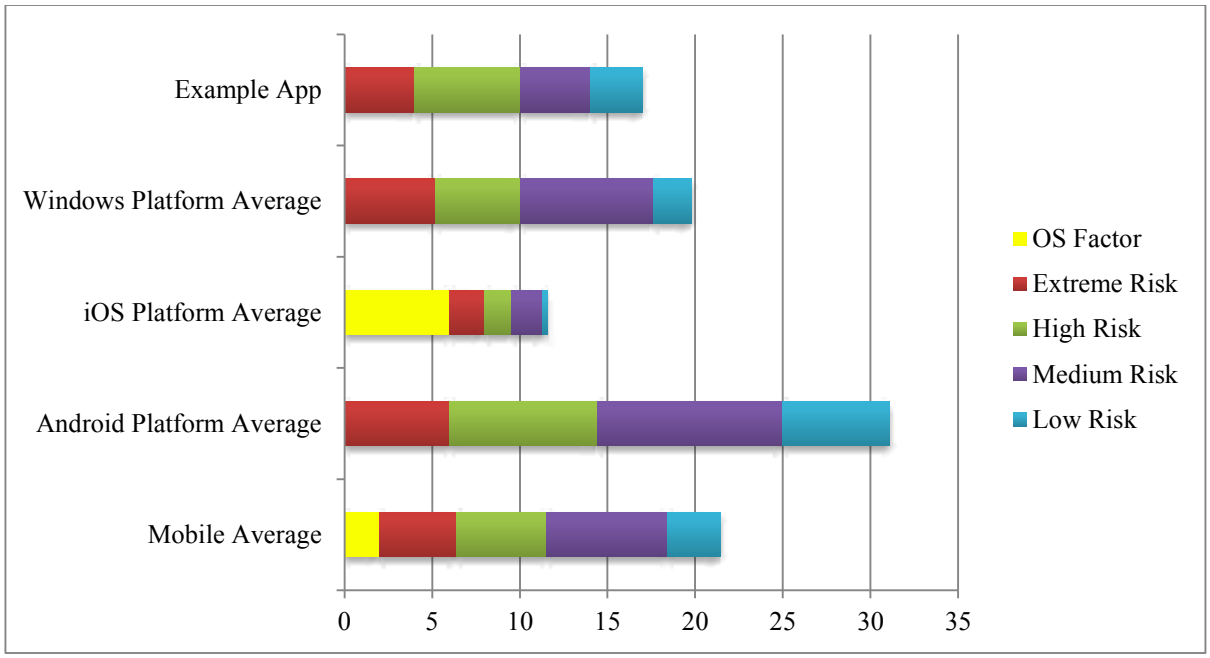

Figure 4-1: Example PIP Comparison

4.4 Individual Privacy-Invading Permissions

According to the WPD, there are several high-risk permissions that have a high probability of invading a MobDev user's individual privacy. Apps that request permissions that allow for some CRUD manipulation of personal or private data would have a higher risk than apps that request permissions that could indirectly have CRUD access to data on a MobDev. Applications that have the ability to create, read, update, or delete information can be harmful to a user, but are not necessarily invasive in the information they can access. The "read" permission is much more intrusive because it views and accesses personal information. Therefore, this permission can be highly invasive. Consequently, an application that has "read" ability on a permission that contains personal information would increase a PIP more than the other three abilities defined within CRUD access.

The focus of this permission categorization is personal information gathering and dissemination, which does not include other categories such as the potential for costing the owner of the MobDev via in-app purchases, premium rate SMS/MMS/phone calls and other charge-producing actions.

4.4.1 Individual High Risk Permissions

Based on the WPD and the literature review from Chapter 2, high-risk permissions are defined as permissions that contain several or all of the following elements:

1. Read access to personal information (e.g., phone number, email address, home address, social security number, employee ID).
2. Read access to sensitive information about owner/operator of the MobDev (e.g., SMS).
3. Read access to location information (e.g., fine-grained information via GPS/3G/4G networks, coarse-grained data via wireless networks).

Permissions that match the above criteria are as follows (see appendix E.1 for more information):

Table 4-2: Individual High Risk Permission

Permission Category	Permission	Details and Justification
IH1	Location-Gathering Permission	In the literature review, this permission (both coarse and granular settings) is considered one of the highest offending and most concerning permissions. This permission allows a MobDev to gather geographic location information via Wi-Fi, 3G/4G networks, or GPS antenna.
IH2	Personal Information Permission	Includes access to application login information, phone number, email address, and other unique personal information. Includes a unique identifier for a MobDev.
IH3	SMS/MMS Permissions	Permission that permits read, write, delete, and send access to SMS/MMS. Could lead to the access of large amounts of personal information in sent/received text messages.

4.4.2 Individual Medium Risk Permissions

Based on the WPD and the literature review in Chapter 2, medium-risk permissions are defined as permissions that contain several or all of the following attributes:

1. Read access to non-sensitive personal information (e.g., contact/address book for any application, camera (see appendix E.2 for more information)).
2. Read access to other application data.
3. Access to camera or video hardware.
4. CRUD access to the calendar on the MobDev (either the natively-installed calendar application or a third-party application that already has access to the calendar application).

While some of these attributes and characteristics may not directly affect personal privacy, they can influence perception of an individual if their information is being gathered via another person (e.g., contact information being gathered from one MobDev about a different person). General descriptions for these permissions would include the following categories:

Table 4-3: Individual Medium Risk Permissions

Permission Category	Permission	Details and Justification
IM1	Contact Information Permission	This permission is contact information about associates/friends/family of the owner of the MobDev, not information about the owner himself. This privacy invasion may vary as it is based on perception of the owner of the device and not actual data about the owner. This permission and this data could influence the perception about the owner if their contacts information is collected and sent to a third party.
IM2	Other Applications Information Access	A lot of personal information is stored and isolated in each independent application. Allowing another app to have CRUD access to that information allows the external application to aggregate personal information and to learn more about the owner/user of the MobDev. This includes social information (e.g., contacts, calendars and other information gathered from websites of social media applications). (See appendix E.3 for more information)
IM3	Camera/Web Camera Permissions	Ability to access, view, and modify pictures stored on the MobDev. Could possibly include the ability to access and modify cloud-stored pictures depending on the MobDev and cloud service (Google Drive, Dropbox, OneDrive, Box etc.) Also includes web camera access and both forward facing and rear facing cameras for capturing pictures and videos.
IM4	Calendar Permission	CRUD (or less) access to personal/cooperate calendar information. Main privacy invading feature is read ability of meetings, appointments and other commitments, allowing for the mapping of a person‘s schedule, potentially with locations.

4.4.3 Individual Low Risk Permissions

Based on the WPD and the literature review in Chapter 2, low-risk permissions are defined as permissions that do not have access to personal, private, or sensitive information, but could potentially gather that information about a user/owner of a MobDev. A general description of this type of permission would include the following:

1. Full, limited, restricted, and specific access to networks, LAN networks, Peer-to-Peer networks, pair networks, and other similar connections (e.g., Wi-Fi, 3G, 4G, Bluetooth, NFC, RFID).
2. Read access to memory/file system not including application specific permissions (e.g., file manager, disk manager).

3. Access to read/update the phone status, including intercepting phone calls, interrupting calls, and other similar actions.
4. Permission to activate the microphone on the MobDev to record surrounding sounds.

Table 4-4: Individual Low Risk Permissions

Permission Category	Permission	Details and Justification
IL1	Full and Limited Network Connectivity	Full network connectivity introduces the unidentified variable of which site or server the MobDev is connected to and what information is being passed to those machines. It is easier to reduce the possibility and increase the knowledge of privacy invasion if an application's network connection is limited to a single domain, or a couple of domains, instead of full Internet access. While this permission may appear to have a high potential for the dissemination of personal information, it is such a common permission that it is difficult to give this a high-risk or medium-risk score. This is an implied permission on some platforms. (See appendix E.4 for more information)
IL2	Bluetooth/NFC/ RFID Permissions (see appendix E.5 for more information)	This permission could allow for an information dispersal vector. However, due to the limited range for this protocol's connectivity and the need to pair a MobDev with a Bluetooth receiver, these permissions have been set to low instead of medium or high risk.
IL3	Phone Call/Status Permissions	It is important to note that this permission is mostly limited to cellular-enabled MobDevs (a percentage of the devices being considered in this study) and is normally only used for viewing the call history of a MobDev. This permission can be used to intercept, block, and make phone calls, but due to the limitation on scope of devices that have the ability to make phone calls this risk has been reduced to low risk.
IL4	Microphone Permission	Grants access to listen to and record noise in close proximity. Includes the ability to record sound and potentially store voice print information.
IL5	Storage/Internal Memory Permission	CRUD access to MobDev storage including viewing and manipulating device data. This permission is implied on some platforms (such as iOS).

4.4.4 Individual No Risk Permissions

These permissions mostly deal with interface, and cosmetic modifications, including modifying wallpaper, changing the user interface and modifying lights and other visual elements. While these permissions can be considered an annoyance, they do not invade personal privacy. Due to the lack of risk and impact in these permissions on this research, no-risk permissions are not considered as a factor in building an application's PIP and are therefore not enumerated in this section.

4.5 Combinations of Privacy-Invading Permissions

Individual permissions are not nearly as invasive when they do not have additional permissions to collect or distribute that information. For example, location permissions might be highly invasive with the ability to collect location information, but without a method to disseminate that information via network access (limited or full access) there is little or no chance that the application can send that information to a collection server or computer. These permission combinations play an important role in an application's PIP.

One additional factor considered is that applications produced by the same person, group, or company may be able to share information between applications. Due to this, one application may request access to the location permission and then pass that information to a second application that has full or limited network access. Segregating the permissions like this would reduce the PIP (as currently constructed) for each application while increasing a cross-application PIP (see appendix E.6 for more information). While this is an important use case to consider, it is not incorporated into the version of the framework developed in this research, but

could be considered in future expansions and research for the framework. The subsections below list risk of privacy invasion for combinations of permissions.

An important note with the current version of this framework is that network access is one part of all of the combinations considered. To reduce PIP inflation and to create a more accurate representation of a PIP analysis of an application, network access is not added as combination permission. If network access is a permission requested, then any other permission requested will also have the combination category of that permission.

4.5.1 Combinations Extreme Risk Permission

These permission combinations have a high probability of privacy invasion and are considered extremely risky. The publisher of the application must be trustworthy and have no bad intentions. However, if the publisher's servers or application is ever compromised, the attacker could gain access to all of those permissions and the information that they can access. Following the literature review in Chapter 2 and the WPD, the following permission combinations have been identified as having an extremely high possibility of privacy invasion.

Table 4-5: Combinations Extreme Risk Permission

Permission Category	Permission Combination	Description
CE1	Network/Internet Access + Location Data	Access to location data is a very invading permission. The ability to send that information to any website/server/computer in the world greatly increases that risk.
CE2	Network/Internet Access + Personal Information	Access to read/view personal information (device identifier, name, email, phone number) can allow a person to create a detailed profile about the owner/user of a MobDev. The ability to send that gathered information to any server/computer anywhere in the world greatly increases the risk of privacy invasion.

4.5.2 Combinations High Risk Permission

Similar to extreme risk, high-risk score/profile for combinations of permissions could very likely gather and disseminate personal information and data, either by the application publisher or by an attacker via the application. Table 4-6 enumerates and details these high-risk combinations. For the framework, only combinations of two permissions and their potential for privacy invasion are considered. Future work could be done to incorporate combinations of more than two permissions into the framework (see Section 6.3.2)**.**

Table 4-6: Combinations High Risk Permission

Permission Category	Permission Combination	Description
CH1	Network/Internet Access + Camera	With metadata tagging that can be embedded in photos and videos and the possible dissemination of personal pictures/videos, these two permissions combined can provide a lot of information about a MobDev user, especially if the camera is activated remotely and provides live images and/or video stream of the user.
CH2	Network/Internet Access + SMS/MMS	SMS/MMS/Email contain a variety of personal information. Add to that the risk that this information can be sent to any website/server/computer greatly increases the privacy-invasion risk.

4.5.3 Combinations Medium Risk Permission

Similar to extreme and high risk permission combinations, medium risk combinations were detailed and defined using the literature review in chapter 2. Table 4-7 enumerates and details these medium-risk combinations.

Table 4-7: Combinations Medium Risk Permission

Permission Category	Permission Combination	Description
CM1	Network/Internet Access + Microphone	Gathering audio data (voice recording) and passing that over the Internet can provide information about what the MobDev owner and those in close proximity to them are saying. That information and act can provide extensive and immediate information about those individuals.
CM2	Network/Internet Access + Contacts	This combination of permissions could allow for the gathering of contact information and its dispersal to a server or other type of system that gathers that data and then uses or sells that information. While this is not a direct invasion of personal privacy it is an invasion that can result in the loss of personal influence and clout as those in a MobDev user's contact list trust the user less due to their information being stolen and distributed.
CM3	Network/Internet Access + Storage/Internal Memory/SD Card	With access to the internal data and the Internet comes the possibility of gathering any and all data off of the MobDev and sending it over the Internet to a sever. This could include SQLite databases on a MobDev, files from the file structure, or even whole directories.
CM4	Network/Internet Access + Access to Other Application Data	Information about which applications are used, when they are used, and how often they are used can provide a detailed digital profile about a person. This risk increases when that data can be gathered and sent to any server/website/computer anywhere in the world.

4.5.4 Combinations Low Risk Permission

Similar to extreme, high, and medium risk permission combinations, low risk combinations were detailed and defined using the literature review in chapter 2. Table 4-8 enumerates and details these high-risk combinations.

Table 4-8: Combinations Low Risk Permission

Permission Category	Permission Combination	Description
CL1	Network/Internet Access + Bluetooth/NFC	Due to the fact that NFC and Bluetooth usually connect to peripherals that contain limited data and are not widely used, this is a low risk combination. However, with the increasing popularity of NFC financial transactions (mobile wallets) this could easily be categorized as high risk before too long.
CL2	Network/Internet Access + Phone	Access to the phones state and capabilities won't cause as much privacy invasion (especially since MobDevs are used less for phone calls now than the feature phone of a few years ago). It can provide some limited information about phone status, recent calls sent and received, and other similar data.
CL3	Network/Internet Access + Calendar	Gathering personal schedule data (where a user will be and when) and then passing that information over the Internet to a server can be very invasive. This however depends on how much the MobDev user uses the calendar.

4.5.5 Combinations No Risk Permission

Combinations of permissions that result in a no risk categorization do not affect the potential for privacy invasion and are not included in this framework or in the PIPs generated by this framework.

4.6 Mobile Operating System Considerations

With the differences between each mobile operating system some extra considerations are required to help the framework impartially critique each platform. Adding an operating system factor helps to account for discrepancies in permissions requested as opposed to permissions used and granted by both applications and the mobile operating system. The operating system factor takes into account permissions granted by a MobDev without an application requesting the permission(s) by passing the mobile operating system through the framework and giving it a raw PIP. This raw PIP is then added to the PIP generated by the permissions requested by the application.

It is important to note that some platforms may not give any permissions by default, resulting in an operating system raw PIP of zero, while other platforms might have several categories of permissions, which could add a sizeable operating system factor to the overall PIP for each application.

4.7 Platform Specific Permission Categorization

The following sub-sections include a brief summary of how permissions are currently handled by each platform. Additionally, each privacy-invading permission is sorted into a risk category (e.g., high individual risk, medium combination risk, etc.) to assist in developing a PIP. Tables 4-9, 4-10 and 4-11 provide the following: a list of privacy invading permissions for each platform, a short description of the permission and which previously defined categories apply to that permission. As part of the categorization processes, if an application has the same categorization applied to it several times, only one instance is applied to the application's PIP, instead of inflating a PIP by double counting a permission. If different permissions result in the same category being applied to the PIP for an application, it provides a potential second (or more) vector to access the private information. This is done to help normalize applied permissions and allow for a more consistent comparison of PIPs between MobDev platforms (i.e., Android, iOS, and Windows Phone).

A PIP for each application is created in chapter 5, as well as a comparison between the PIPs for each application.

4.7.1 Granularity of Permissions Available

Each platform provides a base set of permissions (e.g., location services, Internet access, access to internal files, etc.) but depending on the platform, the granularity of these permissions can influence a PIP, creating skewed results. For example, both Windows Phone and iOS have a single permission to access the location services permissions, while Android has five individual permissions (see Appendix A) and one group permission, which encompasses the five individual permissions (see Appendix B). These differences in in how permissions are handled, requested, and managed by a mobile operating system is one of the biggest challenges in developing this framework due to the multiplicity of ways a permission can be requested and implemented on each different platform. The framework accounts for these differences in permission granularity by not double-counting categories already being applied to an application. For example, Windows Phone allows for access to the following potentially invading resources:

- Music Library
- Video Library
- Photo Library
- Photo, music, and video library

Within the framework structure, each of these is categorized as IL5 and CM3, which could drastically increase the raw PIP for an application that grants these permissions. To help in accounting for this difference in granularity between applications, only one instance of IL5 and CM3 is added to the applications PIP, instead of four different instances.

4.7.2 Android Permissions Categorization

Android application permissions currently use a hierarchy of permissions, including individual permission (see Appendix A for a complete list of permissions) or group permissions (see Appendix B for a complete list of group permissions) that cluster several similar individual permissions together (e.g. coarse-grained location and fine-grained location can be clustered into a location permission group) and granting access to all of the permissions. Table 4-9 enumerates the permissions presented to a MobDev user when an application is installed and/or when permissions are managed. Included in Table 4-9 are the common names of potentially privacy-invading permissions as displayed to a user when an application is installed on an Android device ("Review App Permissions - Google Play Help" 2014) as well as the permissions categorization in relation to the framework developed in this thesis. A complete list of Android individual permissions can be found in Appendix A, and a complete list of Android permissions groups can be found in Appendix B.

Table 4-9: Android – Privacy-Invading Permissions and Framework Categorization

Permission Requested	PIP Individual Permission Category	Description
In-app purchases	None	An app can ask you to make purchases inside the app. However, due to the fact that this does not invade privacy this does not receive a categorization as part of a PIP.
Device & app history	IH2, CM4	An app can use one or more of the following: read sensitive log data, retrieve system internal state, read your web bookmarks and history, retrieve running apps.
Identity	IH2, CE2	An app can use account and/or profile information on the device. Identity access may include the ability to find accounts on the device, read owner's contact card (example: name and contact information), modify owner's profile, and add or remove accounts.

Table 4-9: Continued

Permission Requested	PIP Individual Permission Category	Description
Contacts/Calendar	IM1, IM4 CM2, CL3	An app can use your device's contacts and/or calendar information. Contacts and calendar access may include the ability to read your contacts, modify your contacts, read calendar events plus confidential information, add or modify calendar events and send emails to guests without the owner's knowledge.
Location	IH1, CE1	An app can use your device's location. Location access may include approximate location (network-based).
SMS	IH3, CH2	An app can use your devices text messaging (SMS) and/or multimedia messaging service (MMS). This group may include the ability to use text, pictures, or video messages. **Note:** Depending on the plan, the owner may be charged by the carrier for text or multimedia messages. SMS access may include the ability to receive text messages (SMS), read your text messages (SMS or MMS), receive text messages (MMS, like a picture or video message), edit your text messages (SMS or MMS), send text messages (SMS or MMS, which may cost the owner money), or receive text messages (WAP).
Phone	IL3, CL2	An app uses the phone and/or its call history. **Note:** Depending on the plan, the owner may be charged by his carrier for phone calls. Phone access may include the ability to directly call phone numbers (this may cost money), write call log (call history), read call log, reroute outgoing calls, modify phone state, and make calls without the owner's intervention.
Photos/Media/Files	IL5, CM3	An app can use files or data stored on your device. Photos/Media/Files access may include the ability to read the contents of your USB storage (SD card), modify or delete the contents of your USB storage, format external storage, and mount or unmount external storage.
Camera/Microphone	IM3, IL4, CH1, CM1	An app can use your device's camera and/or microphone. Camera and microphone access may include the ability to take pictures and video, record audio, and record video.
Device ID & call information	IH2, IL3, CE2, CL2	An app can access your device ID(s), the device's phone number whether you're on the phone, and the number connected by a call.
Other	IL1, IL2 IM2, CM4, CL1, All Combinations	An app can use custom settings provided by your device manufacturer or application-specific permissions. This can include Bluetooth permissions, NFC permissions, and network permissions. **Note:** If an app adds a permission that is in the "Other" group, you will always be asked to review the change before downloading an update. Other access may include the ability to: read your social stream (on some social networks), write to your social stream (on some social networks), and access subscribed feeds. When you review individual permissions, all permissions, including those not displayed in the permissions screen, will be shown in the "Other" group.

Unmodified Android (also known as vanilla Android) does not allow for user management of individual permissions after an application is installed. However, modified ROMs based on Android (e.g. Cyanogenmod) provide the user with the abilities to manage permissions and access that an application can use. Such ROMs provide the user with this management ability in a feature called "Privacy Guard" which allows for one-off modifications to a single permission requested by an application. Modifications of the native ROM on a MobDev are not within scope for this thesis. Figure 4-2 shows the screen and permission information (including a short description of what the permission permits) provided to a user when they install an application on an Android device.

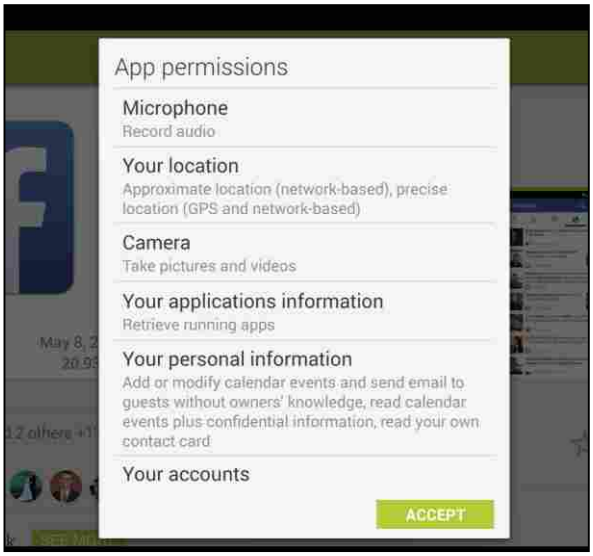

Figure 4-2: Android Permission Request (Facebook Application)

4.7.3 iOS Permissions Categorization

iOS currently uses an as-needed permission model, meaning that a permission is not granted until it specifically requests access to that resource in which case an alert appears on the device requesting that the user grant permission for that access to the application. After a permission has been granted or denied, access to that resource for that application can be manually modified within the settings of the device. One of the major downsides to this model is that iOS provides a much more limited list of permissions for developers to access: however, some recent inclusions in iOS 8 (announced June 2014 with a developers beta release, publicly available fall 2014) allows for permissions expansion (see appendix E.7 for more information). Table 4-10 enumerates the permissions as presented by iOS to the MobDev user for acceptance and management. Included in table 4-10 is the categorization for each of those permissions.

Table 4-10: iOS Privacy Permissions and Framework Categorization

Permission Requested	PIP Permission Category	Description
Location Services	IH1, CE1	Wi-Fi or GPS defined geo-location.
Contacts	IM1, CM2	Personal contacts, including name, phone number, email address, and physical address.
Calendars	IM4, CL3	Allows an application to read/modify/delete elements in the calendar on the iOS device.
Reminders	None	Allows an application to read/modify/delete elements in the reminders saved on the iOS device.
Photographs	IL5, CM3	Photos could contain geo-location information as well as be of a personal nature. This permission allows an application to access the photos and either manipulate, modify, delete, or otherwise manage their data and metadata.
Bluetooth Sharing	IL3, CL1	The ability to connect a peripheral device to the MobDev. This device could control or access a wide variety of personal information on the MobDev
Microphone	IL4, CM1	The ability to turn off and on the microphone, allowing for the MobDev to record audio clips or videos with sound.
Various Application Permissions (see appendix E.8 for more information)	IM2, CM4	The ability to access information and data stored by other applications. (e.g., using login information between applications).
Network Access (see appendix E.9 for more information)	IL1	The ability to access the Internet. Includes full, limited, and restricted access.

Figure 4-3 depicts the interface used by iOS devices to manage permissions, particularly privacy invading permissions.

iOS devices are fairly unique in permission management in that an application comes with a base set of permissions (primarily Internet access). Other permissions are granted as applications request them, which indicates that some permissions might never be requested and granted if the user never touches those features. The additional option to disable permissions and features increases user management of personal privacy.

Figure 4-3: iOS Permission Management

4.7.4 Windows Phone Permission Categorization

Windows phone is newer than either iOS or Android and is essentially a lightweight version of Windows 7 and Windows 8 (depending on the model of phone being referenced). Because it is being modeled after full-featured operating systems, Windows phone provides much more detailed permissions with fairly precise descriptions of what each permission is

allowed to access and accomplish. Table 4-11 explains privacy invading permissions as presented to the MobDev user for acceptance. The table includes the categorization of those permissions as part of the framework.

Similar to Android, Windows phone clickwraps permission requests in a single accept all when the application is installed. However, Windows phone does not currently allow for post-installation management of individual permissions; the permissions that an application requests are an all or nothing action. Figure 4-4 below depicts the permission request before the installation of an application on a Windows 8 phone.

Table 4-11: Windows Phone Permissions and Framework Categorization

Permission Requested	PIP Permission Category	Description
Appointments	IM4, CL3	CRUD access to calendar and appointments within calendar.
Contacts	IM1, CM2	Access to all contact data and metadata.
Identity Device	IH2, CE2	Access to a unique identifier for a specific MobDev
Identity User	IH2, CE2	Access to personal information about the owner of the MobDev
Camera	IM3, CH1	Access to a MobDevs camera and associated hardware.
Location	IH1, CE1	Access to GPS and Wi-Fi location information.
Media Photo Library	IL5, CM3	Access to view pictures taken by camera and stored in cloud services.
Microphone	IL4, CM1	Access to microphone, specifically to record audio.
Networking	IL1	Full, limited and restricted network/Internet access
Proximity/NFC	IL2, CL1	Access to utilize the NFC capabilities of the MobDev.
Removable Storage	IL5, CM4	Access to internal memory as well as any SD card added to device.
Sensor	None	Ability to access hardware sensors, including accelerometer.
Wallet	None	Ability to access and manage financial transactions.
Web Browser Component	IM2, CM4	Access to data and metadata in web browser.
Front Camera	IL3, CH1	Access to only the front camera on the MobDev and associated hardware.
Rear Camera	IL3, CH1	Access to only the rear camera on the MobDev and associated hardware.
Bluetooth	IL2, CL1	Access to the Bluetooth capabilities on the MobDev.

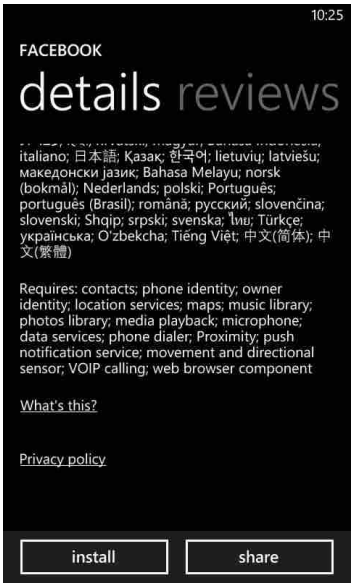

Figure 4-4: Windows Phone Permission Request (Facebook Application)

4.8 **Extensibility and Modularity of Framework**

While this thesis is limited to one user and their subjective preferences in relation to privacy, it does allow for modifications to the framework to take into account a users personal preferences to privacy risk. For example, if a different user does not consider location to be a high-risk permission as defined in section 4.4.1, they could assign that permission to a different risk category. These types of adjustments would allow to the customization of the framework to adapt for an individual or group's privacy needs.

This extensibility and modularity is particularly useful for a company that has specific privacy requirements for company issued or used mobile devices. The framework allows for the selection of risk for permission group, increasing its ability to handle the different user profiles and use cases that it may have to handle.

4.9 Application Selection

The application selection process was defined in sections 3.3 and all sub-sections. The following sub-sections detail which applications were selected for testing following that methodology.

There are some situations in which some of the application selection criteria do not fit the exact selection outlined in sections 3.3 to 3.4 and all included sub-sections. In these situations, the application selected is justified as being similar to an application that fits the selection criteria.

4.9.1 Android Application Selection

Android applications selected for testing and verification of the privacy framework are as follows (criteria from chapter) (see appendix E.10 for more information):

- Facebook – This application fulfills the cross-platform requirement. This application is one of the most downloaded applications as defined by Google Play ("Facebook - Android Apps on Google Play" 2014).
- Instagram – This application fulfills the cross-platform requirement. This application is one of the most downloaded applications by Google Play ("Instagram - Android Apps on Google Play" 2014).
- WhatsApp Messenger – This application fulfills the cross-platform requirement. This application is one of the most downloaded applications as defined by Google Play ("WhatsApp Messenger - Android Apps on Google Play" 2014).

- Netflix – This application fulfills the cross-platform requirement. This application is one of the most downloaded applications as defined by Google Play ("Netflix - Android Apps on Google Play" 2014).
- Fruit Ninja Free – This application fulfills the cross-platform requirement. This application is one of the most downloaded applications as defined by Google Play ("Fruit Ninja Free - Android Apps on Google Play" 2014).
- Subway Surfers – This application is one of the top applications as defined by Google play ("Subway Surfers - Android Apps on Google Play" 2014).
- YouTube – This application is one of the top applications as defined by Google play ("YouTube - Android Apps on Google Play" 2014).
- Gmail – This application is one of the top applications as defined by Google play ("Gmail - Android Apps on Google Play" 2014).
- CM Security and Find My Phone – This application fulfills the security application requirement. This was one of the highest-rated security applications by Google Play ("CM Security & Find My Phone - Android Apps on Google Play" 2014).
- 360 Security - Antivirus Free – This application fulfills the security application requirement. This was one of the highest-rated security applications by Google Play ("360 Security - Antivirus FREE - Android Apps on Google Play" 2014).

4.9.2 iOS Application Selection

iOS applications selected for testing and verification of the privacy framework are as follows (criteria from chapter 3 that are fulfilled by a specific application are also included, as are reference materials as to where to find each application):

- Facebook – This application fulfills the cross-platform requirement. This application was one of the highest-rated applications as listed on iTunes ("Facebook on the App Store on iTunes" 2014).
- Netflix – This application fulfills the cross-platform requirement. This application was one of the highest-rated applications as listed on iTunes ("Netflix on the App Store on iTunes" 2014).
- Pandora Radio – This application fulfills the cross-platform requirement. This application was one of the highest rated applications as listed on iTunes ("Pandora Radio on the App Store on iTunes" 2014).
- Skype for iPad (see appendix E.11 for more information) – This application fulfills the cross-platform requirement. This application was one of the highest-rated applications as listed on iTunes ("Skype for iPad on the App Store on iTunes" 2014).
- Fruit Ninja Free – This application fulfills the cross-platform requirement. This application was one of the highest-rated applications as listed on iTunes ("Fruit Ninja Free on the App Store on iTunes" 2014).
- The Weather Channel for iPad – This application fulfills the requirement for one of the top rated applications by iTunes ("The Weather Channel for iPad on the App Store on iTunes" 2014).
- Angry Birds HD Free (see appendix E.12 for more information) – This application fulfills the requirement for one of the top rated applications by iTunes ("Angry Birds HD Free on the App Store on iTunes" 2014).

- Words With Friends HD Free – This application fulfills the requirement for one of the top rated applications by iTunes ("Words With Friends HD Free on the App Store on iTunes" 2014).
- Find My iPad – This application fulfills the security application requirement. This was one of the highest rated security applications ranked by iTunes. Third party applications stores and applications were not evaluated at this time (see appendix E.13 for more information) ("Find My iPhone on the App Store on iTunes" 2014).
- Lookout – Backup, Security, Find Your iPhone, iPad or iPod Touch – This application fulfills the security application requirement (see appendix E.14 for more information). ("Lookout – Backup, Security, Find Your iPhone, iPad or iPod Touch on the App Store on iTunes" 2014).

4.9.3 Windows Phone Application Selection

Windows Phone applications selected for testing and verification of the privacy framework are as follows (criteria from chapter 3 that are fulfilled by a specific application are also included, as are the reference materials as to where to find each application):

- Facebook – This application fulfills the cross-platform application criteria as well as one of the top rated applications as defined by the Windows Phone application store ("Facebook | Windows Phone Apps+Games Store (United States)" 2014).
- Skype – This application fulfills the cross-platform application criteria as well as one of the top rated applications as defined by the Windows Phone application store ("Skype | Windows Phone Apps+Games Store (United States)" 2014).

- WhatsApp Messenger – This application fulfills the cross-platform application criteria as well as one of the top rated applications as defined by the Windows Phone application store ("WhatsApp | Windows Phone Apps+Games Store (United States)" 2014).
- Pandora – This application fulfills the cross-platform application criteria as well as one of the top rated applications as defined by the Windows Phone application store ("Pandora | Windows Phone Apps+Games Store (United States)" 2014).
- Netflix – This application fulfills the cross-platform application criteria as well as one of the top rated applications as defined by the Windows Phone application store ("Netflix | Windows Phone Apps+Games Store (United States)" 2014).
- Angry Birds Epic – This application is one of the top rated applications as rated by the Windows Phone store ("Epic | Windows Phone Apps+Games Store (United States)" 2014).
- Piano Tiles – This application is one of the top rated applications as rated by the Windows Phone store ("Piano Tiles - Don't Tap The White Tile | Windows Phone Apps+Games Store (United States)" 2014).
- Extreme Survival Run – This application fulfills one of the top rated applications as rated by the Windows Phone store ("Extreme Survival Run | Windows Phone Apps+Games Store (United States)" 2014).
- AVG Family Safety 8 – This application is one of the top rated security applications as rated by the Windows Phone store ("AVG Family Safety 8 | Windows Phone Apps+Games Store (United States)" 2014).

- Lock and Hide – This application is one of the top rated security applications as rated by the Windows Phone store ("Lock & Hide | Windows Phone Apps+Games Store (United States)" 2014).

5 FRAMEWORK ANALYSIS AND RESPONSES

This sections analyzes the results of the mobile privacy intrusion framework prototype and answers the purposed questions and hypotheses:

- **Question 1 (Q1):** What are the risks to information privacy on MobDevs and how are these currently represented by application permissions?
- **Hypothesis 1 (H1):** A framework for mobile application permissions analysis across platforms can robustly reveal privacy risks for mobile devices and mobile applications.
- **Hypothesis 2 (H2):** The framework demonstrates through an analysis of current applications across multiple platforms that it is effective in identifying privacy concerns and risks.
- **Question 2 (Q2):** Are the permissions requested by security applications (e.g. mobile antivirus) greater than those requested by other applications and does this pose a greater risk to information confidentiality?

5.1 Privacy Risks for MobDevs (Q1)

From the review of literature found in chapter 2 and the use of the framework in chapter 4 the following privacy risks for each mobile platform were found:

1. Lack of understanding about permissions requested by applications by a MobDev user.
2. Low value given to personal privacy.

3. Lack of knowledge and understanding on how to modify permissions after installing or permitting an application permission to utilize a resource.
4. Lack of care to monitor applications and their potential to access and disseminate personal information and data.
5. Combinations of permissions (especially high risk privacy invading permissions) can lead to information-disseminating applications.
6. Grouping similar and non-similar permissions into permission groups.
7. Free applications often request higher privacy-invading permissions and combinations of permissions than paid applications. This is because free applications rely on ads and ad libraries for revenue rather than the purchase of the application. The privacy-invading permissions usually found in ad libraries include (but are not limited to) the following:
    a. Location permission – Used to tailor and adapt ads to the specific location of the user amongst other information that can be gathered from location data.
    b. Browser information and bookmarks permission – To customize ads placed in a free application based on items a user usually looks at on the Internet. A similar practice is already implemented on many modern websites which use cookies to track a person's browsing history and preferences to place relevant ads on websites that they visit.
    c. Information about other applications – Applications installed on a MobDev can provide a variety of information about a person, such as the games they enjoy playing, if they have installed and used travel applications, and potentially information about financial tracking through banking applications or other financial monitoring applications.

d. Other personal information that can be used to create a digital profile about a MobDev owner. This is often done to more efficiently customize ads to the MobDev user.

8. Lack of monitoring and auditing of applications available through each platform's store. While there is some monitoring and auditing, the literature review found many instances in which an application was able to bypass the auditing tools and algorithms and present an application on the various app stores for purchase by MobDev users.
9. Inability for users to modify which permissions are active or inactive after an application is installed (Windows Phone and Android MobDevs).
10. Unknown data exfiltration by a MobDev operating system or mobile applications.
11. Requesting and using more permissions than are displayed for a user when an application is installed via the clickwrap method.

While each platform handles permissions differently, they each do allow for some level of personal management in which permissions can be accessed and can inform the user about what granting those permission means to their personal privacy.

5.2 **Analysis Framework Summary (H1)**

While each platform may handle permissions differently, each platform generally provides similar permissions to the developers for access to part of the app while also informing the MobDev user which permissions are requested by an application. This framework creates a PIP for each application selected for testing. The PIPs created by the framework can provide insight into privacy management across current major platforms and future mobile and non-mobile environments (i.e., computer browsers, and new mobile environments) as well as help to

identify abuse of privacy in mobile applications. These general permission groups found in Chapter 4 section 5 provide groups that can be applied to applications on a variety of platforms and still provide a Privacy Invasion Profile (PIP) that is easy for both the common person as well as the technical professional.

5.2.1 Operating System PIP Factor

The Windows Phone platform does not automatically grant any permission to an application. All permissions must be requested by the application and granted by the MobDev user. All permissions an application requests are displayed before a user is able to install an application.

The Android platform does not automatically grant any permission to an application. All permissions must be requested by the application and granted by the MobDev user. When an application is installed it states that there are no special permissions requested, which includes most privacy-invading permissions. However, this is not all of the permissions requested by an application. A full list can be found at the bottom of an application's page on the Google Play store or via Android device settings.

The iOS platform automatically grants the following permissions (and related categories) to all applications, without the application requesting the permission:

1. Network Access – IL1 and all combinations of permissions.
2. Camera – IM3 and CH1

Between these permissions each iOS application has a raw operating system PIP of the following: one high-risk permission, one medium-risk permission, and one low-risk permission. After passing these categories through their various factors, the final raw operating system PIP

applied to each iOS application is 6. This is applied in the graphs found later in this chapter, where further analysis is presented on individual applications and between applications on different platforms.

5.3 **Demonstration of Framework (H2)**

This section contains a graphical representation and analysis of the various applications and a comparison between applications on a single platform, similar applications across platforms, and security applications across all platforms. These figures are used to compare PIPs between applications and do not necessarily represent an application's PIP. For a complete breakdown of permission categorization for each application on each platform see Appendix D.

It is important to note that all applications were selected, downloaded, and analyzed between May 1, 2014 and August 1, 2014 (see appendix E.15 for more information). Any changes by developers (both application developers and platform developers) during or after this timeframe may not represented by the data collected during this research.

5.3.1 Platform Specific Application Comparison

Initially, a PIP did not include a weighted factor (i.e., extreme permissions multiplied by a factor of 4, etc.). Due to this lack of representation PIPs did not present an accurate comparison of permissions between applications on a single platform, or across multiple platforms. The weighting provided a normalizing feature that helped to show the impact of extreme and high risk permissions (both for individual and combined permissions) and more accurately represents the likelihood of a MobDev user's personal information being collected and distributed by mobile applications. As depicted in the following figures (Figure 5-1, Figure 5-2, Figure 5-3,

Figure 5-4, and Figure 5-5) and analysis, the consistency between applications, both on a single platform and across platforms, indicates that the framework does provide an analysis tool that provides a profile for analysis and simplified understanding.

Android Comparison

Figure 5-1 depicts the results of analyzing the Android applications with the framework defined and designed in Chapter 4.

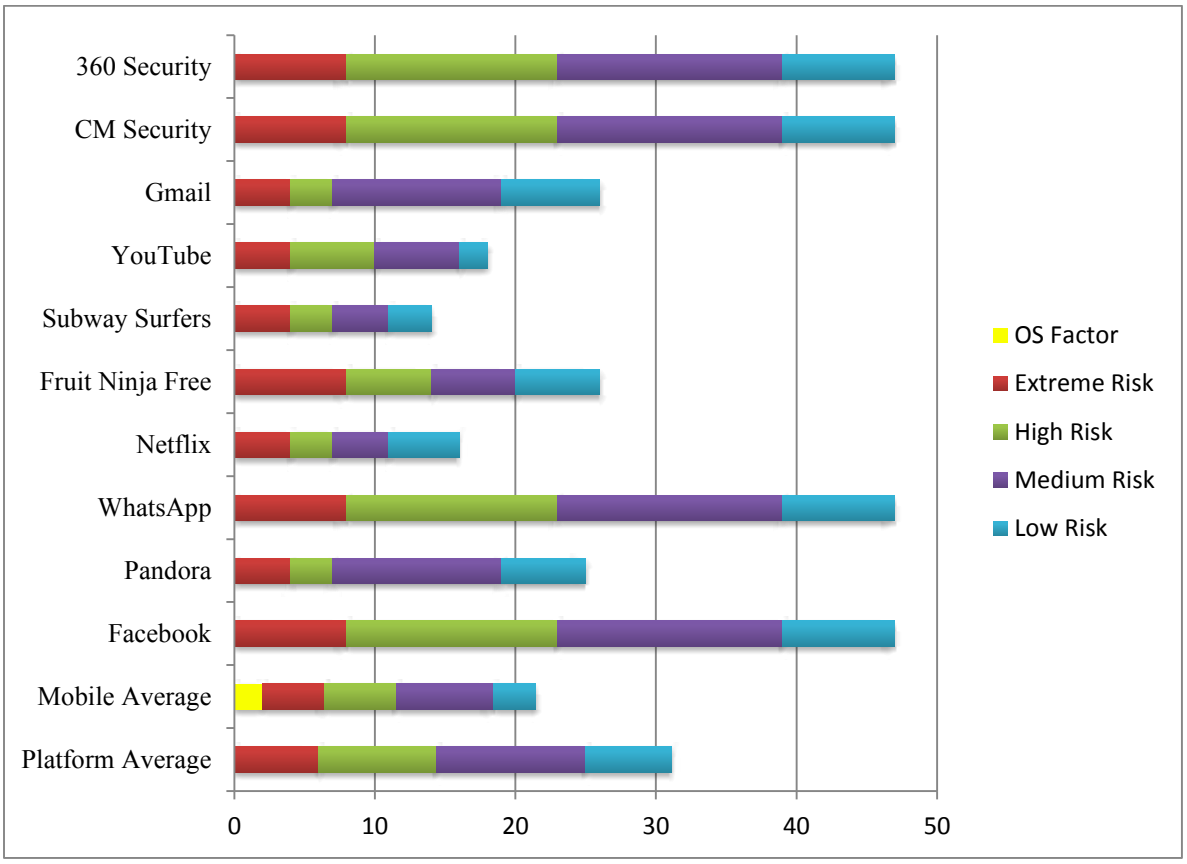

Figure 5-1: Android PIP Comparison

Most Android applications were consistent in their raw PIP when compared to non-security applications (see Figure 5-1), scoring between 14 and 26. However, there were a few applications (i.e., Facebook and WhatsApp) that requested more permissions than other non-security applications. In fact, both the Facebook and WhatsApp applications requested more privacy-invading permissions than security applications. From this data we can conclude that some applications request far more invading permissions and combinations of permissions than a user might permit. It is generally expected that security applications request more invading permissions. It is important to notice the large difference between most applications (Gmail, Fruit Ninja, and other applications with raw PIPs under 30) and both the social media applications (none less than 45) and the security applications (none less than 45). As per H1, the framework has revealed how intrusive WhatsApp, Facebook, Security 360, and CM Security can be to a MobDevs user's personal privacy.

iOS Comparison

Figure 5-2 depicts the results of analyzing the iOS applications with the framework defined and designed in Chapter 4.

Most iOS applications request a much smaller number of permissions compared to other platforms. This is purposefully done to create a controlled mobile environment that as Apple states, just works. Even with the controlled mobile environment, the permissions requested by mobile applications and the PIPs generated by each application indicate similar trends to Android and Windows Phone. Social media applications request approximately the same number of potentially invading permissions (Facebook and Skype both had a raw PIP score of 16 and 10 respectively) and security applications had similar scores (Lookout had a raw PIP of 17 and Find

my iPad had a raw PIP of 13, which was as low as several non-security applications). Part of the smaller gap between security applications and normal applications is attributed to the fact that Apple has such a closed mobile environment, allowing for little deviation from a small standard set of permissions available to developers.

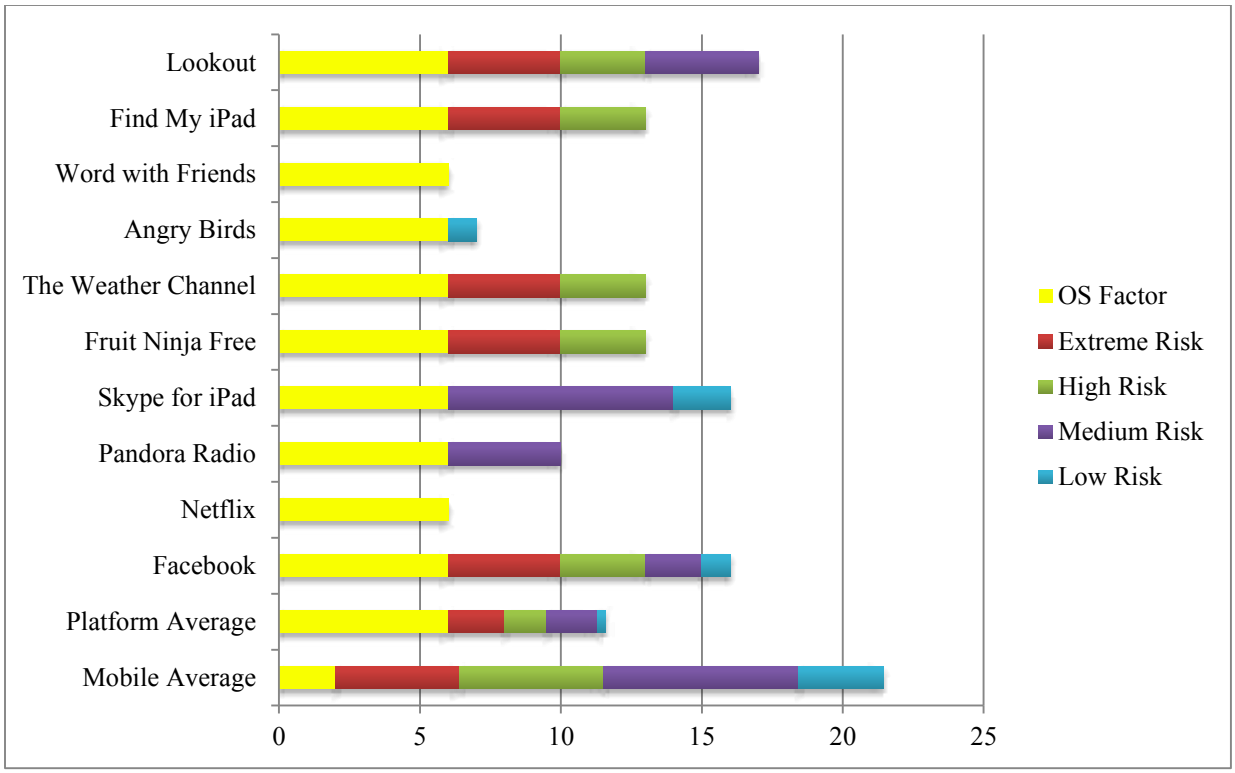

Figure 5-2: iOS PIP Comparison

Similar to Android, there is a large gap between social applications (Facebook and Skype) and Security applications (Lookout and Find My iPad) when compared to other applications. The non-social and non-security applications had raw PIPs between 6 and 10, while the security and social applications' raw PIPs were never less than 10 with all but one having a raw PIP over 13.

Windows Phone Comparison

Figure 5-3 depicts the results of analyzing the Windows Phone applications with the framework defined and designed in Chapter 4.

Windows Phone continues the same pattern, where social media applications request more potentially invading permissions than other applications, including security applications. Almost double the permissions were requested by both social media applications (Facebook and WhatsApp both had raw PIPs of 38 and 39 respectively) in comparison to the security applications that were analyzed (Lock and Hide has a raw PIP of 24 and AVG Family Safety has a raw PIP of 14).

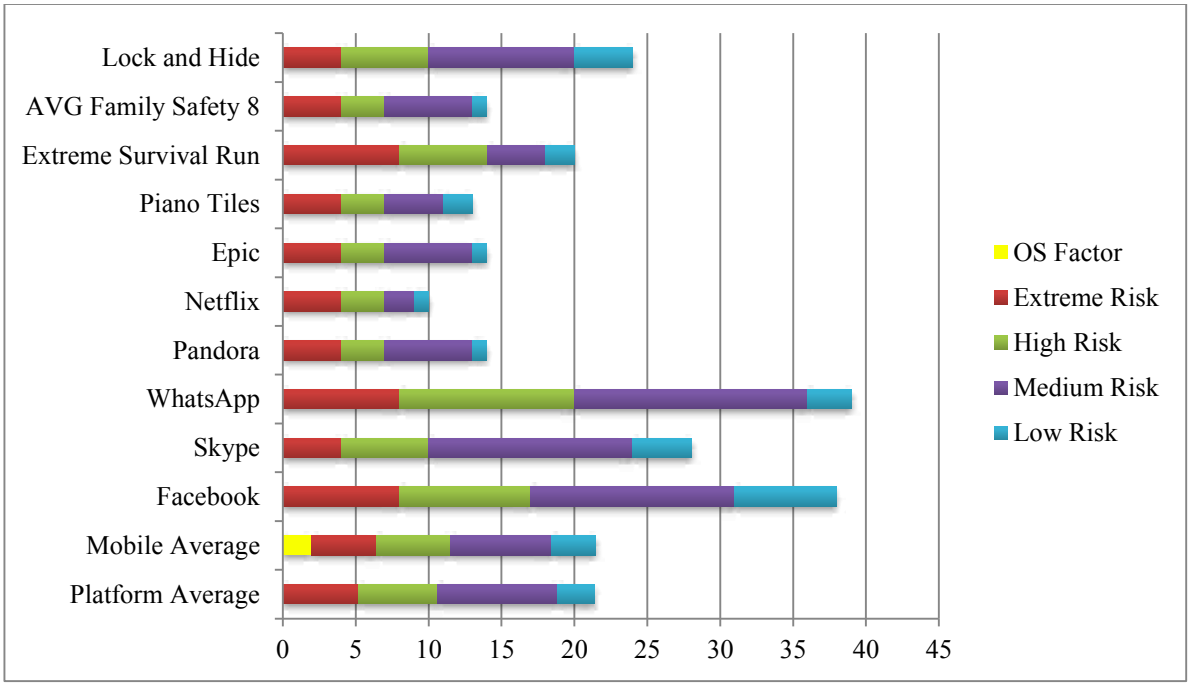

Figure 5-3: Windows PIP Comparison

While not as extreme as both the iOS applications and Android applications, Windows Phone applications follow the same pattern with the difference between social and security applications when compared to other applications. The four most intrusive applications are social applications (Facebook, WhatsApp, and Skype) and one security application (Lock and Hide) with a similar separation between this set of applications (none had a raw PIP less than 24, with two being over 35) and the other applications (none with a raw PIP higher than 20 with only one over 14).

5.3.2 Cross-Platform Comparison

Figure 5-4 depicts the results of analyzing the applications across the three main platforms (i.e., Android, iOS, and Windows Phone) with the framework defined and designed in Chapter 4.

The cross-platform applications selected for this research provided some interesting information when analyzed using the framework. For example, if an application's raw PIP was lower than the average raw PIP for its platform, then its counterpart application(s) on a different platform also had a raw PIP below the average raw PIP for its platform. Similarly, if an application's raw PIP was higher than its platform's average, then its counterpart applications on a different platform also had raw PIPs higher than their platform's average raw PIP. This comparison is shown in Figure 5-4, supporting how raw PIPs compare for applications on different platforms as well as against each platform's average and an overall mobile average. This helps to support the framework by demonstrating its consistency in creating a PIP for the same application across multiple mobile platforms.

As shown in Figure 5-4, there are no extreme cases of an application not following a similar pattern to its counterparts on different mobile platforms. The one exception to this is some platform-induced differences, particularly with iOS and its environment controls, which limits available permissions. These limitations make iOS applications less invading than applications on either the Android platform or the Windows Phone platform, but when compared to the number of available permissions the differences are far less dramatic than when initially analyzed.

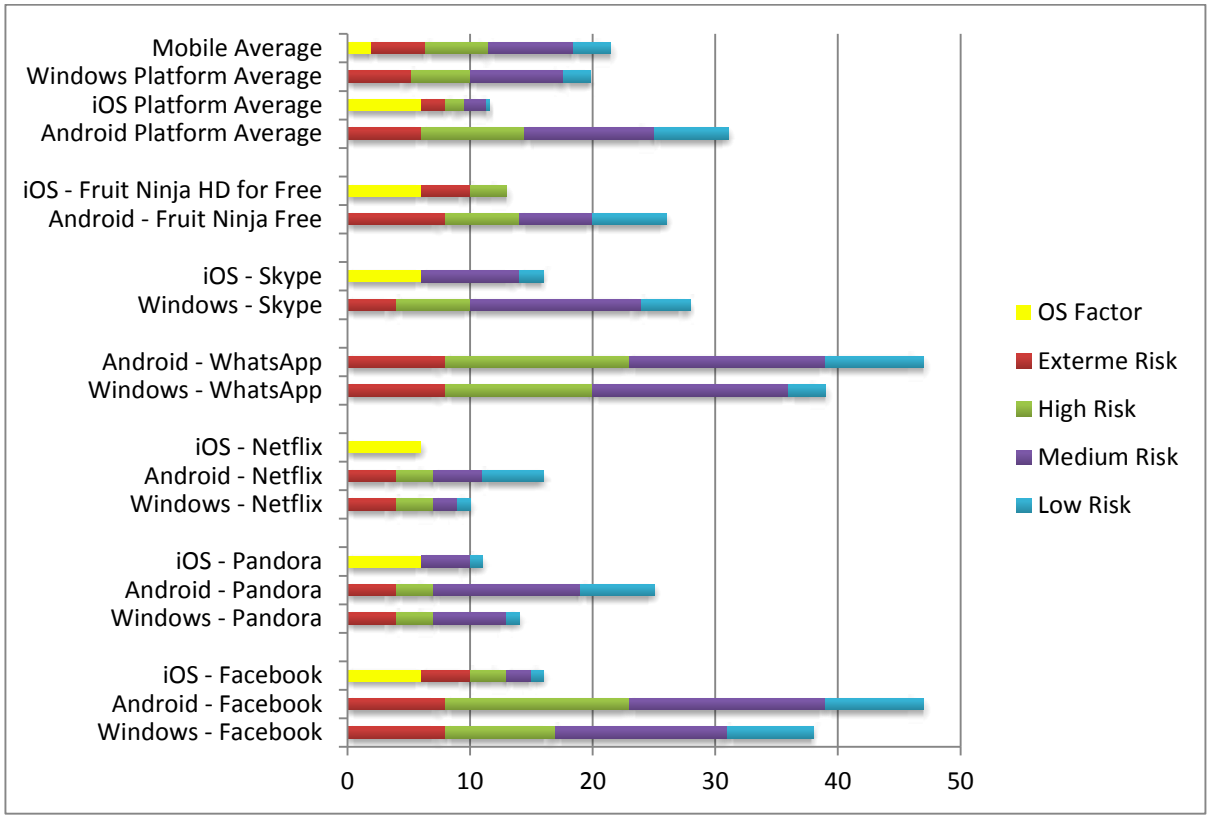

Figure 5-4: Cross-Platform Application PIP Comparison

Generally, security applications require more permission to monitor events, processes, and actions on a MobDev. However, recent changes to requested permissions for some

applications (Facebook and Facebook Messenger) have brought out how many permissions many applications request, many of which they might not need and are simply used to gather information about a user and to create a digital profile of that user ("Why You Should Delete All Facebook Mobile Apps Right Now | Techcafeteria.com" 2014). This information is consistent with the data gathered and displayed throughout this chapter and across all platforms. Each platform has a handful of applications that require few privacy invading permissions. Besides those few applications (applications which bring down each platform's average raw PIP, as well as the overall raw PIP average), a large number of applications request a wide range of privacy-invading permissions, which can be very risky for individuals using those applications.

5.4 **Cross-Platform Security Application Comparison (Q2)**

Figure 5-5 depicts the results of analyzing security applications across all three platforms (i.e., Android, iOS, and Windows Phone) with the framework defined and designed in Chapter 4.

Figure 5-5 represents a comparison of raw PIPs for security applications across platforms as well as how those PIP compare to each platform's average raw PIP and the average raw PIP for all the applications analyzed. Security applications follow similar trends as the applications and analysis performed in Section 5.3 where if an application has a higher raw PIP than the average for its platform, its counterparts on other platforms have a raw PIP that is also higher than its mobile platform's average PIP. The one exception to this with security applications is the Windows Phone application AVG Family Safety 8. AVG Family Safety 8 has a raw PIP that is lower than the average raw PIP for Windows applications. Further analysis shows that AVG Family is more of a media monitoring application for parents to monitor the music, pictures and other files on their child's MobDev. While this is still a type of security application, AVG

Family is not a traditional security application. Lock and Hide (the other Windows Phone security application) requests permissions (such as location, unique identifier, camera, and Internet access) that are more consistent with security applications on the other mobile platforms.

To help answer Q2 of this research, with the exception listed above, all other security applications access many more permissions than the average raw PIP for their platform or for the average raw PIP for all mobile applications analyzed. Security applications consistently requested a larger number of potentially privacy-invading permissions not used by other applications. The exception to this was social media applications (Facebook, Skype, WhatsApp, etc.), which consistently requested the most of the permissions, even more than the security applications.

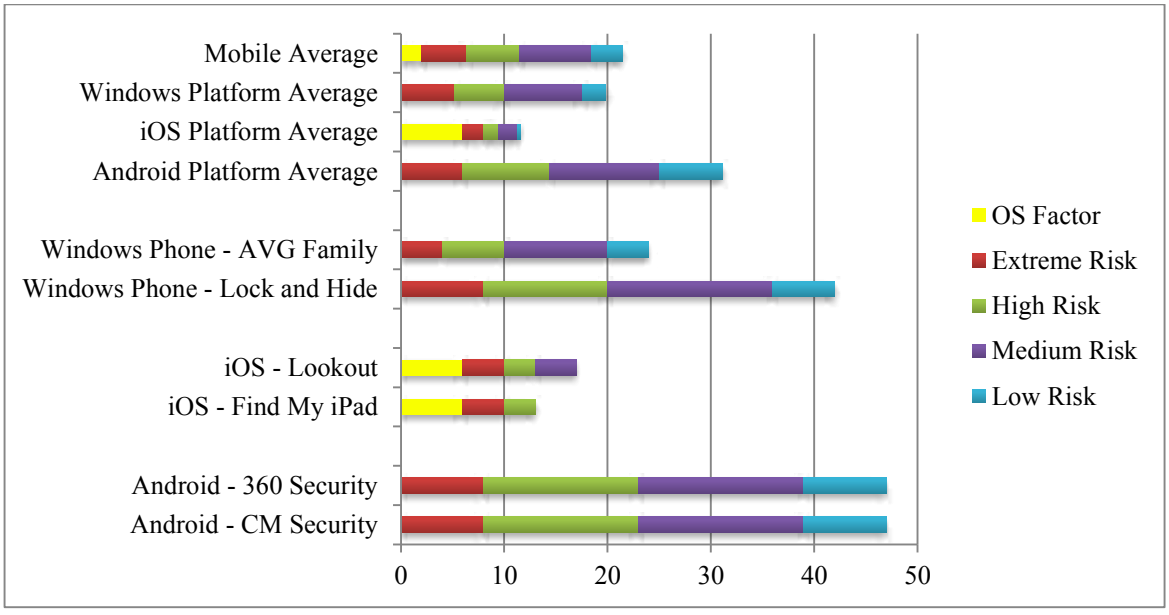

Figure 5-5: Cross-Platform Security Application PIP Comparison

Therefore, in answer to Q2, yes, security applications request more privacy-invading permissions than almost all other mobile applications across multiple mobile platforms, with the one above-mentioned exception of social media mobile applications. Security applications with raw PIPs higher than a specific mobile platform's average pose a greater risk of invading a MobDev user's privacy than other applications, especially since those averages comprise of security applications as well as social media applications, which raises those averages to their current level. Almost all tested security applications across all platforms (with one exception) had raw PIPs that are higher than the average raw PIP for each platform. Additionally, all but one of the applications had raw PIPs higher than the overall raw PIP average. This information assists in answering Q2 and indicates that security applications are the most likely to request permissions beyond what is needed for their security functions. The difference between a raw PIP of an application and both its platform raw PIP and the overall mobile average raw PIP is even more dramatic when it is noted that those averages include the high raw PIPs of the security applications. Remove those PIPs from the averages and those averages go down drastically, further demonstrating the high risk of privacy invasion for these applications. This provides a detailed answer to Q2: yes, the high PIPs for security applications indicate that there is a much greater potential for personal privacy invasion by a security application.

6 CONCLUSIONS AND FUTURE WORK

6.1 Conclusion

Android and Windows Phone both have less security risk due to no permission being granted without being requested by an application. Alternatively, iOS has a higher baseline because is automatically grants several permissions without an application's request. iOS also has less permission creep and expansion due to the limited number of available permissions on the iOS platform compared to Android and Windows Phone.

Many applications request as many permissions as security applications, accessing personal information without promise of protection often found in security applications. This could be disconcerting for MobDev users if they understood how much personal information could be accessed by mobile applications.

6.2 Platform Challenges, Improvements and Trends

The following section is a summary of challenges faced with each MobDev platform, recommended improvements for MobDev privacy, observations, and conclusions based on how each MobDev platform currently handles privacy issues (particularly in relation to the framework and how the current privacy structure for each platform fit into the framework), and potential research that could be done with or applied to the framework.

6.2.1 Android Changes and Challenges

In current and all previous versions of Android there were no privacy controls beyond clickwrapped permissions when downloading the application. In addition to the built-in capabilities to limit application permissions, there are also third-party applications that can be installed to monitor and alert a user based on the permissions an application is using. This option is convenient because it alerts a user only when the application actually requests and uses a specific permission. This helps to further reduce false positives when applications simply request permissions due to a code copy and not an actual need for permission. The biggest caveat to these types of applications is that they often request a large number of permissions to be able to monitor processes and network usage to identify when permissions are actually being used by applications. Currently, stock Android does not contain a built-in feature that allows for the management of individual permissions. However there are custom ROMs (e.g., Cyanogenmod) and third-party applications (e.g., PDroid) that allow for user management of individual permissions.

One of the biggest challenges with Android is that there is the flexibility to modify the ROM to be able to manage permissions more effectively, but users are unable to do so in stock Android. The limitations on the scope of this research to only include only stock Android reduced the options for managing permissions. However, with this research being focused on the lay user and not the technical professional, these limitations helped to study the ROM that would be most commonly used by those within the target user group: everyday users who are not going to modify the ROM on their device.

Another challenge with the Android MobDevs was that the permissions requested at install are not all of the permissions used by the application. Specifically, the “Other” category of

permissions is not displayed at the time of install for the application. A complete list of permissions used by an application and a short description can be found on devices running Android 4.4.4 following the menu Settings > Apps > "Specific Application" and then scrolling to the bottom of the screen being displayed (see Figure 6-1 for an example).

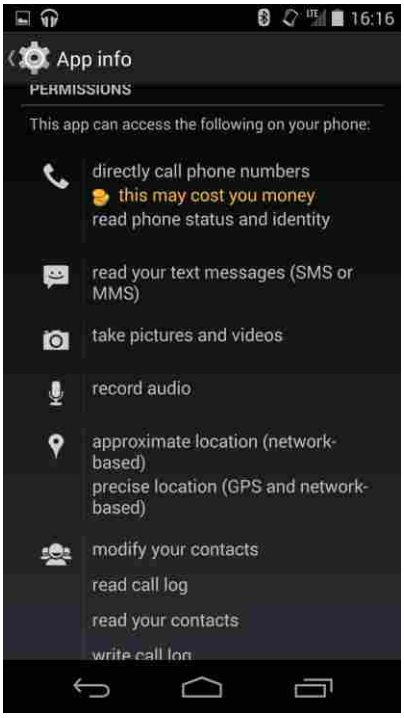

Figure 6-1: Android Application Used Permission List (Part 1)

These complete permission descriptions can be found on an application installation and information page online at the Google Play website or via the Google Play application by scrolling to the bottom of the page and clicking on the "Permissions" hyperlink (see Figure 6-2).

The selective display of permissions requested at the time an application is installed leads a MobDev owner to believe that one set of permissions were requested without detailing what all

of those permissions are, especially what is included in the “Other” permissions. This could be happening as an attempt at further data exfiltration or it might simply be an oversight. This discrepancy helps to further display risks to MobDev users (Q1) in that some privacy information and related permissions are being withheld from general users.

Androids permission granularity was not as extensive as Windows Phone (although very similar) or as limited as iOS applications. While the mid-range PIPs generated by Android facilitated the comparison of applications across platforms, Android’s average PIP was still much higher than iOS, which decreases the legitimacy of the highest permission’s cross-platform analysis of Android to iOS.

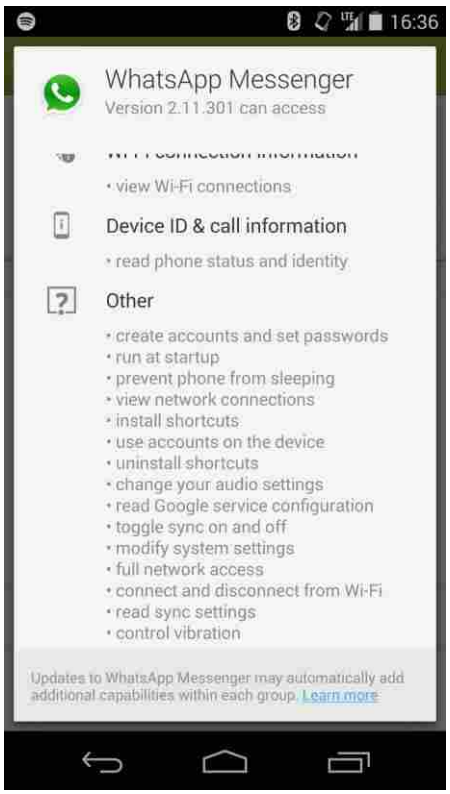

Figure 6-2: Android Application Used Permission List (Part 2)

6.2.2 iOS Privacy Changes and Challenges

Apple limits permissions that an application can request effectively by reducing the number and type of permissions to a base set of permissions (found in section 4.5.2). By not permitting an application to access permission until the application specifically needs access to that permission, iOS has provided the user with additional information about the permission and how it is used. When a user declines to enable a permission for an application, the application continues to function in a base mode while not using the feature that requires that permission.

While at first glance iOS appears to mitigate privacy permission concerns in an effective and easily understandable way, other concerns were found in the literature review both before and during this research. The biggest concerns for users of iOS devices is that Apple might be gathering personal private data from the MobDev without any permission from the user ("Why You Should Delete All Facebook Mobile Apps Right Now | Techcafeteria.com" 2014; "Facebook Messenger App Permissions Spark Privacy Concerns - Tech2" 2014). This is done through background processes that are constantly running on the MobDev. The fact that it is the producer of the MobDev implementing these privacy-encroaching features is very concerning for any user.

One challenge in this research with iOS devices is that an application does not grant access to permissions until the user completes an action that requests that specific permission (e.g., syncing Skype contacts with the contacts on the iOS device, etc.). This difficulty in enabling all permissions for each application could cause incomplete PIPs at this time, due to the manual method of collecting data for a PIP. Every effort was given in the research to enable all permissions so as to create an accurate PIP but with constant changes and inabilities to enable all potential permissions on an application there may be some gaps for iOS application PIPs.

An additional challenge faced with iOS is the mandatory environment regulations and methodology implemented on all iOS devices. Apple wants to provide a streamline experience; some of their permissions work backwards from Android and Windows Phone devices. An example of this is the Facebook application's interaction with the mobile device's calendar. With Android and Windows Phone, permission was requested by the application to access the calendar. iOS follows a different methodology: it has the calendar application request permission to access the Facebook calendar. Differences in application methodology and implementation caused most iOS application PIPs to appear less severe and safer while the same amount of information was still being transferred between applications.

6.2.3 Windows Phone Privacy Changes and Challenges

Windows phone is a port from Windows 7/8/8.1, removing some of the features found in the full versions of the operating system. Further modifications to permission requirements may have been made by developers after or during this time and may not be reflected in this analysis. Windows follows a closed source corporate model with their source code for the Windows Phone operating system, similarly to Apple's closed corporate model for iOS but contrasting with Google's open source model for Android. Windows Phone removes privacy permission management from the hands of the user, protecting the user through an application vetting process.

Windows Phone provided the most granular permissions of the three platforms used in this research. This provided easier categorization of application-specific permissions in generating PIPs for Windows Phone applications, improving the accuracy of the PIP for each application analyzed in this research. The high granularity of permissions allowed for an accurate

comparison of Windows Applications using a PIP while making it much more difficult to compare the PIP from a Windows Phone application to the PIP from an Android application and even more so with the lower PIP for iOS devices.

Another challenge with the Windows Phone was unfamiliarity with the operating system and how permissions functioned within the OS environment. This issue was overcome by forced usage and exploration of the device, in an effort to improve understanding of how Windows Phone devices operated, managed permissions, and requested permissions.

6.3 **Recommendations for Standardization of Mobile Privacy**

As evidenced by the wide array of results between applications across platforms, it stands to reason that some type of organization, or organizations, should create a standard for judging and evaluating what mobile application developers should and should not do. Each platform runs their own analysis algorithms for vetting applications but there is no standard that is being followed by the different platforms. Without a standard it is much more likely that privacy-invading applications could slip through the vetting process and be installed on a MobDev. An industry standard needs to be developed. There is one standard being drafted by NIST (Voas et al.), but it does not deal with a mobile privacy standard for more than a couple of paragraphs.

6.4 **Future Work**

A PIP, as developed in this thesis, provides detailed and simple information that allows a non-technical or non-security minded person (i.e., lay user) to understand how their information and privacy might be invaded and disseminated by a mobile application. Current limitations of the framework include (but are not limited to) the following:

1. The framework only allows for manual analysis of an application.
2. Multiple applications produced by the same company/group and the potential for information exfiltration by passing information between applications.
3. No method for directly analyzing the operating system (iOS, Android, Windows Phone).
4. Additional analysis features for social media applications, which would help to account for the high number of permissions requested by these applications.
5. Additional analysis of applications completed within the framework.

6.4.1 Streamline Application of Privacy Framework

A valuable future implementation of this framework would be to add automated analysis, either as a stand-alone application or a web application. This tool would allow a user to enter either an application's URL or the actual application (see appendix E.16 for more information) into the analysis application; the user would be returned a PIP after analysis. This could be done as either an application for each environment (Android, iOS, and Windows Phone) or as a single application capable of analyzing packages from each environment.

If platform-specific applications were created, they would run locally on a MobDev, allowing for the possibility of collecting historical data about which permissions an application requested at any time and what the PIP for the application was at that point in time. This would create a historical profile for an application, showing how a PIP changes over time with application updates. Another possibility would be to incorporate the automated analysis into the online mobile application stores (Google Play, iTunes, Windows Phone store, etc.) allowing for an application to be profiled before downloading and installing an application. While this feature

is far less likely, being able to analyze applications without installing an application and granting it permission to personal information would be a very useful feature.

6.4.2 Multiple Application Privacy Invasion Profile

This research mentioned that applications produced by the same developer or company could share permissions and resources. For example, if application A and application B were both developed by the same developer or company, and application A had location permissions and application B had full Internet access permission and permission to read data from other applications, application A could gather location data over a period of time and application B could collect that data and transmit it over the Internet to a server collecting data. With the current PIP, both of these applications would have fairly low PIPs, while the combination could potentially have a much higher PIP.

Future research and implementation could take these inter-application relationships into account when developing a PIP, especially as the MobDev operating systems continue to change and provide developers with detailed function within an API. For example, with the introduction of iOS 8 in 2014, Apple began providing developers with this ability for the first time.

6.4.3 Social Media and Privacy

Social media and digital social interactions are highly incorporated into MobDevs and mobile applications. Additional research and functionality could be added to the framework to consider, analyze, and include some of these interactions and how they affect the potential invasion of personal privacy, especially between applications and the data that is passed to social media websites and applications.

6.4.4 Additional Analysis and Usability

An additional feature that could be added to a PIP is to increase the readability for a non-technical user: take a large sample of applications across several platforms and do a statistical analysis to define overall categories for a PIP. An example of this could be to take the final PIP and define what PIP would be considered low risk, medium risk, high risk, and extreme risk. This would provide a statistical foundation to compare applications on a single platform and across multiple platforms. This could even be broken down to compare multiple features: first, against the platform the application was created for (half of the official profile) and second, then compare it statistically to all applications across platforms. These two halves could be put into a simple chart with color-coding to facilitate understanding for non-technical users.

Another form of analysis would be to compare the raw number of permissions requested to the number of permissions available on a specific platform. For example, on the Android platform if the Facebook application requested 11 raw and uncategorized permissions out of 147 individual permissions (approximately 45 of which are privacy-invading permissions) and Facebook requested 10 out of 31 permission groups (approximately 16 of which have privacy-invading permissions). A statistical analysis and comparison of how many permissions are requested by an application in relation to the total number of permissions would provide additional insight that could be added to a PIP and increase its readability.

6.5 Contributions

Privacy is a persistent concern with today's technology advancements. As MobDevs become more popular, more users will want to ensure that their privacy is protected, particularly in understanding what data permissions an application has access to and if that data is at risk for

being exploited. Previous to this research, it was found that there was no effort to create a Privacy Invasion Profile (PIP) that would help common users, as well as technical users, understand the MobDev's installed application's potential for invading privacy and distributing private data. The framework presented in this research utilized known permissions for each MobDev platform and commonly mentioned privacy-invading permissions. In summary, this research contributes the following deliverables:

- A working definition of digital privacy or working privacy definition (known as WPD in this research).
- A framework for analyzing the permissions requested by a mobile application. A "Privacy Invasion Profile" (PIP) for mobile applications. A PIP is flexible enough to evaluate future mobile platforms as well as browser extensions and other tools.
- A comparison of applications across platforms, including popular applications and security applications to demonstrate that the framework functions as designed, to identify potential privacy risks.

In conclusion, protecting individual and cooperate privacy is essential in today's world. By limiting application permissions and decreasing a raw PIP, mobile developers can increase their credibility and increase their marketability both for individual applications and as a developer. This framework provides a platform for evaluating current privacy implications for a mobile application and provides a launching point for further research into mobile privacy, specifically for mobile applications.

REFERENCES

"360 Security - Antivirus FREE - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.qihoo.security.

"Amazon.com: Apps for Android." 2014. Accessed May 13. http://www.amazon.com/mobile-apps/b/?_encoding=UTF8&camp=1789&creative=390957&linkCode=ur2&node=2350149011&tag=digitren08-20.

"Android Store (Google Play Store)." 2014. Accessed April 3. https://play.google.com/store.

"Androidrank Android Market App Ranklist - Android Rating Stats." 2014. Accessed June 14. http://www.androidrank.org/listcategory?hl=en.

"Angry Birds HD Free on the App Store on iTunes." 2014. Accessed June 18. https://itunes.apple.com/us/app/angry-birds-hd-free/id409809295?mt=8.

"App Capabilities and Hardware Requirements for Windows Phone 8." 2014. Accessed June 19. http://msdn.microsoft.com/en-us/library/windowsphone/develop/jj206936(v=vs.105).aspx.

"App Manifest | Android Developers." 2014. Accessed April 11. http://developer.android.com/guide/topics/manifest/manifest-intro.html.

"App Store Downloads on iTunes." 2014. Accessed April 3. https://itunes.apple.com/us/genre/ios/id36?mt=8.

"Apple Unveils iPhone | Macworld." 2014. Accessed April 11. http://www.macworld.com/article/1054769/iphone.html.

"Apps for Windows - Microsoft Windows." 2014. Accessed April 22. http://windows.microsoft.com/en-us/windows-8/apps#Cat=t1.

Au, K. W. Y., Y. F. Zhou, Z. Huang, Ph. Gill, and D. Lie. 2011. "Short Paper: A Look at Smartphone Permission Models." In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '11*, 63. New York, New York, USA: ACM Press. doi:10.1145/2046614.2046626.

"AVG Family Safety 8 | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/avg-family-safety-8/1df94db9-d1b4-4a6a-942e-4e04c97fb32c.

Barrera, D., H. G. Kayacik, P. C. van Oorschot, and A. Somayaji. 2010. “A Methodology for Empirical Analysis of Permission-Based Security Models and Its Application to Android.” In *Proceedings of the 17th ACM Conference on Computer and Communications Security - CCS ’10*, 73. New York, New York, USA: ACM Press. doi:10.1145/1866307.1866317.

Bélanger, F., and R. E. Crossler. 2011. “PRIVACY IN THE DIGITAL AGE: A REVIEW OF INFORMATION PRIVACY RESEARCH IN INF...: EBSCOhost.” *MIS Quarterly*, December 1. http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=0388dfe8-d3fe-405b-9ed4-69b342f0b90a@sessionmgr4002&vid=1&hid=4106.

Beresford, A. R., A. Rice, N. Skehin, and R. Sohan. 2011. “MockDroid: Trading Privacy for Application Functionality on Smartphones.” In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications - HotMobile ’11*, 49. New York, New York, USA: ACM Press. doi:10.1145/2184489.2184500.

“Best Android App Store Alternatives (if You’re Tired of Google Play) | Digital Trends.” 2014. Accessed May 13. http://www.digitaltrends.com/mobile/android-app-stores/#!NcCBw.

Christin, D., A. Reinhardt, S. S. Kanhere, and M. Hollick. 2011. “A Survey on Privacy in Mobile Participatory Sensing Applications.” *Journal of Systems and Software* 84 (11): 1928–46. doi:10.1016/j.jss.2011.06.073.

“CM Security & Find My Phone - Android Apps on Google Play.” 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.cleanmaster.security.

Crowther, B. T. 2012. “(Un)Reasonable Expectation of Digital Privacy.” *Brigham Young University Law Review* 2012 (1). Brigham Young University Law School: 343–69. https://www.lib.byu.edu/cgi-bin/remoteauth.pl?url=http://search.ebscohost.com/login.aspx?direct=true&db=lgh&AN=74260232&site=ehost-live&scope=site.

“Cydia.” 2014. Accessed April 22. https://cydia.saurik.com/.

Duri, S., M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J. Tang. 2002. “Framework for Security and Privacy in Automotive Telematics.” In *Proceedings of the 2nd International Workshop on Mobile Commerce - WMC ’02*, 25. New York, New York, USA: ACM Press. doi:10.1145/570705.570711.

Enck, W., P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. Sheth. 2010. “TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones.” In *OSDI*, 10:1–6.

“Epic | Windows Phone Apps+Games Store (United States).” 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/epic/28fcff8a-b545-487b-ae36-7da1521998df.

"Extreme Survival Run | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/extreme-survival-run/65e41b5b-68ae-4c87-ae0b-e1b50a364d72.

"Facebook - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.facebook.katana.

"Facebook | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/facebook/82a23635-5bd9-df11-a844-00237de2db9e.

"Facebook Messenger App Permissions Spark Privacy Concerns - Tech2." 2014. Accessed August 23. http://tech.firstpost.com/news-analysis/facebook-messenger-app-permissions-sparks-privacy-concerns-228735.html.

"Facebook on the App Store on iTunes." 2014. Accessed June 14. https://itunes.apple.com/us/app/facebook/id284882215?mt=8.

Felt, A. P., E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. 2012. "Android Permissions: User Attention, Comprehension, and Behavior." In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, 1. New York, New York, USA: ACM Press. doi:10.1145/2335356.2335360.

"Find My iPhone on the App Store on iTunes." 2014. Accessed June 14. https://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8.

"Fruit Ninja Free - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.halfbrick.fruitninjafree.

"Fruit Ninja Free on the App Store on iTunes." 2014. Accessed June 14. https://itunes.apple.com/us/app/fruit-ninja-free/id403858572?mt=8.

"Getjar." 2014. Accessed May 13. http://www.getjar.com/.

"Gmail - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.google.android.gm.

Han, J., Q. Yan, D. Gao, J. Zhou, and R. H. Deng. 2013. "Comparing Mobile Privacy Protection through Cross-Platform Applications." In *Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA*.

Hann, I. H., K. L. Hui, S. Y. T. Lee, and I. P. L. Png. 2002. "Online Information Privacy: Measuring the Cost-Benefit Trade-Off." *ICIS*. http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf.

Hong, J. I., J. D. Ng, S. Lederer, and J. A. Landay. 2004. “Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems.” In *Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS ’04*, 91. New York, New York, USA: ACM Press. doi:10.1145/1013115.1013129.

“Industry Leaders Announce Open Platform for Mobile Devices | Open Handset Alliance.” 2014. Accessed April 11. http://www.openhandsetalliance.com/press_110507.html.

“Instagram - Android Apps on Google Play.” 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.instagram.android.

Jeon, J., K. K. Micinski, J. A. Vaughan, A. Fogel, N. Reddy, J. S. Foster, and T. Millstein. 2012. “Dr. Android and Mr. Hide: Fine-Grained Permissions in Android Applications.” In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 3–14. New York, New York, USA: ACM. doi:10.1145/2381934.2381938.

Jeon, J., K. K. Micinski, J. A. Vaughan, N. Reddy, Y. Zhu, J. S. Foster, and T. Millstein. 2011. “Dr. Android and Mr. Hide: Fine-Grained Security Policies on Unmodified Android.” http://drum.lib.umd.edu//handle/1903/12852.

Khosla, P. 2004a. “The Quest for Personal Control over Mobile Location Privacy.” *IEEE Communications Magazine* 42 (5): 130–36. doi:10.1109/MCOM.2004.1299356.

———. 2004b. “The Quest for Personal Control over Mobile Location Privacy.” *IEEE Communications Magazine* 42 (5). IEEE: 130–36. doi:10.1109/MCOM.2004.1299356.

Levis, C. 2011. “Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy.” *Fordham Intellectual Property, Media & Entertainment Law Journal* 22. http://heinonline.org/HOL/Page?handle=hein.journals/frdipm22&id=193&div=&collection=journals.

Liang, X., X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen. 2012. “Morality-Driven Data Forwarding With Privacy Preservation in Mobile Social Networks.” *IEEE Transactions on Vehicular Technology* 61 (7): 3209–22. doi:10.1109/TVT.2012.2202932.

Lipton, J. D. 2010. “MAPPING ONLINE PRIVACY.” *Northwestern University Law Review* 104 (2). Northwestern University School of Law: 477–515. https://www.lib.byu.edu/cgi-bin/remoteauth.pl?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=56522750&site=ehost-live&scope=site.

“Lock & Hide | Windows Phone Apps+Games Store (United States).” 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/lock-hide/b74e1e88-4113-41ee-9739-ff69b33c3b66.

"Lookout – Backup, Security, Find Your iPhone, iPad or iPod Touch on the App Store on iTunes." 2014. Accessed June 14. https://itunes.apple.com/us/app/lookout-backup-security-find/id434893913?mt=8.

"Manifest.permission_group | Android Developers." 2014. Accessed May 5. http://developer.android.com/reference/android/Manifest.permission_group.html.

"Netflix - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.netflix.mediaclient.

"Netflix | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/netflix/c3a509cd-61d6-df11-a844-00237de2db9e.

"Netflix on the App Store on iTunes." 2014. Accessed June 18. https://itunes.apple.com/us/app/netflix/id363590051?mt=8.

"Pandora | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/pandora/de2df279-485d-49bb-b53e-3f6a2a9401c1.

"Pandora Radio on the App Store on iTunes." 2014. Accessed June 14. https://itunes.apple.com/us/app/pandora-radio/id284035177?mt=8.

Pearce, P., A. P. Felt, G. Nunez, and D. Wagner. 2012. "AdDroid: Privilege Separation for Applications and Advertisers in Android." In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security - ASIACCS '12*, 71. New York, New York, USA: ACM Press. doi:10.1145/2414456.2414498.

Peng, H., C. Gates, B. Sarma, N. Li, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy. 2012. "Using Probabilistic Generative Models for Ranking Risks of Android Apps." In *Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12*, 241. New York, New York, USA: ACM Press. doi:10.1145/2382196.2382224.

"Piano Tiles - Don't Tap The White Tile | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/piano-tiles-don-t-tap-the-white-tile/9a85aafb-874d-4f57-9cd2-925b3084a651.

Portokalidis, G., P. Homburg, K. Anagnostakis, and H. Bos. 2010. "Paranoid Android: Versatile Protection For Smartphones." In *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10*, 347. New York, New York, USA: ACM Press. doi:10.1145/1920261.1920313.

"Review App Permissions - Google Play Help." 2014. Accessed July 14. https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1.

Sarma, B. P., N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy. 2012. "Android Permissions: A Perspective Combining Risks and Benefits." In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies - SACMAT '12*, 13. New York, New York, USA: ACM Press. doi:10.1145/2295136.2295141.

Seriot, N. 2010. "iPhone Privacy." *Black Hat DC*, 30.

Shekhar, S., M. Dietz, and D. S. Wallach. 2012. "Adsplit: Separating Smartphone Advertising from Applications." *CoRR, abs/1202.4030*. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final101.pdf.

Shin, W., S. Kiyomoto, K. Fukushima, and T. Tanaka. 2009. "Towards Formal Analysis of the Permission-Based Security Model for Android." In *2009 Fifth International Conference on Wireless and Mobile Communications*, 87–92. IEEE. doi:10.1109/ICWMC.2009.21.

Skehin, N., and J. Chung. 2011. "Mobile Computing Systems and Applications." *IEEE Pervasive Computing* 10 (3): 80–83. doi:10.1109/MPRV.2011.53.

"Skype | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/skype/c3f8e570-68b3-4d6a-bdbb-c0a3f4360a51.

"Skype for iPad on the App Store on iTunes." 2014. Accessed June 18. https://itunes.apple.com/us/app/skype-for-ipad/id442012681?mt=8.

Smith, E. 2010. "iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)." *URL Www. Pskl. Us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues. Pdf*.

"Subway Surfers - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.kiloo.subwaysurf.

Taddei, S., and B. Contena. 2013. "Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?" *Computers in Human Behavior* 29 (3): 821–26. doi:10.1016/j.chb.2012.11.022.

"The Weather Channel for iPad on the App Store on iTunes." 2014. Accessed June 18. https://itunes.apple.com/us/app/the-weather-channel-for-ipad/id364252504?mt=8.

Thomson, J. J. 1975. "The Right to Privacy." *Philosophy & Public Affairs* 4 (4). Wiley: 295–314 CR – Copyright © 1975 Wiley. doi:10.2307/2265075.

Tschersich, M., C. Kahl, S. Heim, S. Crane, K. Böttcher, I. Krontiris, and K. Rannenberg. 2011. "Towards Privacy-Enhanced Mobile communities—Architecture, Concepts and User Trials." *Journal of Systems and Software* 84 (11): 1947–60. doi:10.1016/j.jss.2011.06.048.

Tuerkheimer, F. M. 1993. "The Underpinnings of Privacy Protection." *Communications of the ACM* 36 (8). ACM: 69–73. doi:10.1145/163381.163394.

Vidas, T., N. Christin, and L. Cranor. 2011. "Curbing Android Permission Creep." In *Proceedings of the Web*. Vol. 2.

Voas, J., K. Scarfone, S. Quirolgico, and C. Michael. *Technical Considerations for Vetting 3rd Party Mobile Applications (Draft)*. http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf.

Warren, S. D., and L. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5). The Harvard Law Review Association: 193–220. doi:10.2307/1321160.

Westin, A. F. 1968. "Privacy and Freedom." *Annals of the American Academy of Political and Social Science* 377 (May). Sage Publications, Inc. in association with the American Academy of Political and Social Science: 196–197 CR – Copyright © 1968 American Academ. doi:10.2307/1038192.

"WhatsApp | Windows Phone Apps+Games Store (United States)." 2014. Accessed June 18. http://www.windowsphone.com/en-us/store/app/whatsapp/218a0ebb-1585-4c7e-a9ec-054cf4569a79.

"WhatsApp Messenger - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.whatsapp.

"Why You Should Delete All Facebook Mobile Apps Right Now | Techcafeteria.com." 2014. Accessed August 23. http://techcafeteria.com/blog/2014/07/31/why-you-should-delete-all-facebook-mobile-apps-right-now/.

"Words With Friends HD Free on the App Store on iTunes." 2014. Accessed June 18. https://itunes.apple.com/us/app/words-with-friends-hd-free/id400949811?mt=8.

"YouTube - Android Apps on Google Play." 2014. Accessed June 14. https://play.google.com/store/apps/details?id=com.google.android.youtube.

APPENDICES

APPENDIX A. ANDROID MANIFEST – INDIVIDUAL PERMISSIONS

The Android Permissions Manifest was last accessed on May 5, 2014. ("App Manifest | Android Developers" 2014)

Android Permission Manifest

Data Type	Permissions Name	Description
String	ACCESS_CHECKIN_PROPERTIES	Allows read/write access to the "properties" table in the check-in database, to change values that get uploaded.
String	ACCESS_COARSE_LOCATION	Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.
String	ACCESS_FINE_LOCATION	Allows an app to access precise location from location sources such as GPS, cell towers and Wi-Fi.
String	ACCESS_LOCATION_EXTRA_COMMANDS	Allows an application to access extra location provider commands.
String	ACCESS_MOCK_LOCATION	Allows an application to create mock location providers for testing.
String	ACCESS_NETWORK_STATE	Allows an application to access information about networks.
String	ACCESS_SURFACE_FLINGER	Allows an application to use SurfaceFlinger's low level features.
String	ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
String	ACCOUNT_MANAGER	Allows applications to call into AccountAuthenticators.
String	ADD_VOICEMAIL	Allows an application to add voicemails into the system.
String	AUTHENICATE_ACCOUNTS	Allows an application to act as an AccountAuthenticator for the AccountManager.
String	BATTERY_STATS	Allows an application to collect battery statistics.
String	BIND_ACCESSIBILITY_SERVICE	Must be required by an AccessibilityService, to ensure that only the system can bind to it.

Data Type	Permissions Name	Description
String	BIND_APPWIDGET	Allows an application to tell the AppWidget service which application can access AppWidget's data.
String	BIND_DEVICE_ADMIN	Must be required by device administration receiver, to ensure that only the system can interact with it.
String	BIND_INPUT_METHOD	Must be required by an InputMethodService, to ensure that only the system can bind to it.
String	BIND_NFC_SERVICE	Must be required by a HostApduService or OffHostApduService to ensure that only the system can bind to it.
String	BIND_NOTIFICATION_LISTENER_SERVICE	Must be required by a NotificationListenerService, to ensure that only the system can bind to it.
String	BIND_PRINT_SERVICE	Must be required by a PrintService, to ensure that only the system can bind to it.
String	BIND_REMOTEVIEWS	Must be required by a RemoteViewService, to ensure that only the system can bind to it.
String	BIND_TEXT_SERVICE	Must be required by a TextService.
String	BIND_VPN_SERVICE	Must be required by a VpnService, to ensure that only the system can bind to it.
String	BIND_WALLPAPER	Must be required by a WallpaperService, to ensure that only the system can bind to it.
String	BLUETOOTH	Allows applications to connect to paired Bluetooth devices.
String	BLUETOOTH_ADMIN	Allows applications to discover and pair to Bluetooth devices.
String	BLUETOOTH_PRIVILEDGED	Allows applications to pair to Bluetooth devices without user interaction.
String	BRICK	Required to be able to disable the device (very dangerous!).
String	BROADCAST_PACKAGE_REMOVED	Allows an application to broadcast a notification that an application package has been removed.
String	BROADCAST_SMS	Allows an application to broadcast an SMS receipt notification.
String	BROADCAST_STICKY	Allows an application to broadcast sticky intents.
String	BROADCAST_WAP_PUSH	Allows an application to broadcast a WAP PUSH receipt notification.
String	CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call being placed.
String	CALL_PRIVILEGED	Allows an application to call any phone number, including emergency numbers, without going through the Dialer user interface for the user to confirm the call being placed.
String	CAMERA	Required to be able to access the camera device.
String	CAPTURE_AUDIO_OUTPUT	Allows an application to capture audio output.
String	CAPTURE_SECURE_VIDEO_OUTPUT	Allows an application to capture secure video output.
String	CAPTURE_VIDEO_OUTPUT	Allow an application to capture video output.
String	CHANGE_COMPONANT_ENABLED_STATE	Allows an application to change whether an application component (other than its own) is enabled or not.

Data Type	Permissions Name	Description
String	CHANGE_CONFIGURAITON	Allows an application to modify the current configuration, such as locale.
String	CHANGE_NETWORK_STATE	Allows applications to change network connectivity state.
String	CHANGE_WIFI_MULTICAST_STATE	Allows applications to enter Wi-Fi Multicast mode.
String	CHANGE_WIFI_STATE	Allows applications to change the Wi-Fi connectivity state.
String	CLEAR_APP_CACHE	Allows an application to clear the caches of all installed applications on the device.
String	CLEAR_APP_USER_DATA	Allows an application to clear user data.
String	CONTROL_LOCATION_UPDATES	Allows enabling/disabling location update notification from the radio.
String	DELETE_CACHE_FILES	Allows an application to delete cache files.
String	DELETE_PACKAGES	Allows an application to delete packages.
String	DEVICE_POWER	Allows low-level access to power management.
String	DIAGNOSTIC	Allows applications to RW to diagnostic resources.
String	DISABLE_KEYGUARD	Allows applications to disable the keyguard.
String	DUMP	Allows an application to retrieve state dump information from system services.
String	EXPAND_STATUS_BAR	Allows an application to expand or collapse the status bar.
String	FATORY_TEST	Run as a manufacturer test application, running as the root user.
String	FLASHLIGHT	Allows access to the flashlight
String	FORCE_BACK	Allows an application to force a BACK operation on whatever is the top activity.
String	GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.
String	GET_PACKAGE_SIZE	Allows an application to find out the space used by any package.
String	GET_TASKS	Allows an application to get information about the currently or recently running tasks.
String	GET_TOP_ACTIVITY_INFO	Allows an application to retrieve private information about the current top activity, such as any assist context it can provide.
String	GLOBAL_SEARCH	This permission can be used on content providers to allow the global search system to access their data.
String	HARDWARE_TEST	Allows access to hardware peripherals.
String	INJECT_EVENTS	Allows an application to inject user events (keys, touch, trackball) into the event stream and deliver them to ANY windows.
String	INSTALL_LOCATION_PROVIDER	Allows an application to install a location provider into the Location Manager.
String	INSTALL_PACKAGES	Allows an application to install packages.
String	INSTALL_SHORTCUT	Allows an application to install a shortcut in Launcher.
String	INTERNAL_SYSTEM_WINDOW	Allows an application to open windows that are for use by parts of the system user interface.
String	INTERNET	Allows applications to open network sockets.

Data Type	Permissions Name	Description
String	KILL_BACKGROUND_PROCESSES	Allows an application to call killBackgroundProcesses(String).
String	LOCATION_HARDWARE	Allows an application to use location features in hardware, such as the geofencing API.
String	MANAGE_ACCOUNTS	Allows an application to manage the list of accounts in the AccountManager.
String	MANAGE_APP_TOKENS	Allows an application to manage (create, destroy, Z-order) application tokens in the window manager.
String	MANAGE_DOCUMENTS	Allows an application to manage access to documents, usually as part of a document picker.
String	MASTER_CLEAR	Not for use by third-party applications.
String	MEDIA_CONTENT_CONTROL	Allows an application to know what content is playing and control its playback.
String	MODIFY_AUDIO_SETTINGS	Allows an application to modify global audio settings.
String	MODIFY_PHONE_STATE	Allows modifications to the telephone state-power on, mmi, etc.
String	MOUNT_FORMAT_FILESYSTEMS	Allows formatting file systems for removable storage.
String	NFC	Allows applications to perform I/O operations over NFC.
String	PERSISTENT_ACTIVITY	This constant was deprecated in API level 9. This functionality will be removed in the future; please do not use. Allow an application to make its activities persistent.
String	PROCESS_OUTGOING_CALLS	Allows an application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether.
String	READ_CALENDAR	Allows an application to read the user's calendar data.
String	READ_CALL_LOG	Allows an application to read the user's call log.
String	READ_CONTACTS	Allows an application to read the user's contacts data.
String	READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
String	READ_FRAME_BUFFER	Allows an application to take screen shots and more generally get access to the frame buffer data.
String	READ_HISTORY_BOOKMARKS	Allows an application to read (but no write) the user's browsing history and bookmarks.
String	READ_INPUT_STATE	This constant was deprecated in API level 16. The API that used this permission has been removed.
String	READ_LOGS	Allows an application to read the low-level system log files.
String	READ_PHONE_STATE	Allows read only access to phone state.
String	READ_PROFILE	Allows an application to read the user's personal profile data.
String	READ_SMS	Allows an application to read SMS messages.
String	READ_SOCIAL_STREAM	Allows an application to read from the user's social stream.
String	READ_SYNC_SETTINGS	Allows applications to read the sync settings.
String	READ_SYNC_STATS	Allows applications to read the sync states.

Data Type	Permissions Name	Description
String	READ_USER_DICTIONARY	Allows an application to read the user dictionary.
String	REBOOT	Required to be able to reboot the device.
String	RECEIVE_BOOT_COMPLETED	Allows an application to receive the ACTION_BOOT_COMPLETED that is broadcast after the system finishes booting.
String	RECEIVE_MMS	Allows an application to monitor incoming MMS messages, to record or perform processing on them.
String	RECEIVE_SMS	Allows an application to monitor incoming SMS messages, to record or perform processing on them.
String	RECEIVE_WAP_PUSH	Allows an application to monitor incoming WAP push messages.
String	RECORD_AUDIO	Allows an application to record audio.
String	RECORDER_TASKS	Allows an application to change the Z-order tasks.
String	RESTART_PACKAGES	This constant was deprecated in API level 8. The restartPackage (String) API is no longer supported.
String	SEND_RESPOND_VIA_MESSAGE	Allows an application (Phone to send a request to another application to handle the respond-via-message action during incoming calls.
String	SEND_SMS	Allows an application to send SMS messages.
String	SET_ACTIVITY_WATCHER	Allows an application to watch and control how activities are started globally in the system.
String	SET_ALARM	Allows an application to broadcast an intent to set an alarm for the user.
String	SET_ALWAYS_FINISH	Allows an application to control whether activities are immediately finished when put in the background.
String	SET_ANIMATION_SCALE	Modify the global animation-scaling factor.
String	SET_DEBUG_APP	Configure an application for debugging.
String	SET_ORIENTATION	Allows low-level access to setting the orientation (actual rotation) of the screen.
String	SET_POINTER_SPEED	Allows low-level access to setting the pointer speed.
String	SET_PREFERRED_APPLICATIONS	This constant was deprecated in API level 7. No longer useful, see addPackageToPreferred(String) for details.
String	SET_PROCESS_LIMIT	Allows an application to set the maximum number of (not needed) application processes that can be running.
String	SET_TIME	Allows applications to set the system time.
String	SET_TIME_ZONE	Allows applications to set the system time zone.
String	SET_WALLPAPER	Allows applications to set the wallpaper.
String	SET_WALLPAPER_HINTS	Allows applications to set the wallpaper hints.
String	SIGNAL_PERSISTENT_PROCESSES	Allows an application to request that a signal be sent to all persistent processes.
String	STATUS_BAR	Allows an application to open, close, or disable the status bar and its icons.
String	SUBSCRIBED_FEEDS_READ	Allows an application to allow access to the subscribed feed ContentProvider.
String	SUBSCRIBED_FEEDS_WRITE	Allows for adding subscribed feed to RSS applications.
String	SYSTEM_ALERT_WINDOW	Allows an application to open windows using the type TYPE_SYSTEM_ALERT, shown on top of all other applications.

Data Type	Permissions Name	Description
String	TRANSMIT_IR	Allows using the device's IR transmitter, if available.
String	UNINSTALL_SHORTCUT	Allows an application to uninstall a shortcut in Launcher.
String	UPDATE_DEVICE_STATS	Allows an application to update device statistics.
String	USER_CREDENTIALS	Allows an application to request authtokens from the AccountManager.
String	USE_SIP	Allows an application to use SIP service.
String	VIBRATE	Allows access to the vibrator.
String	WAKE_LOCK	Allows using PowerManager WakeLocks to keep processor from sleeping or screen from dimming.
String	WRITE_APN_SETTINGS	Allows applications to write the APN settings.
String	WRITE_CALENDAR	Allows an application to write (but not read) the user's calendar data.
String	WRITE_CALL_LOG	Allows an application o write (but not read) the user's call log.
String	WRITE_CONTACTS	Allows an application to write (but not read) the user's contacts data.
String	WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.
String	WRITE_GSERVICES	Allows an application to modify the Google service map.
String	WRITE_HISTORY_BOOKMARKS	Allows an application to write (but not read) the user's browsing history and bookmarks.
String	WRITE_PROFILE	Allows an application to write (but not read) the user's personal profile data.
String	WRITE_SECURE_SETTINGS	Allows an application to read or write the secure system settings.
String	WRITE_SETTINGS	Allows an application to read or write the system settings.
String	WRITE_SMS	Allows an application to write SMS messages.
String	WRITE_SOCIAL_STREAM	Allows an application to write (but not read) the user's social stream data.
String	WRITE_SYNC_SETTINGS	Allows applications to write the sync settings.
String	WRITE_USER_DIRECTORY	Allows an application to write to the user directory.

APPENDIX B. ANDROID GROUP PERMISSIONS MANIFEST

The Android Group Permissions Manifest was last accessed on May 5, 2014. ("Manifest.permission_group | Android Developers" 2014)

Android Manifest – Group Permissions

Data Type	Group Permission Name	Description
String	ACCESSIBILITY_FEATURES	Used for permissions that allow requesting certain accessibility features.
String	ACCOUNTS	Permissions for direct access to the accounts managed by the Account Manager.
String	AFFECTS_BATTERY	Used for permissions that provide direct access to the hardware on the device that has an effect on battery life.
String	APP_INFO	Group of permissions that are related to the other applications installed on the system.
String	AUDIO_SETTINGS	Used for permissions that provide direct access to speaker settings on the device.
String	BLUETOOTH_NETWORK	Used for permissions that provide access to other devices through Bluetooth.
String	BOOKMARKS	Used for permissions that provide access to the user bookmarks and browser history.
String	CALENDAR	Used for permissions that provide access to the device calendar to create/view events.
String	CAMERA	Used for permissions that are associated with accessing camera or capturing images/video from the device.
String	COOPERATING SYSTEM_MONEY	Used for permissions that can be used to make the user spend money without their direct involvement.
String	DEVELOPMET_TOOLS	Group of permissions that are related to development features.
String	DEVICE_ALARMS	Used for permissions that provide access to the user voicemail box.
String	DISPLAY	Group of permissions that allow manipulation of how another application displays UI to the user.
String	HARDWARE_CONTROLS	Used for permissions that provide direct access to the hardware on the device.

Data Type	Group Permission Name	Description
String	LOCATION	Used for permissions that allow access to the user's current location.
String	MESSAGES	Used for permissions that allow an application to send messages on behalf of the user or intercept messages being received by the user.
String	MICROPHONE	Used for permissions that are associated with accessing microphone audio from the device.
String	NETWORK	Used for permissions that provide access to networking services.
String	PERSONAL_INFO	Used for permissions that provide access to information about the device user such as profile information.
String	PHONE_CALLS	Used for permissions that are associated with accessing and modifying telephony state: placing calls, intercepting outgoing calls, and reading and modifying the phone state.
String	SCREENLOCK	Group of permissions that are related to screen lock.
String	SOCIAL_INFO	Used for permissions that provide access to the user's social connections, such as contacts, call logs, social stream, etc.
String	STATUS_BAR	Used for permissions that change the status bar.
String	STORAGE	Group of permissions that are related to SD card access.
String	SYNC_SETTINGS	Used for permissions that access the sync settings or sync related information.
String	SYSTEM_CLOCK	Group of permissions that are related to system clock.
String	SYSTEM_TOOLS	Group of permissions hat are related to system APIs.
String	USER_DICTIONARY	Used for permissions that provide access to the user calendar to create/view events.
String	VOICEMAIL	Used for permissions that provide access to the user voicemail box.
String	WALLPAPER	Group of permissions that allow manipulation of how another application displays UI to the user.
String	WRITE_USER_DICTIONARY	Used for permissions that provide access to the user calendar to create/view events.

APPENDIX C. WINDOWS PHONE PERMISSION LIST

The Windows Permissions list was accessed on May 18, 2014. This list is limited to Software capabilities. ("App Capabilities and Hardware Requirements for Windows Phone 8" 2014)

Windows Phone – Software Capabilities and Permissions

Permission Name	Phone Version	Description
ID_CAP_APPOINTMENTS	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to appointment data.
ID_CAP_CONTACTS	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to contacts data
ID_CAP_GAMERSERVICES	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to Xbox LIVE services. This capability must be disclosed because an app could share data with Xbox.
ID_CAP_IDENTITY_DEVICE	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to device-specific information such as a unique device ID, or the manufacturer or model name.
ID_CAP_IDENTITY_USER	Windows Phone Operating System 7.1 Windows Phone 8	Gives an app the ability to use an anonymous Microsoft account to identify the user.
ID_CAP_ISV_CAMERA	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to the rear (primary) camera or front-facing camera.
ID_CAP_LOCATION	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to location services for GPS location, both via GPS and Wi-Fi connections.
ID_CAP_MAP	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to mapping functionality.
ID_CAP_MEDIALIB	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to the media library.

Permission Name	Phone Version	Description
ID_CAP_MEDIALIB_AUDIO	Windows Phone Operating System 7.1 only. Windows Phone 8 apps should use the more specific media library capabilities.	Provides read-only access to audio items, including lists of audio items and audio items properties such as title and description, in the media library. It also provides the ability to add or delete songs. Delete operations display an additional prompt to the user.
ID_CAP_MEDIALIB_PHOTO	Windows Phone 8	Provides read-only access to photos in the media library, and photo properties, such as category. It also gives an app the ability to save photos in the Camera Roll and Saved Pictures folders.
ID_CAP_MEDIALIB_PLAYBACK	Windows Phone 8	Provides read/write access to media items that are currently playing. It also gives an app the ability to add media items to the History, Favorites, and New collections. Also supports background and foreground playback from an app's isolated storage using the MediaElement control.
ID_CAP_MICROPHONE	Windows Phone 8	Provides access to the phone's microphone. An app with this capability can record without a visual indication that the microphone is recording.
ID_CAP_NETWORKING	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to network services. This capability must be disclosed because an app could incur charges when a phone is roaming. Important Note: The networking capability is automatically included when an app is deployed from Visual Studio to a Windows Phone or Windows Phone Emulator. If your app requires networking, you must specify this capability in the app's manifest file when you submit the app to the Store. If you don't specify the networking capability, the app could fail when it's installed on a user's phone.
ID_CAP_PHONEDIALER	Windows Phone Operating System 7.1 Windows Phone 8	Provides the ability to use the PhoneCallTask API
ID_CAP_PROXIMITY	Windows Phone 8	Provides access to Near Field Communication (NFC) services.
ID_CAP_PUSH_NOTIFICATION	Windows Phone Operating System 7.1 Windows Phone 8	Provides the ability to receive push notifications from an Internet service. This capability must be disclosed because an app could incur roaming charges.
ID_CAP_REMOVABLE_STORAGE	Windows Phone 8	Provides access to data storage on an external storage component, such as an SD card.
ID_CAP_RINGTONE_ADD	Windows Phone 8	Provides the ability to add ringtones to the phone.

Permission Name	Phone Version	Description
ID_CAP_SENSORS	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to any Windows Phone sensor, including such components as the accelerometer and gyroscope.
ID_CAP_SPEECH_RECOGNITION	Windows Phone 8	Provides access to speech recognition and text-to-speech (TTS) services.
ID_CAP_VOIP	Windows Phone 8	Provides access to voice-over IP (VoIP) calling services.
ID_CAP_WALLET	Windows Phone 8	Provides access to interactions with Wallet such as saving, updating, and deleting deals, membership cards, and payment instruments.
ID_CAP_WALLET_PAYMENTINSTRUMENTS	Windows Phone 8	Provides access to Wallet payment instruments such as credit and debit cards. Doesn't grant access to the secure element for secure NFC transactions.
ID_CAP_WALLET_SECUREELEMENT	Windows Phone 8	Provides access to a Wallet secure element for secure NFC transactions.
ID_CAP_WEBBROWSERCOMPONENT	Windows Phone Operating System 7.1 Windows Phone 8	Provides access to a web browser component. This capability must be disclosed because an app could use scripting, which introduces security risks.
ID_HW_FRONTCAMERA	Windows Phone Operating System 7.1 only.	Indicates that your app has some features that require the front-facing camera. It is used only to warn users that don't have a front-facing camera on their phone. (Windows Phone 8 apps should use the ID_REQ_FRONTCAMERA hardware requirement)

The following is an enumeration of Functional Capabilities for Windows Phone deceives. ("App Capabilities and Hardware Requirements for Windows Phone 8" 2014)

Windows Phone – Functional Capabilities and permissions

Functional capability	Version	Description
ID_FUNCCAP_EXTEND_MEM	Windows Phone 8	Doesn't opt out of lower-memory devices (installs on all devices), but is granted the higher memory allocation instead of the default lower level. Requesting this functional capability means that your app receives the maximum memory limit by the phone type: 180 MB on lower memory phones 380 MB on phones with 1GB of memory.

The following is an enumeration of Hardware requirements for Windows Phone devices. ("App Capabilities and Hardware Requirements for Windows Phone 8" 2014)

Windows Phone Hardware Requirements and Permissions

Requirement	Version	Description
ID_REQ_MEMORY_90	Windows Phone Operating System 7.1	For Windows Phone Operating System 7.1, indicates that the app requires more than 90 MB of memory and is not suited for a lower-memory device. If you are using the Windows Phone SDK 7.1, including this requirement in the app manifest will not prevent the app from being deployed from Visual Studio to the 256-MB Windows Phone Emulator or a tethered lower memory device.
ID_REQ_MEMORY_300	Windows Phone 8	For Windows Phone 8, indicates that the app requires more than 180 MB of memory and is not suited for lower-memory device.
ID_REQ_FRONTCAMERA	Windows Phone 8	Indicates that an app requires a front-facing camera to function correctly. Adding this requirement prevents the app from installing on a phone without a front-facing camera.
ID_REQ_REARCAMERA	Windows Phone 8	Indicates that an app requires a back-facing camera to function correctly. Selecting this option prevents the app from installing on a phone without a back-facing camera.
ID_REQ_NFC	Windows Phone 8	Indicates that an app requires a phone with a chip that enables Near Field Communication (NFC) to function correctly. Selecting this option prevents the app from installing on a phone without an NFC chip.
ID_REQ_MAGNETOMETER	Windows Phone 8	Indicates that an app requires a phone that contains a compass to function correctly. Selecting this option prevents the app from installing on a phone that doesn't have a compass.
ID_REQ_GYROSCOPE	Windows Phone 8	Indicates that an app requires a phone that contains a gyroscope to function correctly. Selecting this option prevents the app from installing on a phone that doesn't have a gyroscope.

APPENDIX D. APPLICATION PERMISSION DATA

The following sections contain the raw data gathered from the applications analyzed for each platform as well as the individual and combination categorization for each of those permissions. Additionally, information about the number and categorization of permissions (individual and combination) for each application is detailed in the following sub-sections.

It is important to note that the numbers in the tables are before they have been multiplied by their severity factor (Extreme Risk = Multiply by 4, High Risk = Multiply by 3, Medium Risk = Multiply by 2, Low Risk = Multiply by 1).

D.1 Android Application Framework Data

Only permissions that could potentially invade privacy are listed in the following tables.

D.1.1 Facebook Application

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app history	IH2	CM4
Identity	IH2	CE2
Contacts/Calendar	IM1, IM4	CM2, CL3
Location	IH1	CE1
SMS	IH3	CH2
Phone	IL3	CL2
Photos/Media/Files	IL5	CM3
Camera/Microphone	IM3, IL4	CH1, CM1
Device ID & call information	IH2, IL3	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	3	2
Medium	4	4
Low	5	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.5	1.1
High	5	2.8	1.7
Medium	8	5.4	3.467
Low	8	6.1	3

D.1.2 Pandora Application

Permission	Permission Individual Categorization	Permission Combination Categorization
Identity	IH2	CE2
Contact/Calendar	IM1, IM4	CM2, CL3
Photos/Media/Files	IL5	CM3
Device ID & call information	IH2, IL1	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	3	3
Low	3	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.5	1.1
High	1	2.8	1.7
Medium	6	5.4	3.467
Low	6	6.1	3

D.1.3 WhatsApp Messenger

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app history	IH2	CM4
Identity	IH2	CE2
Contacts/Calendar	IM1, IM4	CM2, CL3
Location	IH1	CE1
SMS	IH3	CH2
Phone	IL3	CL2
Photos/Media/Files	IL5	CM3
Camera/Microphone	IM3, IL4	CH1, CM1
Device ID & call information	IH2, IL1	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	3	2
Medium	4	4
Low	5	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.5	1.1
High	5	2.8	1.7
Medium	8	5.4	3.467
Low	8	6.1	3

D.1.4 Netflix

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app history	IH2	CM4
Identity	IH2	CE2
Device ID & call information	IH2, IL3	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	1	1
Low	3	2

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.5	1.1
High	1	2.8	1.7
Medium	2	5.4	3.467
Low	5	6.1	3

D.1.5 Fruit Ninja Free

Permission	Permission Individual Categorization	Permission Combination Categorization
Identity	IH2	CE2
Location	IH1	CE1
Photos/Media/Files	IL5	CM3
Device ID & call information	IH2, IL3	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	2	0
Medium	1	2
Low	4	2

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.5	1.1
High	2	2.8	1.7
Medium	3	5.4	3.467
Low	6	6.1	3

D.1.6 Subway Surfers

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app History	IH2	CM4
Identity	IH2	CE2
Photos/Media/Files	IL5	CM3
Device ID & call information	IH2, IL3	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	0	2
Low	2	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.5	1.1
High	1	2.8	1.7
Medium	2	5.4	3.467
Low	3	6.1	3

D.1.7 YouTube

Permission	Permission Individual Categorization	Permission Combination Categorization
Identity	IH2	CE2
Photos/Media/Files	IL5	CM3
Camera/Microphone	IM3, IL4	CH1, CM1
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	1
Medium	1	2
Low	2	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.5	1.1
High	2	2.8	1.7
Medium	3	5.4	3.467
Low	2	6.1	3

D.1.8 Gmail

Permission	Permission Individual Categorization	Permission Combination Categorization
Identity	IH2	CE2
Contacts/Calendar	IM1, IM4	CM2, CL3
Phone	IL3	CL2
Photos/Media/Files	IL5	CM3
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	3	3
Low	4	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.5	1.1
High	1	2.8	1.7
Medium	6	5.4	3.467
Low	7	6.1	3

D.1.9 CM Security and Find My Phone

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app History	IH2	CM4
Identity	IH2	CE2
Contacts/Calendar	IM1, IM4	CM2, CL3
Location	IH1	CE1
SMS	IH3	CH2
Phone	IL3	CL2
Photos/Media/Files	IL5	CM3
Camera/Microphone	IM3, IL4	CH1, CM1
Device ID & call information	IH2, IL1	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	3	2
Medium	4	4
Low	5	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.5	1.1
High	5	2.8	1.7
Medium	8	5.4	3.467
Low	8	6.1	3

D.1.10 360 Security - Antivirus

Permission	Permission Individual Categorization	Permission Combination Categorization
Device & app History	IH2	CM4
Identity	IH2	CE2
Contacts/Calendar	IM1, IM4	CM2, CL3
Location	IH1	CE1
SMS	IH3	CH2
Phone	IL3	CL2
Photos/Media/Files	IL5	CM3
Camera/Microphone	IM3, IL4	CH1, CM1
Device ID & call information	IH2, LI1	CE2, CL2
Other	IL1, IL2 IM2	CM4, CL1, All Combinations

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	3	2
Medium	4	4
Low	5	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.5	1.1
High	5	2.8	1.7
Medium	8	5.4	3.467
Low	8	6.1	3

D.2 iOS Application Framework Data

The iOS application data in the following tables is the composite PIP for each iOS application, including 6 raw PIP points from the Operating System Factor. These 6 points come from network access permissions (IL1 and all combinations of permissions) and camera permissions (IM3 and CH1).

D.2.1 Facebook

Permission	Permission Individual Categorization	Permission Combination Categorization
Location Services	IH1	CE1
Photos	IL5	CM3

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	1
High	1	0
Medium	0	1
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	1	0.5	1.1
High	1	0.5	1.7
Medium	1	0.9	3.467
Low	1	0.3	3

D.2.2 Netflix

Permission	Permission Individual Categorization	Permission Combination Categorization
None	None	None

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	0
High	0	0
Medium	0	0
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	0	0.5	1.1
High	0	0.5	1.7
Medium	0	0.9	3.467
Low	0	0.3	3

D.2.3 Pandora Radio

Permission	Permission Individual Categorization	Permission Combination Categorization
Other Applications (Facebook)	IM2	CM4

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	0
High	0	0
Medium	1	1
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	0	0.5	1.1
High	0	0.5	1.7
Medium	2	0.9	3.467
Low	0	0.3	3

D.2.4 The Weather Channel for iPad

Permission	Permission Individual Categorization	Permission Combination Categorization
Location Services	IH1	CE1

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	1
High	1	0
Medium	0	0
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	1	0.5	1.1
High	1	0.5	1.7
Medium	0	0.9	3.467
Low	0	0.3	3

D.2.5 Skype for iPad

Permission	Permission Individual Categorization	Permission Combination Categorization
Microphone	IL4	CM1
Contacts	IM1	CM2
Photos	IL5	CM3

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	0
High	0	0
Medium	1	3
Low	2	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	0	0.5	1.1
High	0	0.5	1.7
Medium	4	0.9	3.467
Low	2	0.3	3

D.2.6 Fruit Ninja HD Free

Permission	Permission Individual Categorization	Permission Combination Categorization
Location Services	IH1	CE1

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	1
High	1	0
Medium	0	0
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	1	0.5	1.1
High	1	0.5	1.7
Medium	0	0.9	3.467
Low	0	0.3	3

D.2.7 Angry Birds HD Free

Permission	Permission Individual Categorization	Permission Combination Categorization
None	None	None

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	0
High	0	0
Medium	0	0
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	0	0.5	1.1
High	0	0.5	1.7
Medium	0	0.9	3.467
Low	0	0.3	3

D.2.8 Lookout

Permission	Permission Individual Categorization	Permission Combination Categorization
Contacts	IM1	CM2
Location Services	IH1	CE1

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	1
High	1	0
Medium	1	1
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	1	0.5	1.1
High	1	0.5	1.7
Medium	2	0.9	3.467
Low	0	0.3	3

D.2.9 Find My iPad

Permission	Permission Individual Categorization	Permission Combination Categorization
Location Services	IH1	CE1

Category	Individual	Combination
Operating System Factor	3	3
Extreme	0	1
High	1	0
Medium	0	0
Low	0	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	6	6	2
Extreme	1	0.5	1.1
High	1	0.5	1.7
Medium	0	0.9	3.467
Low	0	0.3	3

D.2.10 Words with Friends HD Free

Permission	Permission Individual Categorization	Permission Combination Categorization
Network Access	IL5	ALL

Category	Individual	Combination
Extreme	0	0
High	0	0
Medium	0	0
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	6	2
Extreme	0	0.5	1.1
High	0	0.5	1.7
Medium	1	0.9	3.467
Low	0	0.3	3

D.3 Windows Phone Application Framework Data

Only permissions that could potentially invade privacy are listed in the following tables.

D.3.1 Facebook

Permission	Permission Individual Categorization	Permission Combination Categorization
Appointments	IM4	CL3
Contacts	IM1	CM2
Phone identity	IH2	CE2
Owner identity	IH2	CE2
Video and still capture	IM3	CH1
Location services	IH1	CE1
Music library	IL5	CM3
Photos library	IL5	CM3
Microphone	IL4	CM1
Data services	IL1	All
Phone dialer	IL3	CL2
Proximity	IL2	CL1
SD card	IL5	CM3
VOIP calling	IL3	CL2
Web browser component	IM2	CM4
Videos library	IL5	CM3
Photo, music, and video libraries	IL5	CM3
Camera	IM3	CH1

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	2	1
Medium	3	4
Low	4	3

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.3	1.1
High	3	1.8	1.7
Medium	7	4.1	3.467
Low	7	2.6	3

D.3.2 Skype

Permission	Permission Individual Categorization	Permission Combination Categorization
Contacts	IM1	CM2
Phone identity	IH2	CE2
Video and still capture	IM3	CH1
Music library	IL5	CM3
Microphone	IL4	CM1
Data services	IL1	All
Phone dialer	IL3	CL2
VOIP calling	IL3	CL2
Web browser component	IM2	CM4
Photos library	IL5	CM3
Photo, music, and video libraries	IL5	CM3

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	1
Medium	3	4
Low	3	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	2	1.8	1.7
Medium	7	4.1	3.467
Low	4	2.6	3

D.3.3 WhatsApp Messenger

Permission	Permission Individual Categorization	Permission Combination Categorization
Appointments	IM4	CL3
Contacts	IM1	CM2
Phone identity	IH2	CE2
Owner identity	IH2	CE2
Video and still capture	IM3	CH1
Location services	IH1	CE1
Music library	IL5	CM3
Photos library	IL5	CM3
Microphone	IL4	CM1
Data services	IL1	All
Phone dialer	IL3	CL2
VOIP calling	IL3	CL2
Web browser component	IM2	CM4
Photo, music, and video libraries	IL5	CM3
Camera	IM3	CH1

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	3	1
Medium	4	4
Low	2	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.3	1.1
High	4	1.8	1.7
Medium	8	4.1	3.467
Low	3	2.6	3

D.3.4 Pandora

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Music library	IL5	CM3
Data services	IL1	All
Web browser component	IM2	CM4

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	1	2
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	1	1.8	1.7
Medium	3	4.1	3.467
Low	1	2.6	3

D.3.5 Netflix

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Data services	IL1	All
Photo, music, and video libraries	IL5	CM3

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	0	1
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	1	1.8	1.7
Medium	1	4.1	3.467
Low	1	2.6	3

D.3.6 Angry Birds Epic

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Music library	IL5	CM3
Data services	IL1	All
Web browser component	IM2	CM4

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	1	2
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	1	1.8	1.7
Medium	3	4.1	3.467
Low	1	2.6	3

D.3.7 Piano Tiles

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Owner identity	IH2	CE2
Photo, music, and video libraries	IM3	CM3
Data services	IL1	All
Phone dialer	IL3	CL2

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	1	1
Low	1	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	1	1.8	1.7
Medium	2	4.1	3.467
Low	2	2.6	3

D.3.8 Extreme Survival Run

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Owner identity	IH2	CE2
Location services	IH1	CE1
Data services	IL1	All
Phone dialer	IL3	CL2
Web browser component	IM2	CM4

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	2
High	2	0
Medium	1	1
Low	1	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	2	1.3	1.1
High	2	1.8	1.7
Medium	2	4.1	3.467
Low	2	2.6	3

D.3.9 AVG Family Safety 8

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Data services	IL1	All
Web browser component	IM2	CM4
Music library	IL5	CM3

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	0
Medium	1	2
Low	1	0

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	1	1.8	1.7
Medium	3	4.1	3.467
Low	1	2.6	3

D.3.10 Lock and Hide

Permission	Permission Individual Categorization	Permission Combination Categorization
Phone identity	IH2	CE2
Owner identity	IH2	CE2
Video and still capture	IM3	CHI1
Photo, music, and video libraries	IL5	CM3
Microphone	IL4	CM1
Data services	IL1	All
Phone dialer	IL3	CL2
Web browser component	IM2	CM4
Camera	IM3	CH1
Music library	IL5	CM3
Photos library	IL5	CM3

Category	Individual	Combination
Operating System Factor	0	0
Extreme	0	1
High	1	1
Medium	2	2
Low	3	1

Category	Permissions	Platform Avg.	Mobile Avg.
Operating System Factor	0	0	2
Extreme	1	1.3	1.1
High	2	1.8	1.7
Medium	5	4.1	3.467
Low	4	2.6	3

APPENDIX E. ADDITIONAL COMMENTS

E.1 Reference 1

Since the start of this research, both iOS and Android have released API access and permission for fingerprint sensors on their devices, including iPhone 5, iPad Air, iPad Mini (2nd Generation) and Samsung Galaxy S5. Other fingerprint sensor MobDevs may be released before the completion of this thesis. While this permission could have a very high risk for exploitation and privacy invasion (due to the potential of biometric information gathering) this permission will not be considered in scope or factored into a PIP for this research.

E.2 Reference 2

Samsung Galaxy S5. Other fingerprint sensor MobDevs may be released before the completion of this thesis. While this permission could have a very high risk for exploitation and privacy invasion (due to the potential of biometric information gathering) this permission will not be considered in scope or factored into a PIP for this research.

E.3 Reference 3

An exception to this is any kind of third-party login (e.g., Facebook, Twitter, Google). Typically those only collect basic login information credentials. In addition to this exception, it is not considered a privacy intrusion request nor does it enable the ability to post to a social media

website. Therefore neither of these two scenarios is considered privacy intrusion for this research.

E.4 Reference 4

Windows Phone and Android both explicitly request this permission.

E.5 Reference 5

At the time of this research, only Android MobDevs released in the last few years have NFC capabilities. This may or may not change for iOS devices and Windows Phone devices in the future.

E.6 Reference 6

Cross-application PIPs are not within the scope of this research but are addressed in Chapter 6 under future research.

E.7 Reference 7

At the Apple developer conference in June 2014, Apple introduced two additional permissions that would become available for developers with iOS 8. The first permission is access to the fingerprint scanner (located on the home button of the most current version of Apple mobile devices (i.e., iPhone 5S and newer, iPad Air and iPad mini 2nd generation). The second permission is application information sharing. This allows a developer to pass information and data from one application to another, or request information from another

application. Previous to iOS 8 applications were completely independent from each other, limiting their ability to interact with other applications.

E.8 Reference 8

With the introduction of iOS 8 developers were given the option through the API to communicate between applications and not just to access information between data. While this could increase privacy invasion risk on iOS devices because of the potential to share information between applications, this feature was not considered in developing a PIP at this time.

E.9 Reference 9

This is an implied permission. By default all iOS applications have this permission.

E.10 Reference 10

While the actual Google Store website was used for the application information an additional resource was found to help discover the most downloaded Android applications of all time. This resource is ("Androidrank Android Market App Ranklist - Android Rating Stats." 2014).

E.11 Reference 11

Some of the top applications were not available for iPad, only for iPhone. These applications were Instagram and WhatsApp Messenger. Other applications that were not available for iPad had similar applications available specifically for iPad (e.g. Skype for iPad instead of for iPhone and "The Weather Channel for iPad" instead of "The Weather Channel").

E.12 Reference 12

Some original applications were no longer available, but HD versions of the applications were available. In these cases, the HD application was installed instead of the original application. Examples of this include Words With Friends HD and Angry Birds HD.

E.13 Reference 13

This is due to the need to jailbreak the iPhone/iPad in order to install and evaluate these applications. While jailbreaking Apple device is common, this would introduce extra variables that cannot be controlled and is therefore excluded from this research.

E.14 Reference 14

This is due to the need to jailbreak the iPhone/iPad in order to install and evaluate these applications. While jailbreaking Apple devices is common, this would introduce extra variables that cannot be controlled and is therefore excluded from this research.

E.15 Reference 15

Further modifications to permission requirements may have been made by developers after or during this time and may not be reflected in this analysis.

E.16 Reference 16

APK packages for Google applications, IPA packages for iOS applications and APPX for Windows Phone applications.