RETHINKING PERMISSIONS IN ANDROID APPS

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Communication, Culture, and Technology

By

Kenneth M. Olmstead, B.A.

Washington, DC
May 1, 2013

Copyright 2013 by Kenneth M. Olmstead
All Rights Reserved

RETHINKING PERMISSIONS IN ANDROID APPS

Kenneth M. Olmstead, B.A.

Thesis Advisor: Mark MacCarthy, PhD.

ABSTRACT

As mobile devices have become a part of everyday life issues of privacy have become increasingly important to consumers, governments, and companies. Each company that provides mobile devices and platforms (e.g. Apple, Google, RIM, Microsoft) has made its own decisions on how to inform users of information the device is collecting. The primary way users interact with modern mobile devices (smartphones and tablets) is through apps. This study looked at how Google handles notifying users about what information is being collected by apps downloaded from the Google Play Store. Google uses a set of "permissions" that user's must agree to before downloading and using an app. The study looked at the permissions of 1,300 apps in the Google Play Store to determine what permissions users are agreeing to and how they are organized. From this dataset this study offers a set of recommendations on how permissions could better inform users, help app developers understand their role, and help Google improve permissions.

The research and writing of this thesis
is dedicated Professor Mark MacArthy and Professor Michael Nelson, along with all my other Professors and friends at CCT without whom this work would not be possible.

Many thanks,
Kenneth M. Olmstead

TABLE OF CONTENTS

List of Tables

INTRODUCTION

Mobile technologies have transformed virtually every aspect of modern life in a short time period. While the word “privacy” existed well before mobile devices, along with its policy and legal debates, the Internet and mobile devices have radically altered the scope of the term. In the realm of mobile devices the change has made data collection more personal. Before the dawn of mobile devices (smartphones and tablets) there were few items that most people carried on their person at all times. A wallet, a purse, and keys, the mobile device has been added to this list as something that people increasingly have on their person 24 hours a day seven days a week.

The prevalence and permanence of mobile devices gives a level of access to our everyday lives rarely shared with anyone other than our closest friends and family. According to the Pew Research Center as of January 2013, 45% of Americans own a smartphone. Mobile devices can know where we are, where we have been, and predict where we will be. They can map our daily habits, record our search queries, and learn what kind of information we prefer to consume. The companies that have access to this kind of information can do wonderful things with this information when aggregated across hundreds of millions of users, but the huge volume of information their devices are recording has sparked a new privacy debate. These companies are collecting information on a scale never seen before the last ten years. Users must be informed of the information being collected about them.

There is a tradeoff. Users and society in general can benefit greatly from information science. Users should be told upfront what they are gaining from giving up their personal information. This study will look at one method for informing users of this information: the permission list in Android apps available in the Google Play Store.

With the introduction of the smartphone the world was also introduced to the idea of an “app.” “App” is short for “application” and is shorthand for an application that runs on smartphone (or tablet), as opposed to a desktop or laptop. Apps run on the operating system of a mobile device and allow the user to tailor the experience.

The operating system is the master software for a mobile device. The operating system controls all the hardware functioning of the device and other basic functions like making phone calls or connecting to data networks. All of the major operating system providers, iOS (Apple), Android (Google), Blackberry (RIM), and Windows Mobile (Microsoft), have apps and their own versions of “appstores” through which users can download applications, for free or for a fee.

The first appstore for smartphones was launched by Apple as the iTunes appstore in 2007 along with the launch of the first iPhone. In 2008 Google launched the Android Market (rebranded the Google Play Store in 2012) for users to download Android apps. Amazon launched a similar service for users to download Amazon built apps for Android phones in 2011. Blackberry has its own appstore for Blackberry devices called Blackberry World and was launched in 2009 (originally called Blackberry App World) as does Microsoft for Windows 8 devices called the Windows Store. Each appstore has its own method for informing users about information being accessed or collected by apps.

This study examined the permission polices of 1,300 apps available in the Google Play Store. Analyzing this dataset offers one way to evaluate what information Android users are giving up to their apps. From that this study offers several recommendations on how to improve this system that will benefit both the users of Android and Google (the provider of the Android operating system).

In the Android operating system, apps must ask “permission” of the operating system to interact with any feature of the device’s hardware or any aspect of the operating system’s software. This idea of asking “permission” of the operating system is then extended to asking the user for permission as well.

For example, if the app wants to interact with the text message functions of the app it must ask the operating system to use that feature. The same permission is then addressed to the user. The app is asking the OS if it can access the text message functioning of the device and at the same time the user is being told that the app will be able to access their text messages.

Before downloading an app users must agree to a set of these “permissions” that is provided to them at the time of download in the Google Play Store (Google’s appstore, Google Play Store and Google appstore will be used interchangeably throughout this paper). The set of permissions tells the user what features of the device the app will be accessing *and* what information the app will be collecting.

In the iOS operating system app developers go through basically the same process when designing an app. Apps must “ask” the operating system for permission to use any feature of the device or the iOS operating system. Apple differs from Google in this respect. In this case Apple notifies users when an app accesses certain features. This happens at the iOS level *not* at the application level.

For example, if an app is attempting to use the GPS function of the device the user is shown a prompt explaining that the app wishes to access the GPS. This prompt is not written or provided by the app developer, but by Apple itself. In this case the process is: 1) the app developer designs the app and asks iOS to use certain features of the device 2) Apple has a set list of features that if an app is asking to access

them the user must be notified 3) the user is notified by Apple that an app is attempting to access a feature on the predetermined list.

The Android operating system operates differently. Google does not decide that users should be notified about certain features. Rather, the permission policies that users agree to when they first download an app are a way of serving the same function. For an Android app the process is: 1) the app developer asks Android to use features of the operating system 2) the entire list of features the app is asking for is presented to the user before the app is downloaded as a single list 3) the user either agrees *to all of the permissions* and downloads the app, or does not agree and does not download the app.

In this process the only place where Google steps in is during step one. Google monitors the entire Android ecosystem for malicious activity. Through this process Google can discover if an app is misbehaving. This is another difference between the Apple and Google app ecosystems that is worth noting. Every app that is submitted to the iTunes store (the Apple appstore) is screened by Apple employees for both content and function. It is at this point that Apple would see that an app is asking for what Apple deems is sensitive information.

Apps that are submitted to the Google Play Store are scanned by Google for malicious activity and functions that may crash a device, but Google employees rarely assess individual apps. Google is looking for technical issues such as apps that are being used to create spam. Apps that may be violating user's privacy may not be doing anything that is *technically* wrong and therefore would not be detectable by Google's scans.

These two systems are not a question of better or worse. Both systems have their strengths and weaknesses. This study will look at Google's permission policy scheme as one model for notifying users about what kinds of information an app is collecting and using and if it is an adequate system for notifying users of possible privacy risks. Apple's version is an entirely separate model, worthy of a study of its own.

Chapter 1

Apps in Context

Privacy has been an issue discussed (in the modern context) for over a century. Justice Louis Brandeis published the landmark article entitled "The Right to Privacy" in 1890 attempting to establish the rights citizens (in the United States) have to privacy.[1]

The Internet, and by extension the mobile space, has greatly expanded this discussion. Mobile apps are one piece of any discussion about privacy. Mobile privacy is not a "new" privacy concern per se, but rather a set of much older privacy concerns magnified by rapidly changing technologies. In other words, simply because technology has changed the methods, as well as the scale, of information collection does not mean that the essential privacy principles have changed.

A brief discussion of two theories about how to understand privacy is necessary to help put permissions into a larger framework. There are two main sets of privacy theories that will inform the discussion of mobile permissions: the harm framework and contextual integrity.

[1] Louis D. Brandeis, "The Right To Privacy," *Harvard Law Review* (1890).

First articulated by John Stuart Mill the harm principle is not specific to privacy. It is about under what circumstances any specific conduct of an individual can be limited. In his seminal work On Liberty Mill argues that: "the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others."[2]

Put another way the purpose of any law should be to prevent individuals from harming each other. A key piece of this idea articulated by Mill, but expanded on since, is that the harm must be demonstrable. There must be evidence that an individual is harmed. In the U.S. that has often been interpreted as physically or financially harmed.

Timothy Muris and J. Howard Beales argue that the real question about how to deal with personal information is actually about what harm similar information has *actually* caused harm to individuals: "A far better approach to privacy protection is to focus on the consequences of information use and misuse for consumers."[3]

The point of their article is to articulate the argument that protecting individual users' complete privacy is not the only concern. Collecting and using user information can have many benefits, including economic benefits, that companies and governments can use to benefit society as a whole. One example of this is emergency care. Ambulances could have immediate access to healthcare information. Users may be uncomfortable with a government agency having quick access to their medical records, but few would suggest that an EMT trying to save their life should not have access to the same information.

[2] Mill, John Stuart. *On Liberty and Other Essays* (Digireads Books, 2010), pp
[3] Howard J. Beales and Timothy Muris, "Choice or Consequences: Protecting Privacy in Commercial Information." *University of Chicago Law Review* 75 (2008), pp 109-135.

In the harm framework, disclosures such as permission policies for mobile apps have to be clear enough so that users are aware of the risk that information flows might be harmful to them.

An alternative is the theory of privacy as contextual integrity. It will also help inform how to evaluate whether mobile app permission policies are adequate as a form of disclosure.

Helen Nissenbaum refers to her framework as "contextual integrity" because it is a way to understand shifting values and understandings of privacy. It is uniquely suited to a constantly evolving problem. It attempts to understand privacy in terms of entrenched norms regarding the appropriate flow of information. As Nissenbaum puts it in her book Privacy in Context: Technology, Policy and the Integrity of Social Life, "What people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*, and an account of appropriate flow is given here through the framework of contextual integrity."[4] From this point of view, the key to understanding the adequacy of Android permissions is the context in which the app is used.

The mobile app environment is a microcosm of contextual integrity. In a broader sense healthcare information and financial information are two different contexts. In the app environment each app is its own context. In 2012 The Nielsen Company estimated that the average user in the United States downloads 41 apps over the life of his or her smartphone.[5] That is 41 different contexts a user must navigate. Given the vast differences between the kinds of information apps collect it is important for users to understand what the app is doing and why it is asking for certain permissions. Not all apps are created

[4] Nissenbaum, Helen , *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Standford University Press, 2010) PP.

[5] The Nielsen Company, *State of the Appnation*, May 16, 2012, http://www.nielsen.com/us/en/newswire/2012/state-of-the-appnation-%C3%A2%C2%80%C2%93-a-year-of-change-and-growth-in-u-s-smartphones.html.

equal. Mobile apps fall into categories created by Google. Map apps are generally the same, as are email apps etc.

These two theories – the harm framework and contextual integrity - are used to complement each other in understanding the role of disclosures in the mobile app environment. A flaw with the contextual integrity framework is that it relies on existing norms to make a determination about a specific situation.

As mentioned above each app typically falls into a recognized context. If an app reads a user's contact list in order to make new connections (many apps have this feature like Twitter or Facebook) there is an existing norm. Selling that contact list to a third party would be a major breach of a well-established cultural norm. An adequate disclosure system for mobile apps would let users know about a potential violation of this cultural norm. This process can work for many apps. Many apps merely move well-accepted activities into the mobile world.

There are cases, however, where apps create entirely new situations. These are cases of radically new activities that are only possible with mobile devices and newer technologies. Examples of this are apps that automatically broadcast a user's location (Google Latitude, for example). In this case it is difficult to compare this activity to an existing cultural norm because this possibility has only existed for a short time.

It is important to note in many cases new norms are developing with new apps, but the same norms are developing at different rates for different users. Some users might be comfortable embracing an app that automatically broadcasts their location, others would uncomfortable.

This is where the harm framework can be used to fill in the gaps. Is the new collection of information by a mobile app exposing users to a significant risk of harm? How can this potential for harm be balanced with possible economic or social benefits?

The questions outlined above can then begin to help deal with brand new contexts. Some contexts are well established and some are not. The mobile app world is full of both and requires both these frameworks to tackle mobile privacy concerns.

Fair Information Practice and Principles

Long before the advent of the Internet governments in the U.S., Canada and Europe began working on general principles for how governments and companies should behave when collecting personally identifiable information (PII). The Fair Information Practices and Principles (FIPPS) began in the Federal Trade Commission (FTC) in 1973 as a part of a report from the US Secretary Advisory Committee on Automated Personal Data Systems entitled Records, Computers and the Rights of Citizens.

From that starting point other U.S. government agencies and agencies in Europe took those beginning principles and built on them. Today, at least in the U.S., FIPPS are generally the same as they were when they were first released.

The FIPPS provide the most generally accepted policy framework for evaluating the adequacy of the privacy aspects of information management practices. To that end it is useful to use the most recent

interpretations of FIPPS released by the White House. This version of FIPPS has a particularly useful provision that specifically refers to "contexts" as being important when judging privacy[6]:

- **Individual Control:** Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- **Transparency:** Consumers have a right to easily understandable and accessible information about privacy and security practices.
- **Respect for Context:** Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security:** Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

How do mobile app permissions fare when looked at through the lens of these FIPPS? They certainly make users aware of how the mobile apps are functioning. Under FIPPS disclosures should let users know not only what information is being collected and how the app interacts with the mobile device, but also what is done with the information after it is collected. No permission tells the user what the company

[6] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy,* February, 2012.

will do with that information once it has collected it. That information is housed in a privacy policy that, as discussed in detail below, is usually available in a separate website (outside the Google Play Store).

Individual control as outlined by the White House is a multi-faceted concept and permission policies are a piece of that puzzle. They provide part of the disclosure that can make individual control meaningful. A related concept is the idea of if permissions are an "opt-in" or and "opt-out" system.

Opt-in vs. opt-out frameworks are much broader ideas that apply to more than just privacy. A classic example of the differences between how this choice can affect users decisions is the organ donor system. The United Network of Organ Donor Share (UOS) is a non-profit organization that tries to coordinate the organ donation system in the United States. In the U.S. it varies from state to state of individuals have to opt-in to donate their organs when the die or opt-out. In a paper trying to understand how this decision affects a real world problem researchers found that:

"109,931 people nationwide were on the United Network for Organ Sharing waiting list at 3:20pm on Wednesday, December 1, 2010. There were 8,477 donors from January until July, 2010. This discrepancy leaves tens of thousands of people to die while awaiting transplant. However, in 1999 and 2000 combined an estimated 260,000 people died in Pennsylvania alone. These deaths would seemingly leave more than enough presumptive donors to cover the demand for vital organs created throughout the entire country. Moreover, a single donor is capable of saving lives of four individuals and improve the lives of more than five additional individuals. Consequently, the number of presumptive organ donors far exceeds the number of donors actually needed to meet the demand. This demand is not being met as a direct result of presumptive donors neglecting to declare donative intent prior to death."[7]

The final sentence above, put another way, says that users are not choosing to opt-in to the donor system purely because they are either forgetting to make the decision or are not informed of the decision at the right moment in the process. The authors go on to make the point that by looking at states where the system is "opt-out" rather than "opt-in," the donation rate is far higher than in states where individuals must opt-in.

[7] Rachel Berstein, "Opt-In or Opt-Out?," Marquette Law School (2011).

This rather macabre example is an illustration of how the order and framing of a choice can dramatically affect the outcome. "Respect for context" another interesting principle that is unique to the White House list. While the other principles map almost exactly to the general FIPPS framework, respect for context does not.

This principle echoes the discussion above about Helen Nissenbaum's idea of contextual integrity. In the context of permissions this principle would be the idea that the permissions an app is asking for should reflect the general context of the app. Ostensibly an app that gives a user more ringtones should not have ready access to the GPS function of the phone or the content of user text messages. This would be out of context. The ringtone function of the phone has no reason to need access to these functions. This is not to say that there is *never* a case where an app may need a permission that seems out of context.

The "access and accuracy" principle of the White House report is another that permission policies attempt to tackle. This principle says that users need access to any information collected about them and must have the right to correct it if it is incorrect. The issue with permissions is that they state whether or not the app will be collecting information, but do not state how that information will be used. Nor do they tell users how to access information about them after it has been collected. Information about what a mobile app developer (or OS developer) will do with the information it collects is always housed in the privacy policy, rather than the permissions, as is the developer policy with respect to access and correction.

"Focused collection" is a related idea to access and accuracy, but not one addressed by permissions. This principle refers to how much information companies collect and retain. While permission policies do tell

users when information is being collected, there is no notice if that information is being retained and what is being done with it.

The final principle of “accountability” refers entirely to the practice of the companies and their data handling. Permission policies are a part of this, but in general this is a much larger question of how companies handle all of the information they are collecting.

It is important to note here that FIPPS is not a set of universal principles, the list used above is one used by the White House in the United States. Mobile technologies, on the other hand, are truly global. In that vein there are other policy processes happening around the world that seek to redefine FIPPS, or create entirely new standards for mobile privacy (and privacy in general).

The European Union (EU) has taken a different approach to dealing with privacy than the U.S. While FIPPS is a general guide in the U.S., actual laws and regulations are segmented by the type of information, healthcare, financial, etc. The EU has taken a more holistic view of privacy and in 2012 released a draft regulation to replace the existing EU privacy directive to take into account new technologies not included in the original directive. Despite the update the goal is still to enshrine “privacy” across any information type as a single idea. While the draft regulation caused a stir in 2012, its implications will be played out in the EU member states and courts for years going forward.

Concurrently the Asia Pacific Economic Cooperation (APEC) has developed its own privacy framework to deal with the same issues. The framework is a set of guidelines for businesses, governments, and other entities involved in data collection and transfer on how best to ensure the flow of information, while

protecting individual privacy. The context for this framework is clearly an economic one. As APEC states in the foreward of the framework:

"A framework to enable regional data transfers will benefit consumers, businesses, and governments. Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region."[8]

Since the adoption of that framework in 2005 APEC has continued to define its own privacy standards and in 2012 convened a working team with the EU to ascertain the interoperability of the two sets of privacy regulations. The goal for those proceedings is to ensure that that the two sets of privacy concepts can work together to foster data flows.

The focus of this paper will be the FIPPS principles as laid out above, but it is important to note that thinking on mobile privacy at the policy level is changing rapidly around the world. These principles inform a broader policy process of which permissions are one piece.

Permissions: A Form of Notice and Consent

The emphasis on notice and consent in the FIPPs framework is the dominant theme in privacy policy in the U.S. and will play a role in organizing this study. The study will examine how an app in the Android ecosystem attempts to provide notice and consent through the use of permissions. Do permissions adequately fulfill the spirit of notice and consent provided by the FIPPs framework?

This study will show that the permissions do not adequately fulfill the notice and consent portion of FIPPs. The issue is not that permissions do not provide users with *any* form of notice or consent. Clearly

[8] Asian Pacific Economic Cooperation Privacy Framework, *Asian Pacific Economic Cooperation Privacy Framework Privacy Framework*, 2005.

they do. But the notice provided by permissions, and the time at which it is provided, is inadequate. It does not give users a clear picture of what data is being collected about them and how that data is being used. An overarching issue discussed below is the distinction between the list of permission policies studied in depth in this study and the privacy policy that is generally housed outside the Google Play Store on the app developer's website.

A major piece of information not housed in the list of permissions is what happens to the information once it is collected. This is one role of the privacy policy. For many companies the list of permissions is essentially a subset of the broader privacy policy. The issue is that in this system users must go to two places to really understand what is happening to their information. The permissions tell them what their mobile device is doing and the privacy policy tells them what the company is doing with all of their information (including the information covered by the permissions). Users should not be required to do that level of research to get an idea of what is happening to their information.

This paper assesses the adequacy of the permissions in light of the principles of contextual integrity, the harm framework, and FIPPS. If an app does not provide notice when it collects information in a way that violates the contextualist principle of appropriate flow of information, then the disclosure is inadequate. If the context is so new that entrenched norms of appropriate information flow have not yet emerged, this paper will turn to the harm framework. If an app does not provide notice when it collects information that poses a significant risk of harm to the data subject, then the disclosure is inadequate.

Chapter II

State and National Privacy Policy Process

Currently the concept of mobile privacy falls under several different policy areas in the U.S. At the state level California has been most active in tackling mobile privacy issues. California passed a law requiring companies that collect data online to provide privacy policies to the public and has extended that concept to mobile app providers. In addition the Californian Attorney General has reached an agreement on mobile app privacy with major participants in the mobile ecosystem.

The mobile marketplace is made up of different entities that all have different roles. For the purposes of this study there are three main entities that have differing levels of control over user privacy: operating or "platform" providers, app developers, and third parties like advertising networks. An operating system provider (also referred to as a platform) is any company that provides the OS for a mobile device. The operating system is the software that governs all aspects of a mobile device, a mobile app runs on top of the OS and must adhere to the rules and function of the OS. The most common OS providers are Google, Apple, RIM, and Microsoft.

An app developer is any company that provides a mobile app that is available for download in an app store (in the case of this study the Google Play Store.) Finally, there are "third party" companies like advertising networks that run ads across mobile applications and even across platforms. Google runs its own advertising network, but there are others like Mobi that are neither OS providers nor app developers. These companies tie together multiple apps via their ad network. Ad Networks are important because they are often the "third party" that mobile apps share information without outside OS developers.

California Attorney General Agreement

In February 2012 the California Attorney General and six mobile platform providers (Amazon, Apple, Google, Hewlett-Packard, Microsoft, and RIM) agreed to a set of core principles about privacy in the mobile space. There were four principles that the parties agreed to:

- Where required by applicable law, mobile applications that collect personal data from their users must conspicuously post a privacy policy or some statement describing the privacy practices of the application. The policy or statement must provide clear and complete information regarding how the application and the application developer handle the personal data collected.

- Mobile platform developers will implement an optional data field that will allow application developers, in submitting their applications, to provide a privacy policy or statement regarding the privacy practices of the application. Where developers provide such information in the submission process, the platform developers will then provide consumers with access to each policy or statement through the platform's online application store or marketplace.

- Platform developers will each implement a method for application users to report to the platform developers any non-compliance by apps with their stated privacy policies, terms of service, or other applicable laws.

- Platform developers will each implement a process for responding to reported instances of application developers' non-compliance with privacy policies and/or applicable law.

From that joint statement the California Attorney General continued to work on mobile guidelines and in January 2013 issued formal recommendations directed at mobile app developers and platforms. The report was compiled using input from different stakeholders in the mobile industry (i.e. app developers, platform providers, wireless carriers).

The recommendations themselves are organized by what party the recommendations are aimed at. The report includes specific recommendations for: app developers, mobile ad networks, app platform providers, operating system providers and mobile carriers.

The first set of recommendations attempts to give app developers guidelines to think about during the app development process. The guidelines suggest that the first step for an app developer is to create a checklist to categorize the kinds of data the app will be using. The second step is to decide what information can be categorized as "personally identifiable." The third step, create a statement based on this checklist that will inform consumers about the information being collected or accessed by the app.[9]

The guidelines go on to give some information on what kinds of information app developers should be more careful about collecting and notifying about. Once this is in place it must then be formulated into a privacy policy. The report singles out "short form statements" as important for app developers to create based on their privacy policies. This paper argues that permissions in the Google Play Store are a type of "short form" notice.

[9] California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, January, 2013.

In broad terms the report urges app developers to be transparent above all else. The point of creating these checklists and privacy policies is to inform consumers of how their information is being collected and used.

The recommendations for platform providers are less specific, but in general the theme is the same. Platforms should provide users with information on how and when their information is being collected by the platform. The report emphasizes that the platform should educate and provide tools to app developers to enhance their ability to protect their user's privacy.

One interesting piece of the California guidelines is that it directly addresses advertising networks. The guidelines are essentially the same as the recommendations for other players. Advertising networks should provide clear privacy policies that tell users what data is being collected. The California report goes one step further; it gives advertising networks direct technical suggestions on how to serve mobile ads. For example, the report advises advertising networks to: "Avoid delivering ads outside the context of the app. Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop."

Advertising networks are in a unique position. Ad networks can circumvent the functioning of an app and take a user outside of the app they are using to serve an ad in the mobile browser. This puts the advertising network outside the control of the app developer and the platform provider.

These recommendations came from the original joint statement, but California's effort to affect change in the world of mobile apps started earlier than these two documents.

California Online Privacy Protection Act

Currently there is no national legislation directly related to mobile app privacy. California, though, has regulations relating specifically to mobile privacy. In 2003 (effective in 2004) California passed the California Online Privacy Protection Act (calOPPA). The act required any company operating a website or online service to have a privacy policy explicitly telling consumers that their personal information is being collected, how that information is being used, and if it is being transferred to third parties other than the originating entity.

In December 2012 the California attorney general used the act to sue Delta Airlines. The issue was Delta's mobile application "Fly Delta." The suit alleges that at the time of the suit the app collected significant amounts of personally identifiable information (PII). Delta did not provide a privacy policy specifically for that app in any of the stores from which the app could be downloaded or anywhere on Delta's website.

The California law does not specify where or how the information should be posted, simply that it has to be "readily accessible." Delta did not have the information *anywhere*. The law, however, does not say that the information has to appear in the app permissions or in an appstore.

Presumably because the information is being collected by a mobile app users should be told within the app that their information is being collected by the app itself, but the law does not say Delta has to organize the information that way. In a larger company, like Google, where users are interacting with multiple services on various platforms the decision of how to inform users becomes complex.

Federal Trade Commission Mobile App Privacy Report

In February 2013 the FTC released a staff report outlining how mobile app developers should treat users. The report said that app developers must clearly tell users when their information is being collected and what the app is doing with that information.

The report outlined several measures mobile app developers should take to ensure users understand what is being done with their information. The recommendations were tailored to different players in the market (like the White House version of FIPPS): platforms and operating system providers, app developers, advertising networks, and finally a loosely defined group of app developer trade associations, academics, usability experts and privacy researchers.

The report made many recommendations relating to permission policies for both app developers and platform and operating system providers. The first in both categories is: “Provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation.”

Permissions tell users that an app will access some feature of the phone and the user must agree to all the permissions or not download the app. There are several problems with this setup. The first is that it assumes that users agreeing to permissions mean that the user is affirming that the app can collect all of the information it is asking for. If some of the apps are asking for 40 or more permissions it is unreasonable to expect that a user is giving express consent for all of the permissions.

One controversial solution to this problem is “just-in-time” notifications. These kinds of notifications can be served by the apps or by the platforms (as discussed above Apple provides just-in-time notifications at the OS level) or by app developers in individual apps (or by both). With this kind of notification users would be prompted each time an app is asking to collect some kind of information or turn on some feature. For example, if a user was interacting with an app that offers coupons and the app asks for the user’s GPS location in order to serve more relevant coupons then the app must tell the user it will be accessing the GPS function of the phone.

A problem with this kind of system is who is responsible for giving the notification? In the Apple ecosystem Apple has taken it upon itself to give this kind of notification. In the Google ecosystem the onus is on the app developer to choose to do this or not.

According to the FTC report “...before allowing apps to access sensitive content through API’s, such as geolocation information, platforms should provide just-in-time disclosure of that fact and obtain affirmative express consent from consumers.”

Another interesting proposal is to create a kind of dashboard that collects and categorizes what kinds of information all of the apps on a device are collecting in one convenient place. This proposal could help users keep track of all the permissions they have cumulatively agreed to.

One final recommendation, only for platform and operating system providers, is to create a “Do Not Track” regime specifically for mobile devices. Users should be allowed to opt their device out from any

tracking by any app by changing one setting, as opposed to opting out in every individual app.[10] This is an adaptation of the "Do Not Track" regime already being put in place for browsers on the web.

The report also recommends that app developers work more closely with ad networks and third parties. An example of how this could work in the app world is a company called Flurry. Flurry is one of many mobile services that app developers (not users) can work with to collect cross platform data on how users interact with apps. The benefit for an app developer is that Flurry not only helps the app developer with complex analytics about the app they own, but developers also gain access to anonymized data from all of the other apps Flurry works with that shows how users interact with apps.

The purpose of Flurry is to serve more relevant ads, but the data they are collecting comes from tens of thousands of individual apps all owned by different developers. In the context of mobile permissions users are notified that information is being collected on how they use the app, but they are not told in the same place that the same information is being used to power services like Flurry.

This is an example of a more general issue of permission policies. They do not disclose what the information is being used for. They do not even say to whom the information is provided such as ad networks. The permission polices say simply that it is being collected. This is related to a more general problem with permission policies. Often the information that third parties obtain user information is disclosed to the user, but it is disclosed in the privacy policy that is located in a separate location.

[10] Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency*, February 1, 2012.

In order to get a full picture of what information is being collected, and where it is going, users must go to two completely separate locations. The objective of the permissions disclosure is simply to tell the user how the app is interacting with the mobile device, while the privacy policy is a much broader document covering all of the user's information collected by that app's developer. In the case of Google, for example, a user with an Android phone interacts with Google across mobile devices and web based platforms (like Google Search). The Google privacy policy covers *all* Google services, while the permissions of the Gmail mobile application only refer to that app.

The above are the most important recommendations of the FTC report. Many recommendations are repeated for different players in the mobile space. The final three recommendations for app developer trade associations are all about education:

- Develop short form disclosures for app developers;
- Promote standardized app developer privacy policies that will enable consumers to compare data practices across apps;
- Educate app developers on privacy issues[11]

Concurrently with the FTC process the National Telecommunications & Information Administration (NTIA) is holding meetings to attempt to better structure mobile privacy notifications.

[11] Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency*, February 1, 2012.

National Telecommunications & Information Administration Multi-stakeholder Process

In June of 2012 the NTIA announced it would begin a process that would bring together platform providers, app developers, regulators, researchers and users together. As the NTIA puts it the goal of the meetings would be to: "…develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data."[12]

The current principles resulting from this process are in draft form and outline suggestions for short form notices (of which Android permissions are one type) and how to better link those short form notices to longer form privacy policies. The suggested guidelines state what kinds of information app developers must disclose to users and how those notifications should be organized. The process is entirely voluntary for app developers currently.

The first set of criteria for app developers refer to what kinds of data app developers must disclose they are collecting, there are seven key kinds of data according to the current draft[13]:

- **Biometrics** (information about your body, including fingerprints, facial recognition, signatures and/or voice print.)
- **Browser History and Phone or Text Log** (A list of websites visited, or the calls or texts made or received.)
- **Contacts** (including list of contacts, social networking connections or their phone numbers, postal, email, and text addresses.)

[12] National Telecommunications & Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency*, Updated April 3, 2013.

[13] National Telecommunications & Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency*, Updated April 3, 2013.

- **Financial Information** (Includes credit, bank and consumer-specific financial information such as transaction data.)
- **Health, Medical or Therapy Information** (including health claims and information used to measure health or wellness.)
- **Location** (precise past or current location and history of where a user has gone.)
- **User Files** (files stored on the device such as calendar, pictures, text, and video.)

The information listed above is covered, in some form, in the Android permission policies. The next set of criteria, however, refer to cases where apps should disclose when and with whom they then share the data they have collected. This set of information is not covered in Android permissions as they are currently written. The draft recommends that app developers should tell users when they share data with the following third parties[14]:

- **Ad Networks** (companies that display ads to you through apps.)
- **Other Apps** (The company that built, owns, or controls Other apps that the consumer may not have a relationship with.) [The App Publisher is not a third party.]
- **Carriers** (Companies that provide mobile connections)
- **Data analytics providers** (Companies that collect and analyze your data.)
- **Government entities** (Any sharing with the government except where required by law.)
- **Consumer Data resellers** (Companies that buy and/or sell consumer information to other companies for multiple purposes including offering products and services that may interest you.)
- **Operating systems and platforms** (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.)

[14] National Telecommunications & Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency*, Updated April 3, 2013.

- **Social networks** (Companies that connect individuals around common interests.)

The short form notices should cover all of the information on both of these lists. The draft goes on to make some design suggestions for how the short form notices should be written and presented. Finally, the draft suggests that apps link to their longer form privacy policies.

This final point is one that is implemented in some, but not all, of the apps covered in this study. The key takeaway from the NTIA process for current Android permission policies is that it provides a checklist of information that should be disclosed to users. Permissions evaluated in this study technically provide some information to users about the kinds of data being collected. But the disclosures are not complete or displayed in ways that are useful for users.

Chapter III

Mobile Privacy Research

There has been research on mobile applications in the private sector as well as academia. The research covers many different areas. In 2008, Caium Tang and Dapeng Oliver Wu did a study published by the Institute of Electrical and Electronics Engineers (IEEE) looking at location information in modern wireless networks.

This research focused mainly on the networks themselves and how location information could be stolen over the network. While they did not look directly at permissions for apps their research is relevant to this discussion because four of the permissions discussed below relate to location information.

The research demonstrated that location information provided by mobile networks can be accessed by third parties in certain situations. The permissions specifically related to this are "Approximate Location (network based)," "Precise Location (GPS and Network Based,", "Mock Location," and "Access Extra Location Provider Commands." These permissions allow an app to use cell phone towers, GPS and Wi-Fi networks to triangulate the location of a user. According to this research the location information collected from cell towers is not entirely secure and that fact is not disclosed in the current permissions language.[15]

[15] Caimu Tang. "Mobile Privacy in Wireless Networks Revisited." *IEEE Transactions on Wireless Communications* Vol. 7 Issue 3 (2008).

Giving Users Choice

In 2011 four researchers in the United Kingdom attempted to create a technical solution to the issue created when many different apps collect user information and use different settings. Currently each app has its individual set of permissions and settings. This forces users to look at each app individually to discern what information is being collected. There is no way to get a holistic view of the information being collected by a mobile device.

This results in users having dozens of potential locations to look at. The researchers created a program called "MockDroid." The purpose of the program is to do exactly what was discussed above in the choice and consent section of FIPPS.

It gives users the option when agreeing to permission policies to turn off certain features before they begin using the app. According the authors: "This approach allows users to revoke access to particular resources at run-time, encouraging users to consider the trade-off between functionality and the disclosure of personal information whilst they use an application."[16]

The idea is that MockDroid gives users a better understanding and control over the permissions they are agreeing to and allows them to better understand the connection between the permissions and the functions of the app that are actually affected. One question about this method is at what moment the choice is presented.

[16] Alastair Beresford and Andrew Rice et al, "MockDroid: trading privacy for application functionality on smartphones," *HotMobile (*2011)

Currently users must download the MockDroid app and install it on their device. Once it is downloaded MockDroid then runs each time the user attempts to run any of the other apps they have downloaded, giving the user the option to turn on or off features in each app. The problem with this process is that users must first download an app to run it and have MockDroid screen it. In the case of apps users pay for it is only *after* they download an app and install it that they get the choice to turn features on or off. If they are presented with a situation where there are so many features they want to turn off that they no longer want the app, there is no way to refund their money. This is a clear example of how important the moment of choice is.

Another issue with MockDroid comes from how apps run in the Android environment. All apps on Android are "sandboxed." This means that each app only has access to information from the Android operating system. It cannot directly interact with other apps on the phone. For example, the Gmail email client cannot change or affect in any way the functioning of the Facebook mobile app. This feature is mostly for security reasons; it prevents malicious apps from running amok ruining other mobile applications.

Mockdroid is sandboxed, just like any other app on Android. So it cannot directly affect any other app. It must work solely through the Android operating system. The problem this creates for MockDroid is one of truly cross-app functionality. In theory MockDroid will give users the option to turn off features the user feels are hurting their privacy across any app. However, MockDroid will only be able to do this if the app in question *already offers* this option, and has implemented it in its relationship with the Android operating system. In other words MockDroid cannot force turn off features of another app if that app does not already provide the option.

This does not diminish the ability of MockDroid to provide information to users, but it does diminish the possibility to truly be a one-stop shop for both information and the ability to turn features on or off.

Understanding Privacy Contexts

To better understand the different contexts of privacy in mobile social networking researchers at the University of Bath Department of Computing used focus groups to try and better understand how users address their own privacy in the context of mobile social networking.

The researchers found that users did not have one set of processes or opinions about their own privacy in the context of mobile social networking. Rather that mobile social networking is really an extension of social networking in general and privacy is a complex issue as a result:

> "Secondly, according to our findings, mobile contexts seem to be multi-faceted entities defined by a complex articulation of groupings and sub-groupings whose interactions are regulated by individual perceptions, exclusively shared knowledge, unspoken codes of conduct, and different types of interconnection between the physical and virtual world. Our study indicates a need to systematically investigate these facets."[17]

In the context of mobile social networking each individual's perception of their own privacy seemed to shift depending on the social network and who they were interacting with on the network. For example, when asking participants of the study to talk about their Facebook habits researchers found that many participants would choose to share certain kinds of information differently with different people on Facebook as the researchers put it:

[17] Clara Mancini et al, "From Spaces to Places: Emerging Contexts in Mobile Privacy," (paper presented at the Proceedings of the 11th International Conference on Ubiquitous Computing, Orlando, Florida, September 30-October 03, 2009).

"Inside knowledge boundaries. These were set in communication contexts within Facebook amongst network members or between members and non-members. Participants seemed to use contextual knowledge to establish privileged, exclusive or private communication channels with individuals or groups."[18]

Put another way users would post to Facebook and include information that only certain people among their network would know the context for and therefore be able to understand the post. This is a way to communicate in one fashion to certain people and not to others without resorting to changing Facebook privacy settings. However, the researchers found that the criteria for this option were constantly shifting depending on the intended group. In some cases participants did want their entire Facebook network to understand their musings; in other cases they were attempting to target specific individuals.

In another study about mobile social networks Chen and Rahman, researchers at the University of Massachusetts Lowell found that in the case of some mobile social networks it is unclear how much location information is being collected and is publicly available from social networks.[19]

As the researchers put it: "The analysis of the privacy designs for existing mobile SNAs suggests that both feedback and control of information construction and accessibility are weak for existing applications. A particular problem is automatic mash-ups between various SNA sites, which expose personal information flow to multiple entities and inconsistent access policies may result in privacy breaches..."[20]

---

[18] Clara Mancini et al, "From Spaces to Places: Emerging Contexts in Mobile Privacy," (paper presented at the Proceedings of the 11th International Conference on Ubiquitous Computing, Orlando, Florida, September 30-October 03, 2009).

[19] Chen, Guanling and Farug Rahman, "Analyzing Privacy Designs of Mobile Social Networking Applications," (Paper presented at Institute of Electrical and Electronics Engineers (IEEE) and the International Federation of Information Processing (IFIP) International Conference on Embedded and Ubiquitous Computing, Shanghai, China, December 17-20, 2008).

[20] Ibid.

The researchers are referring to cases where social networks allowed users to broadcast their location. That location was also fully accessible to outside parties, including the researchers. In one such case researchers found that in the case of the mobile Twitter app users could agree to have the app automatically attach location information to each tweet a user posted. The researchers were then able to map the movements of some prolific Twitter users.

The study was conducted of the Twitter iPhone app, but the principle is the same for Android. In the case of the Twitter app on Android devices users agree to the permission policy that says the app can access users location information using both “approximate location” and “precise location.”

The UMass study shows that even in the case of Twitter, which tells users expressly and more than once that their GPS location is being accessed, the language states that Twitter shares geolocation information of each Tweet via the public API. This means that location information on most Tweets is publicly available (while the full feed of everything on Twitter in real time, the “fire hose,” does have a fee associated with it, this geolocation information is available in other ways at no cost).

The geolocation settings differ from the website, to the Android app, to the iPhone app. The privacy policy on the Twitter website is the only place where Twitter states how the information can be used, including sharing some location information with third parties. What the UMass study shows is that some users are choosing to include location information with their Tweets; but what these users may not know is that the information can be used to create fairly detailed maps of their routines by anyone with the programming skills.

Android Permissions Studies

As mentioned above Android permissions are actually serving two purposes. The first purpose is the app asking the operating system for permission to access certain functions and the second is to then relay that information to the user. A group of researchers at Berkeley created a program to map the permissions an app is asking for to the permissions that are actually presented to users. The goal was to discover if apps are using features that they are not disclosing to the user in the permission policies.

The study found that around one-third of the 940 apps the researchers studied were using permissions that were not disclosed in the permissions presented to users.[21] The researchers found that in most cases the apps were only missing a few permissions in their disclosures and as a result came to the conclusion that in most cases these are probably simply errors of documentation: "Our results show that applications generally are over privileged by only a few permissions, and many extra permissions can be attributed to developer confusion. This indicates that developers attempt to obtain least privilege for their applications but fall short due to API documentation errors and lack of developer understanding."[22]

The researchers concluded that app developers most likely misunderstood the connection between the functioning of the app and disclosing those functions to the user. A further question is that even if the permission policies were constructed correctly, do users actually read or understand them?

[21] Felt, Porter Adrienne, Erika Chin, Steven Hanna, Dawn Song and David Wagner. "Android Permissions Demystified." (Paper presented at the Conference on Computer and Communications Security, Chicago, Illinois, October 17-21, 2011).

[22] Felt, Porter Adrienne, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin and David Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," (Paper presented at Symposium on Usable Privacy and Security, Washington , DC, July 11-13, 2012).

User Comprehension of Permissions

A study at the University of California Berkeley attempted to answer this question through surveys and laboratory experiments. The study found that 17% of respondents in both the survey and the lab experiments paid any attention to the permission policies at all; the other 83% paid no attention to the permissions during the installation process. More telling, of the17% that did read the permission policies, only 3% were able to answer three comprehension questions about the permission policies they had just read.

While the study did find a small minority of participants that did demonstrate both attention and comprehension of the permissionaa, the vast majority did not. The researchers concluded that this indicates that Android permissions are not adequately preparing users to make decisions about their privacy. If most users are not even reading the permissions, let alone understand them, it is clear that Android permissions are not doing the job they were designed for, "However, low rates of user attention and comprehension indicate that significant work is needed to make the Android permission system widely accessible."[23]

This study will look at the permission policies themselves to better understand how users are presented with information about their privacy. It quantifies the number and type of permissions that users agree to when they download apps and describes when and how choices are permitted. The results of this study lead to recommendations as to how the same information can be presented in a more effective way.

[23] Felt, Porter Adrienne, Erika Chin, Steven Hanna, Dawn Song and David Wagner. "Android Permissions Demystified." (Paper presented at the Conference on Computer and Communications Security, Chicago, Illinois, October 17-21, 2011).

Chapter IV

Study Design and Findings

Mobile devices have changed the way users interact with almost every other aspect of their lives. From banking, to relationships, to news, mobile devices touch on so many aspects of everyday life it is often hard to fathom how much information these devices collect. It is less obvious how, and if, society will be able to deal with these new information flows as they rapidly evolve.

This study focuses on one area where users interact directly with mobile operating system providers (e.g. Google and Apple). In the world of smartphones (and tablets) the main way through which users interact with these devices is through the use of apps. Apps are incredibly varied in their purpose and function. As of Fall 2012 there were 675,000 apps in the Google Play Store spread across 26 categories and 700,000 apps in the iTunes Store spread across 23 categories. Throughout this paper the term “app” will be synonymously with “mobile application” and will only refer to mobile applications. Everything from email, to weather, to health has an app. To borrow a phrase from Apple, there is an app for that.

This study will cover the top 25 apps in 26 categories in the Google Play Store (both the top free and top paid app in each category for a total of 50 app per category) for a total of 1,300. App permissions in the Google Play Store are freely available to any user on the web or through the Google Play Store on mobile devices on the Android operating system.

The basic tool for analysis was a matrix of 1,300 apps and 126 permissions, where each column shows a permissions used by an app, and each row shows the apps that use a permission. Additional information was collected about each app: if the app was free or paid, if it was paid the price of the app, the category

the app was placed in by Google (games, social networking, etc.), how many times the app had been downloaded in the previous 30 days, and finally the total number of permissions the app required.

The permission policy of an app is presented to a user once the user clicks “install” in the Google Play Store. In the case of a free app the user clicks “install” and is then presented with a second screen that asks the user to “accept and download.” What the user is “accepting” are the permission policies listed on screen.

In the case of a pay app the process is slightly different. Here the user clicks “buy” (sometimes it is a button that lists the price of the app) and is then prompted to click a button that says “accept and buy.” On this screen the user can review the permissions and then choose to purchase the app. If the user agrees they are then sent to the payment process. In either case in order to download and use an app the user is always presented with the permissions and prompted to “accept.”

A side issue, not covered in this paper, is how apps are updated. In the Google Play Store the user can choose to automatically update apps or not. By default apps are not automatically updated and the user must prompt the app to update automatically. There is one case, however, where the user is asked to agree to the permission of the app a second time.

In most cases the user merely hits “update” and the new version of an app is downloaded and installed. If an app has an update that includes a *change to the permissions*, then the user is prompted to agree to the new list of permissions, the added permissions are displayed at the top and labeled as “new.”

As stated above apps are presented to the user in 26 categories organized by the function of the app.

App Categories

The list of top apps was recorded and coded between January 1st and January 14th, 2013 and coded from the web version of the Google Play Store found here: https://play.google.com/store/apps?feature=corpus_selector

The first category "Games" is subdivided into eight sub-categories in the Google Play Store. For the purpose of this study "Games" is treated a single category and the top apps in the "Games" category were studied, as opposed to the individual types of games.

Every category in the Google Play Store is represented in this study, except for one: Widgets. Widgets were not treated as a separate category in this study because they themselves are not "apps"; they are rather add-ons to existing apps that allow apps to be placed on the home screen. In addition all of the apps that appeared in the "Widgets" category are represented in one of the other categories below.

The categories studied as presented by the Google Play Store are:

1. Games
2. Books & Reference
3. Business
4. Comics
5. Communication
6. Education
7. Entertainment
8. Finance

9. Health & Fitness
10. Libraries & Demo
11. Lifestyle
12. Live Wallpaper
13. Media & Video
14. Medical
15. Music & Audio
16. News & Magazines
17. Personalization
18. Photography
19. Productivity
20. Shopping
21. Social
22. Sports
23. Tools
24. Transportation
25. Travel & Local
26. Weather

Some other considerations were made when picking apps:

- The first category of “books and reference” includes apps that are really app version of books. These books are apps. The alternative are books ordered through the Google Play Store that are only readable through the Google Books app. This study included only books that appeared in the “books and reference” list. It did not include books sold through the Google Books app.

- In some cases users can download an app and then must download a “license” from the Google Play Store to use the full version of the app. In the Google Play Store they are listed separately as an app and a “license” for the app. The “license” for the app was skipped in this study and the next app on the list was coded. This is because the “license” is not an app in itself, but rather a piece of software that tells the developer that the user wanted to buy the full version of a free app. As a result “licenses” are not apps and therefore do not have a permissions (or the “license” carries the exact same permission as the app being licensed).

Study Findings

The first step to understanding permission policies is to understand the sheer volume of permissions. This study found that among the sample of 1,300 apps there were 126 separate permissions an app could ask for.

The average number of permissions an app uses is 8, but there is a wide variance across different types of apps. On the high end one app asked for 47 permissions. On the low end 97 of the 1,300 apps asked for no permissions at all.

There is a relationship between the types of apps and the number of permissions they ask for. Apps categorized as Communications or Social use the most permissions on average, 17 and 14 respectively. This makes sense given that these types of apps have more functionality than apps that, for example, set a user’s wallpaper. It follows that more complex apps would more permissions.

On the other end of the spectrum Medical, Education and Live Wallpaper apps ask for only 4 or so permissions on average. These apps are more varied in what they do. Live Wallpapers for example are

merely animated backgrounds for smartphones. (Wallpapers are static images, while “live” wallpapers are animated and usually interactive)

Table 1. Average Number of Permissions by App Category

App Category	**Average Number of Permissions**
Communication	16.98
Social	14.30
Travel	10.44
Tools	10.30
Business	9.96
Productivity	9.68
Music	8.70
Transport	8.44
Personalization	7.78
Media & Video	7.66
Lifestyle	7.57
Health & Fitness	7.46
Shopping	7.40
Weather	7.32
Sports	7.30
News & Information	7.16
Game	6.90
Photography	6.84
Entertainment	6.66
Comics	6.24
Financial	6
Books & Reference	5.42
Medical	4.84
Education	4.66
Live Wallpaper	4.31
Libraries	3.18

Paid vs. Free Apps

The average price of the apps in the paid category was $3.77. This number was skewed by a handful of apps that cost well above that average. The majority of apps cost between $0.99 and $3.00.

The most expensive apps on the list are highly specialized apps, with the most expensive of all being a GPS Navigation app for aviators priced at $49.99.

Table 2. Price Range of Apps

App Price	Number of Apps
$0.99	131
$1.00-$2.00	160
$2.00-$3.00	113
$3.00-$4.00	80
$4.00-$5.00	77
$5.00-$6.00	19
$6.00-$7.00	8
$7.00-$8.00	8
$8.00-$9.00	5
$9.00-$10.00	24
$10.00-$11.00	3
$11.00-$12.00	2
$14.95-$14.99	9
$16.81	1
$19.99	5
$29.99	2
$37.99	1
$39.95	1
$49.99	1

Free apps ask for more permissions than paid apps do. On average apps that are free ask for nine permissions; paid apps only ask for six. One explanation is that there are several permissions related only to Google services that only appear in the free apps category (because all Google apps are free). Another explanation comes to light when comparing apps that have both free and paid versions: advertising.

In three apps in this study there is some evidence that permissions are being asked for in order to serve ads. The app Kids Math and Numbers comes in a "lite" (free) and a paid version. The paid version of the app asks for no permissions at all while the free version asks for six. The free version also has less features than the paid one (so the extra permissions cannot be attributed to some extra feature of the app). Three of the six permissions are related to allowing the app to connect to the Internet, while the other three allow the app to see certain functions of the phone.

Another app called ROM Manager fits a similar pattern. ROM manager is an app that helps user's that have "rooted" their phone deal with the applications on the phone.[24] ROM Manager has a free and premium version (that costs $5.99). The only discernible difference between the two is that the premium version allows users to turn off advertisements in the settings menu. The free version of ROM Manager asks for 11 permissions, while the premium version asks for three.

Yet another app called BaconReader for Reddit has some evidence that its paid version requires fewer permissions because of its lack of advertising. The free version of BaconReader for Reddit asks for 10 permissions in total, while the premium version asks for seven. Across these examples there are two types

[24] In the world of Android devices the term to "root" a device means to give the user more access to the OS on the phone than is normally allowed. Users that choose to root their devices gain "root access" to the Android OS. There are several reasons user would want to do root their phones. Many carriers (Verizon, AT&T, etc.) place restrictions on certain functions available in the Android OS. Another is that rooting a device allows applications not available in the Google Play Store to be installed on the device. Rooting is generally for more advanced user's.

of permissions in particular that seem to separate the free apps from the paid ones. In the case of BaconReader the free version asks to find the user's location using the "Approximate Location (Network-Based)."

The other type of permission is that in these examples the free version also asks for different kinds of network permissions. In the case of Bacon Reader, Rom Manager, and Kids Numbers and Math the free version of the app asks to interact with Wi-Fi networks, while the paid version does not. In the case of Kids Numbers and Math the free version asks for several other permissions related to connecting to the Internet.

The explanation of the location information is fairly straightforward; the app can find a user's location to serve more relevant ads. The need for connection to the Internet also makes sense; however in the case of BaconReader and ROM manager the different versions ask for different kinds of network connections and it is unclear why this is.

In both cases the paid and free version of these apps do ask for permissions to connect to the Internet. ROM manager premium asks for "View Network Connections," while the free version asks for that permission and "View Wi-Fi Connections" and "Receive Data From Internet." The same pattern appears in Bacon reader, the free version asks for network and wi-fi connections but the paid version only asks for network connections. It is less clear how different types of connections to the Internet would help apps serve ads.

Among paid apps, however, there does not seem to be a relationship between the price of the app and the number of permissions the apps ask for. While some of the higher price apps do ask for more permissions

on average,these apps require more features of the device. For example, the paid app that asks for the most permissions is an app called Tasker. Tasker costs $1.99 and asks for a total of 43 permissions, putting in second place for any app in the sample, including free apps (Viber: Free Calls & Text was the only app that asked for more permissions, 47 in total).

Tasker requires this high number of permissions because it is an app that can control virtually every function of the phone. Its purpose is to allow users to set schedules for most features of the phone by time of day, date, GPS location, specific events like a phone call, and several other variables. Tasker is simply a versatile app and therefore would need more permissions than a less complex app.

Table 3. App Price by Category

App Category	Average App Price
Travel	$8.85
Business	$8.49
Transport	$5.43
Communication	$5.05
Medical	$4.61
Productivity	$4.59
Sports	$4.31
Financial	$4.07
Personalization	$4.06
Music	$3.92
Weather	$3.53
Media & Video	$3.49
Tools	$3.36
Books & Reference	$3.17
Shopping	$2.98
Entertainment	$2.97
Health & Fitness	$2.91
Social	$2.74
Lifestyle	$2.63
Photography	$2.56
Education	$2.33
News & Information	$2.30
Game	$1.96
Live Wallpaper	$1.75
Libraries	$1.64
Comics	$0.41

Another way to look at these permissions is to look at how often the permissions themselves appear across all apps.

Frequency of Permissions

Given the number of permissions, 126, it is important to note that not all permissions are used with the same frequency. Table 4 displays how often permissions are used. It shows, for example, that 56 permissions are used by fewer than 10 apps, and that only1 permission is used by over 1,000 apps. One hundred of the 126 permissions are used in 50 or fewer apps. Well over half the permissions are only used by less than 20 apps and 15 of the permissions only appear in one app out of the total 1,300.

Table 4. Permissions by Number of Uses

Number of Apps that Use A Permission	Number of Permissions In Each App Range
Over 1,000 apps	1
500-1,000 apps	6
200-500 apps	9
100-200 apps	10
50-100 apps	10
10-50 apps	44
1-10 apps	56

The permissions that are used the most are permissions that are required for most apps to function. The permission that was used the most often was “Full Network Access” and it was used by 1,085 apps.

This permission allows apps to access data networks that the device is connected to. Many apps need this permission to create connections to the Internet. While it is not required for an app to connect to the Internet, it does allow apps to create connections that are more specific to each app’s needs. The permissions states: “Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.”

On the other end of the spectrum, permissions that are used infrequently are some permissions that are very specific, and in many cases give the app access to PII or vital device functions. The permission “Modify Your Own Contact Card” was used by only one app (Google +) and gives the app the ability to modify the user’s information in the “contact card” on mobile devices.

Essentially the “contact card” is the place on the device where all of the personal information like the user’s name is stored and this permission allows the app to modify or add to it. The permissions states: “Allows the app to change or add to personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.”

Because Google + is a Google product and integrated into the Android OS itself, this permission is not out of the ordinary in its use by Google+; still it is a sign of a possible privacy risk. If this same permission were used by other apps it would be more troubling.

Another example of a permission that rarely used gives an app access to sensitive information of the device “Retrieve System Internal State.” This permission is only used by three apps and states: “Allows the app to retrieve internal state of the system. Malicious apps may retrieve a wide variety of private and secure information that they should never normally need.” This app also includes a curious phrase, “malicious apps,” that is discussed in further detail below.

It is this idea, that some permissions are more serious than others, that leads to the next finding of this study, that the current categories permissions are organized by are insufficient to reveal privacy risks.

Categorizing Permissions by the Information Accessed

The next finding of this study is that the categories permission are currently in, as presented by Google, are confusing and insufficient to reveal privacy risks. There are 126 permission policies found in this

sample that an app could theoretically ask for and they are broken into nine categories by the current system.

Those categories are not particularly useful for user's and are often disorganized themselves. The current categories are: Services That Cost You Money, Your Accounts, Your Location, Your messages, Your Personal Information, Hardware Controls, Network Communications, System Tools, and Default. But these categories do not reveal the extent to which information flows might pose privacy risks.

This study finds that the permissions could be reorganized into three categories based on what kinds of information the permission collects or interacts with: permissions that collect or access no information at all, permissions that collect or access information that is device related and is not PII, and finally permissions that do collect or access PII. These categories are exclusive, permissions do not fall into more than one category. However, it is important to note that over time permissions could move between categories as PII is formally redefined.

PII is information that can be used to identify individuals; a useful version of this list appeared in the Children's Online Protection Act (COPPA) and is a person's: first and last name, physical address, social security number, email address.[25]

After COPPA was passed the FTC amended its Children's Online Protection Rule to include new forms of PII: IP address, device ID, cookies, geolocation information, photo's, videos and audio files (in the case of COPPA that "contain the child's image or voice, for this study that is expanded to any user's

[25] Children's Online Protection Act of 1998, 15 U.S.C § 6501-6506 (1998)

image of voice). For purposes of this study, user information includes these additional types of information.[26]

Those pieces of information by themselves can identify an individual; however at some point *all* information about an individual becomes PII when combined with other information.

There is an interesting discussion to be had here about the boundaries of PII itself. For the purpose of this paper PII will include the traditional definition as listed in COPPA, plus the additional forms listed above. There is an argument to be made that even PII as currently defined is becoming outdated by advances in technology. The key concept to understand about how the FTC defines PII is that any information that can be used with *reasonable effort* to identify an individual person is considered PII.

Technology is rapidly changing the definition of "reasonable." As Paul Ohm puts it in his article "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization": " Reidentification science disrupts the privacy policy landscape by undermining the faith we have placed in anonymization." Put another way, PII as traditionally defined may not be enough to protect user's privacy in the face of advancing computer science technologies.

While this paper focuses on uses PII as traditionally defined, there will be some discussion below of how PII becomes blurred in the case of Android permissions.

[26] Federal Trade Commission, *Statement of FTC Chairman Jon Liebowitz Updated FTC COPPA Rule*, December 19, 2012.

Criteria for Categorizing Permissions

The first criterion used to determine which category a permission falls into is if the permission is asking to record information. Certain permissions, like “Control vibration” which was used by 338 apps, do not ask for any kind of information. In this case users should consider the permission, but it poses little or no threat to the user’s privacy and would therefore be put in the first category.

In the case of “control vibration” the biggest harm that could come to a user is that the battery life of the device could be adversely affected by the vibration. In this case this permission is not collecting any information at all about the user or the device; it is merely allowing the app to turn on or off a hardware feature of the device.

The second criterion is if the app is asking to collect information, what kind of information is being collected? In this case not all information is created equal. Some permissions ask for information about the functioning of the device so the app can function more efficiently, but do not collect information about the user or information from which the user could be identified.

An example this is a permission “read sync settings,” used by 49 apps. This permission allows the app to read the settings through which the phone is automatically syncing information. By default some mobile devices will sync email data, this permission allows an app to see if that sync setting is turned on or off, but does not allow the app to read the information being synced. The permission merely allows an app to see *whether or not* information is being synced. It poses little threat to the user because there is no PII being recorded or any other information about the user. The app is simply trying to read sync settings so it can set up its own data syncing process and would therefore be placed in the second category.

Finally there are permissions that collect user information. “Read call log”, used by 143 apps, is an example of this. In this case the app is asking for the ability to read the user’s call log. The app will have the ability to look at the outgoing, incoming and missed calls. In this case both phone numbers and names (if the name is in the user's contact list) would be available to the app. In the case of the read sync settings permission the information collected poses no threat to the user’s privacy, in the case of “read call log” it could pose some threat to users privacy.

To determine whether information poses a threat to a user’s privacy the earlier discussion of contextualism and the harm principle is a useful guide. The question users must ask, and app developers must consider, is does collecting this information pose a threat to users privacy if it is used improperly. Is there another context that the permission can be compared to?

In the case of “read call log” the comparison would be something like a person’s address book (assuming actual paper address books are still in use). Would a user readily give their address book to a third party and is there a reasonable expectation that the third party would have to disclose what they will do with that information? While selling address books is not a normal practice, it can be assumed that in that case a company would be expected not to resell that information without telling the user and could not use that information to discriminate against the user in any way.

If there is not analogy to be made with an established norm then the harm principle comes into play. There is a permission called “Read Your Social Stream”, used by four apps, which:

“Allows the app to access and sync social updates from you and your friends. Be careful when sharing information -- this allows the app to read communications between you and your friends on social networks, regardless of confidentiality. Note: this permission may not be enforced on all social networks.”

Given that social networks are a relatively new phenomenon, let alone interacting with social networks via a mobile device, there is no readily available norm to drawn on to determine how to treat this permission. As a result the harm principle becomes necessary. Could an app with this permission create a significant risk of harm to a user? Given the broad language in this permission the answer to that question would be yes.

These three criteria are a way for users to better understand the permission they are agreeing to. But they are also ways to reorganize the permission policies in a more useful way to understand the extent to which the activity poses a privacy threat.

The purpose of these three categories is to give users a sense of what permissions to pay more attention to and which to pay less. Organizing the permissions according to whether they control the device, collect device information or collect user information gives users a more useful way to understand how the permissions relate to their personal information and so the extent to which the permission might create a privacy risk.

Permissions That Collect or Access No User Information

The first categories of permissions are those that do not collect, or access, any user information at all. These permissions fall into two general functions. The first is permissions that only control hardware functions.

The permission “Control Flashlight,” used by 46 apps, allows an app to use the flashlight found in most devices (smartphones and tablets) that include cameras; according to definition the “Control Flashlight”

permission: “Allows the app to control the flashlight.” This permission does not access any user information (or any information at all), its only function is allow an app to turn the flashlight on or off.

The second general function of the permissions in this category could be called “software control.” These permissions do interact with some kind of software functioning of the app, but they do not control, access, or record any user information. An example of this is “Reorder Running Apps,” used by six apps.

This permission states that: “Allows the app to move tasks to the foreground and background. The app may do this without your input.” This is a functioning of the software, giving priority to one app over another. It does not, however, give an app with this permission access to any user information or allow the app to interact with other applications it is reordering.

Another good example of a permission that gives the app control over some aspects of the software and hardware of devices is the permission that allows the app to interact with the sleep function of the device. Android devices can be set to “sleep” after a certain period of non-interaction from a user the device will go to sleep. Sleep is generally meant to prolong the battery life of devices by shutting off certain functions. These functions can include: turning the device screen off, lowering the functioning speed of the processor, and turning off some data syncing functions.[27]

The permission title is “Prevent Tablet From Sleeping Prevent Phone From Sleeping”, used by 474 apps, and the permission: “Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.”

[27] This is not an exhaustive list of functions, just some examples. The sleep function varies by device.

Generally permissions in this category are simple, they only give the app permission to interact with one functioning of the device and usually it is to turn on/off a hardware or software functioning of the device. Some of the permissions, however, are slightly more complex.

An example of this is “Draw Over Other Apps,” used by 31 apps. The “Draw Over Other Apps” permission says: “Allows the app to draw on top of other applications or parts of the user interface. They may interfere with your use of the interface in any application, or change what you think you are seeing in other applications.” In short this permission allows an app to prioritize itself over other apps and other parts of the user interface. For example the Go SMS Pro app is an instant messaging app. In that context “Draw Over Other Apps” allows the Go SMS Pro app to display an incoming instant message to a user when another app is being used.

This permission does not allow the app to access any information in other apps, it merely allows the app to display information over other running apps. One issue with this permissions is overly broad and vague language (which will be discussed in detail below): “They may interfere with your use of the interface in any application, or change what you think you are seeing in other applications.” That language implies that this permission actually gives the app fairly broad powers to manipulate what is being displayed on the device. While it does not imply that the app can collect any user information, it does have security implications.

The question of device security is a different, but related, question that is worth consideration in further research. For example, while the “Control Vibration” permission mentioned above poses no threat to user’s information, an app could use this to seriously harm the functioning of the device (on purpose or by accident.)

Many of the permissions in this category (and many of the permissions on the full list) can pose a threat in this way. This paper's focus is on user's privacy and the security of their information and does not assume any malicious intent on the part of an app. This is not the only frame for organizing this same list of permissions. An interesting study would be to take these same permissions and look at them from the perspective of device and network security.

This category contains permissions that, at least from the point of view of user information and privacy, pose the least threat and therefore are least important to be displayed to the user.

Permissions That Collect or Access Information That is Not PII

The second category of permissions contains those that do access some kind of information, but not PII. These permissions are much more varied than the first category and cover virtually all aspects of device function.

A good example of this kind of permission is "View Wi-Fi Connections," used by 410 apps. This permission allows an app to view all of the Wi-Fi Networks that have been saved by the device (or that the device is connected to). While this kind of information is device related, it is not defined as PII.

Another example of a permission in this category is one that allows an app to read information about other applications on the device. The permission "Retrieve Running Apps," used by 118 apps, says: "Allows the app to retrieve information about currently and recently running tasks. This may allow the app to discover information about which applications are used on the device." This permission allows apps to see what other apps are installed on the device and which apps are running. This kind of

information could not be used to identify the user of the device. It is, however, important to tell users that apps that have this permission do have access to the kinds of activities the user does on the device.

The two above permissions only allow an app to read or collect information about the device, but there is another kind of permission in this category that allows the app to *modify* information. The permission "Modify or Delete the Contents of Your USB Storage Modify or Delete the Contents of your SD Card," used by 884 apps, allows an app to: "Allows the app to write to the USB storage. Allows the app to write to the SD card." This permission is in the second category because it allows the app to modify information on external device storage (as SD Card or USB Drive), but does not interact with or read any user information.

Generally apps in this category perform functions like the examples above. They collect, read, or write some kind of information on the device, but it is not PII. The distinction, and importance, of "modify" vs. "read" vs. "edit" is discussed further in a section below. These terms do not determine which category a permission is placed in in this scheme, but they are important terms for a user to understand.

For example there are permissions whose sole function is to allow the app to delete data. The permission "Delete All App Cache Data," used by three apps, is also in the second category because while it can interact with all kinds of data stored in the cache, it can only delete the data. The permissions says:

"Allows the app to free tablet storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re-retrieve their data. Allows the app to free phone storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re-retrieve their data."

The cache on a mobile device is a part of the device memory where all apps can store temporary files. Often the cache is used to help apps that are used frequently start up faster, by having certain files stored in the cache they can be accessed more quickly than files stored in other parts of the device memory. Generally this permission is used by apps that attempt to speed up a mobile device or create more memory on the device by deleting the cache files of other apps. While it is important for users to be aware an app has this permission, it does interact with PII and can only delete information in the cache, not read or write to it.

These permissions are not as important as the third and final category, but users should be made aware of these permissions in a clear way. The final category includes all permissions that interact with, read, write, or edit information that is classified as PII.

Permissions That Collect or Access PII

The final category is the most important to make users aware of. These permissions allow an app to directly collect, access, or change PII, stored either on the device, on external device storage like an SD card, or data accessed through the cloud. To end up in this category permissions must fulfill one of two criteria. The first, if a permission interacts with any kind of PII it is put in this category.

The second criterion is whether the definition of the permission includes three key phrases. There are 21 apps that were automatically included in the third category because of this. None of these permissions expressly interact with any PII on the device (though in many cases the language is sufficiently vague that they might, a point discussed in detail below). These permissions include one of the following phrases: “not for use by normal apps,” “should never be needed for normal apps,” and “malicious apps...”

Because it is clear that permissions that use these three phrases are being singled out, these permissions are put in this third category. It is often unclear *why* these phrases are included, but for now it is sufficient evidence to put these apps in the third category. The issue of what these phrases mean is discussed in detail below.

An example of a permission in this category that allows apps to access traditional forms of PII is "Read Your Contacts," used by 163 apps, it states:

"Allows the app to read data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge."

This permission gives apps the ability to access traditional PII like first and last name, postal address, e-mail address, and phone number. The scope of this permission depends largely on the level of detail in the user's contact list. At the very least the app would be able to access the user's name (first and last) and email address. Beyond that it could also access any other information the user includes about him or herself and information about each individual in the contact list.

Other permissions in this category allow apps to access newer forms of PII. For example, "Read Your Web Bookmarks and History," used by 26 apps, gives the app access to all of the user's web bookmarks and all of their surfing history: **"**Allows the app to read the history of all URLs that the Browser has visited, and all of the Browser's bookmarks. Note: this permission may not be enforced by third-party browsers or other applications with web browsing capabilities."

This would give the app access to PII because it would allow the app to access cookies on the mobile device. Having access to a user's web bookmarks and surfing history could give the app a lot of personal information, including a host of PII. Because the permissions do not say what the app will do with this information this permission is fairly broad, and creates the risk of an unspecified range of possible harms.

Some permissions were put in this category because the permission expressly says it has access to private or personal information, but does not specify what kind. An example of this is "Read Sensitive Log Data," used by 12 apps. This permission says that it:

"Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the tablet, potentially including personal or private information. Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, *potentially including personal or private information*." (emphasis added)

Unlike the first two examples, "Read Your Contacts" and "Read Web Bookmarks and History," this permission does not outline exactly what kind of information it is collecting and therefore makes it impossible to define if it is collecting PII or not. The language, however, does expressly state that the app could access information "potentially including personal or private information." It is unclear what this means, but Google felt the need expressly say that the app could access "personal" or "private" information, which implies some kind of PII.

The final kind of permission in this category is also one that Google felt the need to make user's expressly aware of, but it is often unclear why. These permissions were in put in the third category because they included one of the phrases mentioned above.

The permission "Display Unauthorized Windows," used by one app, includes the phrase "Not for use by normal apps.", but does not appear to have access to any PII: "Allows the app to create windows that are

intended to be used by the internal system user interface. *Not for use by normal apps*." (emphasis added) This phrase appears in eight permissions.

While this permission is only used by one app, it is hard to understand why the app would need this permission at all. The app is called GO Keyboard and based on its description it is an alternative keyboard to the stock Android keyboard. There are dozens of other similar keyboard apps, but GO Keyboard is the only one that asks for the permission "Display Unauthorized Windows." Given the vague language of the permission it is unclear why this app needs this permission but others do not.

A similar phrase "Should never be used by normal apps." appears in five permissions. For example "Bind to a Wallpaper," this permission is used by 3 apps and states: "Allows the holder to bind to the top-level interface of a wallpaper. *Should never be needed for normal apps.*" (emphasis added)

Here again this permission does not appear to allow the app to access any kind of PII, but by including the phrase "should never be used by normal apps" it is safe to assume that for whatever reason this permission is more potentially harmful than permissions that do not include that phrase

Finally the term "malicious app…" appears in 12 permissions. In each case the words "malicious app" are followed by a different activity. For example, the permission "Edit Your Text Messages (SMS or MMS)," used by 35 apps, states: "Allows the app to write to SMS messages stored on your tablet or SIM card. Malicious apps may delete your messages. Allows the app to write to SMS messages stored on your phone or SIM card. *Malicious apps may delete your messages*." (emphasis added)

Another permission "Directly Call Phone Numbers," used by 105 apps, states:

"Allows the app to call phone numbers without your intervention. This may result in unexpected charges or calls. Note that this doesn't allow the app to call emergency numbers. *Malicious apps may cost you money by making calls without your confirmation.*" (emphasis added)

In both cases the permission uses the phrase "malicious apps…", but in neither case does the permission appear to grant the app access to any kind of PII. The main issue with these three phrases is that they are vague, but are clearly there to point out danger to the user. A full list of permissions and their definitions (categorized by the above criteria) is available in Appendix A.

From these findings this study will make several recommendations for how these permissions could be made more useful for users.

Chapter VI

Recommendations

From these findings this study will make several recommendations for how these permissions could be more useful for users. These recommendations fall into four general categories. The first is related to the categories outlined above and will explain how these new categories can benefit users. The second is related to how the new categories for permissions can be displayed to the user given the small screen size of mobile devices. The third is the language of the permissions themselves. As currently written they are often confusing and not written in a way a normal user can understand. Rewriting the permissions is key to making them more useful for users (this includes combining some permissions that appear to overlap to a great extent). The fourth is using permissions to also inform users what happens to their information once it is collected, how it is used, and if it is shared with third parties other than the app developer.

Benefits of Organizing the Permissions by Privacy Concerns

As discussed above Google currently organizes permissions into eight categories: services that cost you money, your accounts, your location, your messages, hardware controls, network communications, system tools, default. These categories do not relate to privacy risks, and as a result, they provide no guidance to users about privacy risks. A privacy threatening permission could appear in any of the eight current categories. So users would have to check all of them to be sure they were finding permissions that generate privacy concerns.

Putting the current permissions into the new categories as laid out in Chapter 5 of this study would help to make the permissions more useful for users:

- Permissions that collect or access no user information (PII)
- Permissions that collect or access information that is not PII
- Permissions that collect or access PII

By categorizing the permissions according to the information they collect it would give user's a better way to understand how the device is collecting information about them. It might seem that the current categories for permissions do give users an understanding of how the device is collecting information by including categories like "Your location" and "Your Messages." However, the permissions currently under these two categories, however, do not all interact with PII, and so pose very different privacy risks. Put another way, not all permissions that relate to your location and your messages are created equal with respect to privacy because some collect personal information and some do not. Displaying permissions

by categories that are constructed according what information is collect is a more helpful way to direct user's attention to privacy issues.

The first two categories offered by this study – permissions that interact with the hardware and permissions that collect information that is not PII – include permissions that users certainly have the right to know about. But they do not necessarily need to be presented with those permissions first.

Because of the small screen on mobile devices all of the permissions cannot be presented without the user having to scroll (some apps ask for such a small number of permissions that scrolling is not an issue, but their permissions would still be categorized according to the information collected). By limiting the first screen to just permissions in the third category it would create room on the first screen to show users the permissions they should be most aware of.

There would then be an option to see the list of permissions in first two categories on a separate screen. In some cases an app will require no permissions that fall into the third category (or no permissions at all). In those cases the first screen would simply state: "This app requires no permissions that interact with your personal data. Click here to see permissions the app does require."

This touches on another problem with the current Google Play Store permissions setup that involves apps that do not require any permissions to run. There are two different phrases that appear when an app does not ask for any permissions: "This application requires no *unsafe* permissions to run." and "This application requires no *special* permissions to run." (emphasis added)

It is unclear what the difference between these two phrases is. For example the app "Kids Numbers and Math" says that it requires no *special* permissions to run while another app Simple Sticky Note says it requires no *unsafe* permissions to run.

Kids Numbers and Math is an app that helps kids learn math skills through games and tests and Simple Sticky Note allows users to put notes on their home screen. Both are fairly straightforward apps and it makes sense that they would not require permissions. The difference between the two phrases, however, is not apparent given the functions of these two apps.

In apps that use the phrase that includes "unsafe" often also include a "show all" link (mentioned above) that then includes additional permissions. In the case of Simple Sticky Note "Run at Startup" appears below the "show all" link. This lack of clarity in these two phrases leads to another issue found in some apps in this sample.

Typos and Incorrect Permissions

Some of the apps in the sample included typos and incorrect permissions. In the example above "Access Extra Location Provider Commands" had a typo (in the definition "to to" appears, a typo). More troubling examples are apps that seem to ask for permissions they do not need or apps that do not ask for permissions they seem to need.

On the former one app entitled "Sex Facts" is the only app in the sample that asks for the permission "Force Tablet Reboot Force Phone Reboot." The app is not complicated; it gives the user random facts about sex and allows them to share those facts. The app only asks for four permissions in total and the

other permission are common ones that many apps ask for: “Full Network Access,” “Control Vibration,” “View Network Connections,” and “Force Tablet Reboot Force Phone Reboot.”

The first three permissions are not only common but necessary for many apps to function at all. The permission “Full Network Access” is used by 1,085 apps and in this case is need for the app to give users the facts and for the users to share those facts. In the proposed new categories “Full Network Access” falls under the second category because it accesses device information but no PII.

“Control Vibration” is used by 338 apps and only allows the app to control the vibrate function of the phone. “Control vibration” falls under the first category because it does not access any information at all. “View Network Connections is used by 918 apps and allows the app to see what networks the device is connected to. “View Network Connections” would fall under the second category as well, like “Full Network Access” it also accesses information, but not PII.

Finally there is “Force Tablet Reboot Force Phone Reboot.” As noted this is the only app that uses this permission and it allows the app to: “Allows the app to force the tablet to reboot. Allows the app to force the phone to reboot.” This permission is not required for any app to function given the purpose of this app it is hard to see why it would need this permission at all. According to the categories outlined by this study this permission would still fall into the first category, though this would be a case where Google should look into apps that use this permission given its ability to harm the device.

Another example of seeming overreaching that is related to the collection of PII is the Brightest LED Flashlight app. According to the description of this app, and after testing the app, it is clear that this app is incredibly simple. It only has two options when loaded, a button to turn the flashlight on or off and a

button to turn the sound on or off (the flashlight can make a noise when turned on). There is no settings menu and the only other item on the screen is advertising. Despite this seemingly barebones app it asks for a total of 16 permissions.

Of those 16 permissions six fall under the first category, eight in the second and three in the third. The three permissions this app asks for that collect some kind of PII are: “Precise Location (GPS and Network-Based)”, “Approximate Location (Network-Based),” and “Read Phone Status an Identity.”

There are two explanations why this app would require all of these extra permissions other than “Control Flashlight.” The first is error on the part of the developer (this paper will assume not malicious intent, though that is another option). While this is possible, and does explain some of the issues above like typos, it is unlikely in this case. Because this app only theoretically needs one permission to run it is unlikely the developer included an extra 15 by accident. The more plausible example is that the app has advertising (discussed in Chapter 5).

While the current permission screen does attempt to deal with the issue of screen space with a “show all” link, that link is often misused and makes the categories more confusing. In some cases the “show all” link appears when there is plenty of room to show the permissions already and in others categories appear on screen twice as a result of the show all link.

Changing the “See All” Link

The first recommendation is to put all permissions in one of three mutually exclusive categories – permissions that operate the hardware, permissions that collect device information and permissions that collect user information. Related to that is the display related recommendation that the permissions that

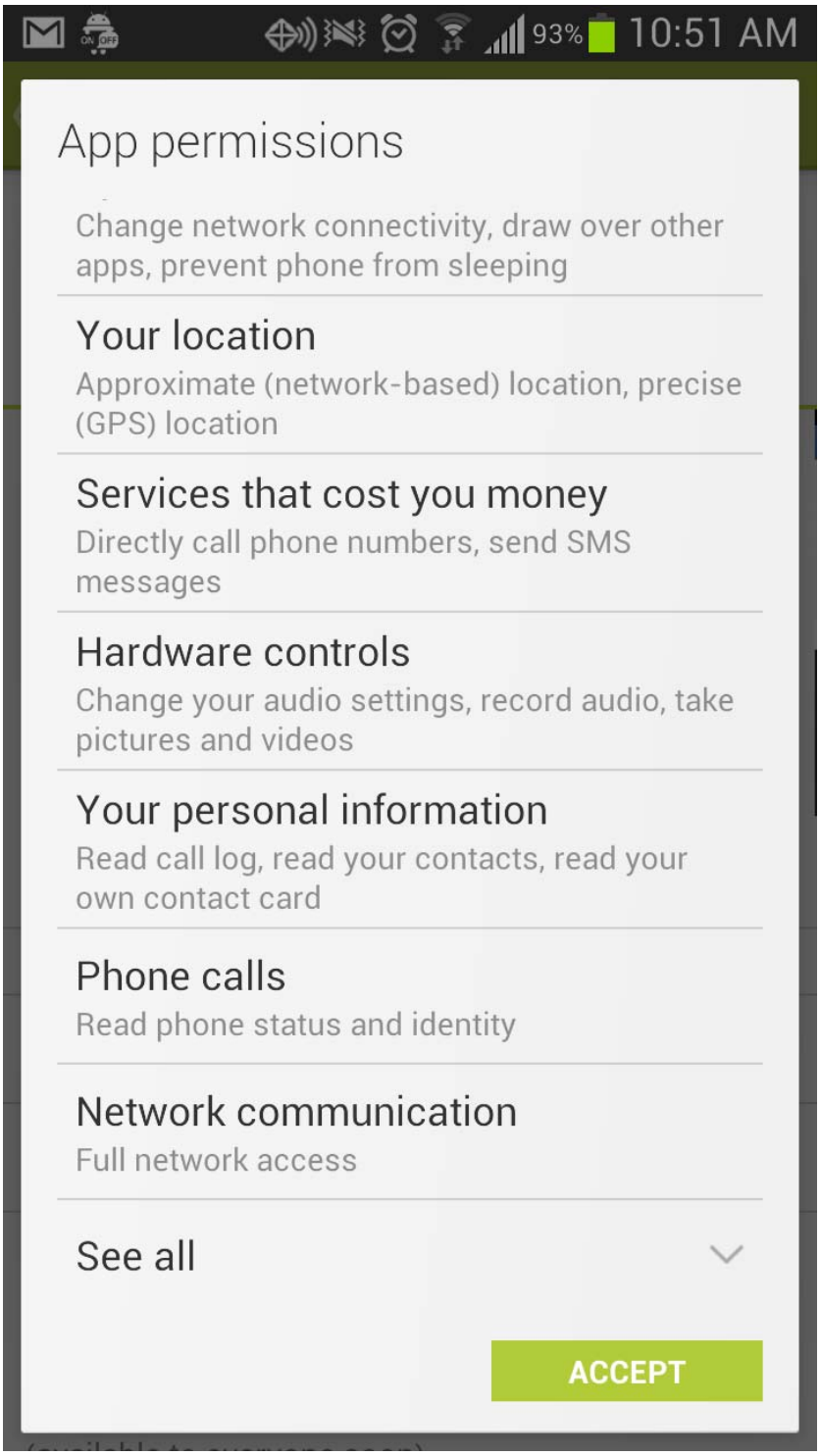
fall into the third category, which pose the greatest privacy risks, should be displayed on the first screen of the mobile device. The other two categories should be displayed on subsequent screens.

This change would be a good step towards make the permissions more useful for users. The next recommendation is to change the "see all" link in the current structure.

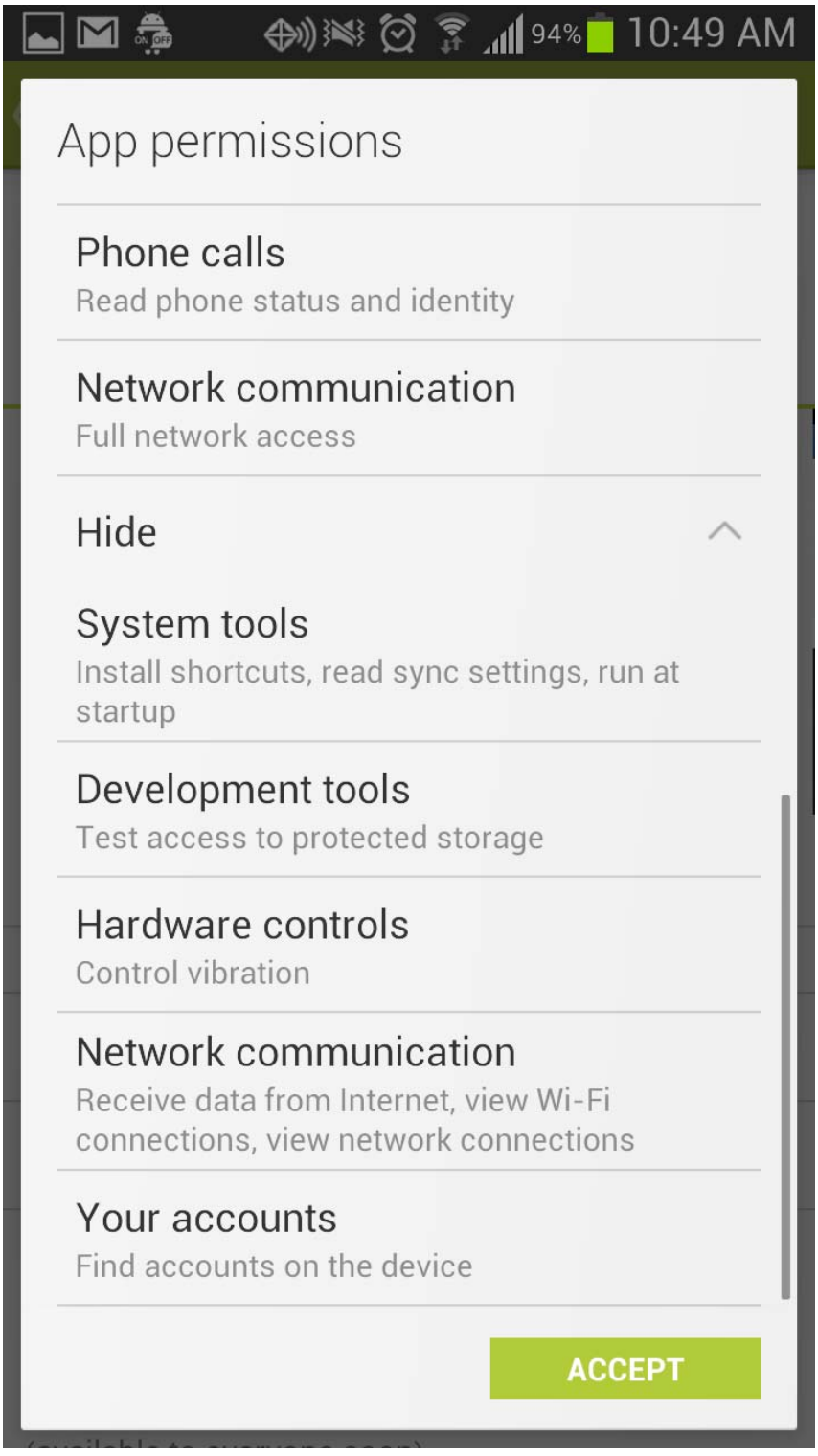
In the current display of permissions, the "see all" link expands the permission list. Presumably this link is there to free up screen space on small mobile devices, however this study found that there does not seem to be a reason for why some permissions appear above this link and some appear below.

In most cases this link is used when there are several permissions, but there is no clear reason for when an app developer should use the link. For example in the Dictionary.com Ad Free app the "see all" link is used when there are only three permissions (all of which could be read on even the smallest screen), in the case of Facebook Messenger there are 25 permissions and "show more" is also used, after the first 13 permissions. It is also unclear why certain permissions appear above the "see all" link and why some do not.

Permissions Above the “See All” Link in the Facebook Messenger App



Permissions Below the “See All” Link (Abridged)



The result of this system is that larger categories in which Google currently organizes permissions (discussed above) can show up both above *and* below the "see all" link with different permissions appearing under each larger category.

In the new categories suggested by this study permissions that fall under the third category would appear first on a single screen. At the top of the permission list there would have to be some language telling the user that the permissions they are seeing all interact with their PII in some way and are being displayed first.

This may not alleviate the issue of small screen space entirely.[28] In the sample of apps studied the majority only used between one and six of the permission that are in the third category (a low enough number that they could all be displayed on most mobile screens). However, there were some apps that used over 10 permissions that fall in the third category (most likely too many to be displayed on a single first screen.)

In these cases the user would have be told to "scroll" to see the rest of the permissions that interact with their PII. Ideally there would not be a need for a second screen and scrolling could be used in the rare cases where an app uses so many permissions in the third category that they can't be displayed in one list.

A second (and third if necessary) screen would be where the other two categories are housed: "Click here to see permissions this app is asking for that do not interact with your personal information." This would tell users who are interested that they can see the rest of the permissions if they wish.

[28] The "show all" link appears as "see more" in the mobile version of the Google Play Store, but the functionality is the same.

The next recommendation is more complex and requires a look into outside research efforts. The language of the current permissions (both the titles and definitions) is opaque at best and while reorganizing the current permission policies is a good first step making the language more useful to users is the next.

Three Key Phrases in Android Permissions

The following section will outline issues with the current language of permission policies and suggest some ways to improve the language. Regulators have had some experience in reworking language to make it more useful for users in the form of financial disclosures. The goal of reworking financial disclosures was to make short form disclosures effective at conveying the information that customers needed to know about their credit cards and other financial agreements. This study will draw on some of the research used for that process to make suggestions about how permissions could be rewritten.

The three phrases mentioned above “Not for user by normal apps,” “Should never be needed for normal apps,” and “Malicious apps….,” are good examples of phrases that are vague and make the permission itself not useful for users.

The first phrase is “Not for use by normal apps.” It is problematic because of the word “normal” and because it implies that while some apps could use it, most should not. There is no way for a user to discern why a specific permission would include this language and if the permission should be of concern.

The second is a similar phrase that may be more problematic, “Should never be needed for normal apps.” This phrase appears in six permissions and is even more problematic because of the strength of the language. This phrase again has the problem of using the word “normal” without any insight into what a “normal” app is, but this phrase goes further to use the word “never.” It is odd that a permission would use the word “never” because it implies that what the permission is asking for something so out of the ordinary that it needs pointing out.

Another problem is that the six permissions that use this language (Should never be needed for normal apps) do not appear to have any relationship to one another and do not appear to have a reason why they specifically have this language. For example, one of the permissions that uses this language is “Change Screen Orientation.” This permission states that: “Allows the app to change the rotation of the screen at any time. *Should never be needed for normal apps.*” (emphasis added)

If this permission did not include this phrase it would clearly be put into the first category of permissions that do not collect any information at all, but because it does include this phrase it was put in the third category. It is the vagueness, and apparent warning, that made it necessary to put these permissions in the third category.

The third term is, “malicious app.” In each case “malicious app” appears in a different context. In the 15 permissions that include this term each uses in the context of “malicious apps could...” with the rest of the statement referring to different activity depending on the permission.

For example the permission “Receive Data From Internet” states: “Allows apps to accept cloud to device messages sent by the app's service. Using this service will incur data usage. *Malicious apps could cause*

*excess data usage." (*emphasis added) In another case the permission "Directly Install Apps" states: "Allows the app to install new or updated Android packages. *Malicious apps may use this to add new apps with arbitrarily powerful permissions."*(emphasis added)

In the first case if the permission "Receive Data From Internet" did not include the term "malicious app" it would have been put into second category because while it interacts with information it does not appear to interact with PII. On the other hand "Directly Install Apps" would have been put in the third category regardless because "…add new apps with arbitrarily powerful permission" appears to allow an app with this permission to install apps on the device *without the user agreeing to the new app's permissions*. So while it does not itself access PII, it could theoretically allow an app to be installed that does access PII without the user's knowledge.

In both cases the language implies that theoretically an app (a "malicious app") could use the permission to inflict harm on the user. The question is how would a user know if an app was using the permission maliciously or not?

These phrases are examples of how vague language can be problematic for these permissions. In the case of these three phrases the recommendation of this paper is that they should not be used at all. They single out certain permission (and by extension certain apps) for no apparent reason. It is not useful to user's to know an app is potentially dangerous without saying why one app is and other apps are not.

The next issue is that there are several cases where permissions overlap to such an extent it is unclear why the user is not presented with a single permission.

Overlapping Permissions

One overarching issue of the current permission policies is the sheer volume of permissions. Another way to simplify the permission list is to combine some permissions into one. One common theme across several permissions is the difference between the terms “read”, “write”, “edit,” “send,” and “modify” in the current permission language.

There are several sets of permissions that interact with a single function of a mobile device, but do so in slightly different ways. One example of this is the SMS (text messaging) function of the phone. Currently there are three separate permissions that involve SMS messages: “Edit Your Text Messages,” “Receive Your Text Messages,” and “Read Your Text Messages.” Generally it is not necessary to break out a single function into these component parts, permissions structured this way could be condensed into one permission statement.

To complicate matters further the “receive” function is split into an additional three permissions that separate the kind of message into SMS messages (text messages), MMS Messages (Multi-Media Messages, or text messages with an attached photo, video, or audio), and WAP Messages[29].

Another confusing aspect of these permissions is that while the “receive” function is broken out by the type of message (SMS, MSS, or WAP), the “read” permission is not. That permission is entitled “Read Your Text Messages (SMS or MMS)” and states:

“Allows the app to read SMS messages stored on your tablet or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality. Allows the app to read SMS messages stored on your phone or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality.:

[29] WAP messages are another kind of SMS message that is “pushed” to mobile devices and displayed as an alert that connects directly to a website, emergency text messages many cities have are WAP Messages as to dangerous weather alerts that many weather apps offer.

So on the one hand the “receive” function was deemed important enough to break out by message type, but the “read” function was not. In addition the read function title says “SMS and MMS.” In the actual language only the term SMS is used, MMS is never mentioned.

The result is that one function, text messaging, is governed by five permissions. There is an argument to be made that some users may want to know this, but given small screen space it is necessary to prioritize this information. These permissions could be distilled into one statement: “This app can interact with your text messages by reading, sending, or editing your text messages. Click here for details.” With the “Click Here” going to the list of the five permissions for those users that want the full details (in addition if the five permissions are broken out “read your text messages” should also be broken into two permissions to be consistent with the “receive” permissions.)

Another example of permissions that could be consolidated are the permissions related to location information. There are four permissions that govern location information: “Approximate Location (Network-Based),” “Precise Location (GPS and Network Based),” “Mock Location Sources for Testing,” and “Access Extra Location Provider Commands.”

The important piece of information that should be conveyed to the user is that their location is being determined by an app with any of these permissions, not *how* that information is being determined. These four permission could be combined into one statement about location services: “This app can determine your location using the Global Positioning System (GPS), cell towers, or Wi-FI Networks. Click here for detailed information.” The “detailed information” link would then go to another screen that explains all the different methods for determining a user’s location.

The third and fourth location permissions are interesting examples of permissions that should have a *more* detailed explanation. The permission “Mock Location Sources for Testing” says: “Create mock location sources for testing or install a new location provider. This allows the app to override the location and/or status returned by other location sources such as GPS or location providers.” Presumably this allows an app to use some other way to determine a user’s location other than the GPS, cell towers, or Wi-Fi networks. The language does not specify what this other method could be. If an app needed this permission, it should specify *exactly* what kind of other information it is using to determine a user’s location.

The permission “Access Extra Location Provider Commands” states: “Allows the app to access extra location provider commands. This may allow the app to to interfere with the operation of the GPS or other location sources.” (the “to” and “to” that appear in language above is a not a typo of this paper, that is the language as it appears in the Google Play Store and another issue discussed in the sections below).

This is an even clearer example of a permission that does not have straightforward language. There is no definition of what “extra location provider commands” is. The phrase, “This may allow the app to interfere with the operation of the GPS or other location sources” implies this permission could allow an app to prevent other apps from using the GPS or other location functions. If that is true this permission needs to explain exactly what this permission does and how it could allow an app to interfere with other functions of the device.

There are several other permissions that follow the same pattern and could be condensed into one permission statement. The detailed information available in the separate permissions would still be available to users, it would just not appear on the initial screen:

- “View Wi-Fi Connections” and “View Network Connections”
- “Read Battery Statistics” and “Modify Battery Statistics”
- “Read Sync Settings” and “Ready Sync Statistics”
- “Modify Gmail” and “Send Gmail”
- “Write Web Bookmarks and History” and “Read Your Web Bookmarks and History”
- “Read Your Own Contact Card” and “Modify Your Own Contact Card”
- “Read Your social Stream” and “Write Your Social Stream”

This recommendation is not outside the realm of the current permission structure. The permission “Add or Modify Calendar Events and Send Email to Guests Without Owners’ Knowledge” states:

“Allows the app to add, remove, change events that you can modify on your tablet, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge. Allows the app to add, remove, change events that you can modify on your phone, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge.”

This permission effectively combines the idea of “read,” “write,” “edit,” “send,” and “modify” into a single permission. While this permission is not a good example of the clearest language possible, it does combine what could be several different permissions into one.

The final recommendation on language is a more general one and involves rethinking the language of all of the permission by general rules on how to write for a general audience.

How to Write Permissions Users Can Understand

For this recommendation there is a body of research available to draw on and existing FTC guidelines that could be adapted easily for mobile permission policies. A key document provided by the FTC that could

be used as a guide is “Getting Noticed: Writing Effective Financial Privacy Notices.” These guidelines are broken up into several sections to help businesses write their own financial privacy notices, but two sections in particular is useful for understanding mobile permissions.

The FTC uses several short tips on how to write clear language in this document that could easily apply to mobile app permissions[30]:

- concise - simple and straightforward, not "jargoned up" or "dumbed down."
- direct - using the word "you" to engage your reader.
- affirmative - telling customers what is, rather than what isn't; what they should do, rather than what they shouldn't do.
- active rather than passive.
- respectful.
- If you must use technical terms, you can still help your reader understand them.
- define the term in a text box close to its use.
- include a glossary in the notice.
- on your website, hyperlink the term to a definition or use a simpler term or phrase in the text and link to the technical term.
- Highlight your company's contact information clearly and conspicuously.

If most of these points were applied to Android permissions they would greatly improve on the current language (other than the one specifically geared towards websites.) The idea of being “concise” is a useful one for Android permissions, but as it stands most of the permissions are concise in the sense that

[30] Federal Trade Commission, *Getting Noticed: Writing Effective Financial Privacy Notices*, October, 2002.

they are only a few sentences at most. Current permissions suffer more often from being “jargoned up” in the words of the FTC and include too many technical terms with no definitions.

Defining technical terms in these permissions is a key point that would make them far more useful. The idea above of including a Glossary is a good one; however, in the case of permissions it would be more useful to define technical terms as they are used. The goal should be not forcing the user to open a new window in order to understand a set of permissions.

The three phrase discussed above are also good examples of how current permissions are not “affirmative” as the FTC puts it. The example of “not for use by normal apps” tells the user that this permission should probably not used, rather than telling the user that it should not be used for normal apps *because of X reason*.

Another minor issue is that there is no consistency across permissions in the use of the word “tablet” and “phone”. Some permissions use both, some only use one. The use of the word “device” across permissions would be an easy fix to this problem.

The FTC goes on to make other suggestions of how best to design financial privacy statements, and one in particular would be useful for Android App permissions.

Highlighting Services That Cost Money

Most of the design suggestions made by the FTC are very specific and minor. It would be up to Google to decide on (the font or the amount of white space for example) and the current set of design choices of the Android app permissions would suffice. There is one suggestion worth noting: “colors for interest.”

A useful category for permissions currently provided in the Google Play Store is “Services That Could Cost You Money.” Currently permissions that fall under this category are ones that could theoretically cost users money directly by adding costs to their cell phone bill. There are two that fell under this category: “directly call phone numbers” and “send SMS messages.” Because both these activities are billable by cell phone companies an app that accesses these services could theoretically cost the user money.

Under the new set of categories both “Send SMS Messages” and “Directly Call Phone Numbers” fall under the third category of permissions that do collect PII because both use one of the key phrases (malicious apps…). While these two would no longer be under the category of “services that cost you money” it is still important to tell users this fact. There is one other permission “Receive Data From Internet” that actually implies, but does not expressly say, it could cost users money: “Allows apps to accept cloud to device messages sent by the app's service. Using this service will incur data usage. Malicious apps could cause excess data usage.”

This permission should also be highlighted as one that could cost user’s money because most cell phone plans do not include unlimited data (of the major carriers only Sprint and T-Mobile still have plans that include unlimited data). In cases where users do not have unlimited data if they go over a certain amount of data a month they are charged extra; therefore an app with this permission could cost user’s money if it causes them to go over their monthly data limit. One way to do this would be to highlight these three permissions with the color green, to connote that they are permissions that cost money. Another way would be to use a dollar symbol (or both)

The above recommendations are suggestions on how to modify the current permission policies to make them more useful for users. The next recommendation is to add information to the permissions about what is being done with the information being collected. Currently permissions only tell the user that information is being collected.

Notifying Users Abut Information Use

None of the permission policies say what the app (or company) will do with the information once it is collected. This would be an important piece of any redesign of permission policies in the Android ecosystem.

This point is an important one and one being discussed at the NTIA multistakeholder meetings as a piece of how to reform short form notices. There are three key steps to notifying users of this information. The first is to tell users what information is being collected (already covered by most permissions). The second is why the app developer collects that information (what the app developer does with the information, for example is the information used to server ads?). And the third, if the developer shares the information with third parties the user must be told who those third parties are and how their information is used.

By limiting this requirement only to apps that fall in the third category of this study this process could be simplified. Not every permission requires that the user is given this kind of detailed information. An issue still being dealt with at the NTIA is that while it is clear user's should be notified of how their information is being used, that notification is still taking place on a small screen and should be useful for user's.

While some recommendations above would alleviate the space problem, adding this information to current permissions would expand the amount of text needed. More study needs to be put into how to connect current permissions regarding information collection, to how those permissions relate to disclosures of how that information is used.

As they currently stand, and even if the above recommendations were implemented, permissions in the Google Play Store would still only be a method for *notifying* users. The next step would be giving user's a choice.

Opt-In vs. Opt-Out

In the framework of "opt-in" vs. "opt-out" the permissions system has already complicated the decision making process. The initial choice presented to users is to accept all of the permission policies in order to use the app, or reject the permissions policies and not get to use the app. In a sense the way the system is set up it is an all or nothing opt-in decision. If users want to use the app at all they must opt-in to all of the permissions the app is requesting and therefore agree to transfer any information the app asks for. The problem is that it is an "opt-all-in" choice. Users must agree to everything to use the product they are downloading (and in some cases paying for).

Once the app is downloaded and users begin to use it they cannot then opt out of any of those permissions without uninstalling the app entirely, except in some cases (see the location services example below). In certain cases users can agree to the permission policies and then turn off some of the features once the app is launched. A common example of permissions that user's often do have control over after they have downloaded the app are the location services of many mobile devices. Some apps allow the user to turn

these permissions on or off. For example, the Twitter app for Android asks the user to allow (or not) the app to access the user's location using the GPS function when the apps is first launched.

In other cases (Foursqure for example), the GPS setting can be turned off in the settings menu after the app is launched, but the users is never prompted to turn it off and the GPS location is on by default. There are few permissions that are like this, the vast majority of permissions cannot be turned off once the user has agreed to the entire permission list.

This final option of giving user's choice is also one of deciding who iss responsible for implementing that choice, the platform (in this case Google) or the app developer.

The Role of the Platform Provider

It is a clear choice by Google to leave this decision up to the app developer's at present. While this system can work, one recommendation is to require apps to prompt the user upon first launch if the user has control over any features in the app. Clearly Twitter made the decision on its own to provide users with a notice and choice when the GPS is accesed, but other apps do not.

The next step in this process would be to move these just-in-time notifications to the OS level. Putting the responsibility on Google to tell user's when an app is interacting with some kind of user information (as opposed to it being the app developer's responsibility as it stands now). This step would be outside the realm of Google culture. This kind of top-down control is not in Google's nature. However, in this case Google is in a unique position to force app in the Android ecosystem to give user's a more clear choice to certain off certain functions.

This would be a fundamental change in the purpose of permissions as they are currently framed. By showing users a list of permissions, and then presenting users with a choice to turn certain permissions on or off *before* they download the app would give users more control over their information, while allowing them to use more apps without having to outright reject certain apps. One concern voice by both app developers and platforms is that giving user's this kind of choice leads them to turn off functions of devices that would hurt the economic model of some apps.

To alleviate this issue one suggestion is to frame the notification by telling user's they have a choice to turn off certain functions, but that will lead to the user not getting the full experience of the app and to the app not being able to pay for its continued existence (this would mostly apply to apps that are free and ad based).

This connection between notifying users of how an app is collecting and using information and how that app is using that information to either make money or for some other purpose like research is a subtle one beyond the scope of this paper, but certainly worth further research. Could permissions be a way to better inform users of the connection between their data and the app economy or research in general? If users knew that their data was being collected, but for a positive purpose, it might cause users to think twice before simply turning of features they have the option to.

A related question to this recommendation that cannot be answered within the scope of this paper is one worth asking: How many users actually reject an app because of its permission list as it stands currently?

Conclusion

This study has shown that the current permissions in the Google Play Store do not satisfactorily inform users of the information they are giving to apps. The next step in the process is to implement the above recommendations in a way that would help users understand what information they are giving to app developers and what is done with that information.

The frame for this entire study is privacy and user information. Other studies will be needed to address the security concerns created by mobile apps. In addition this same method could be used to look at other appstores like the iTunes.

Permissions are the first, and usually only, notice users get about apps they put on their Android mobile device. The permissions should tell users what information the app is collecting and what the app developer does with that information. Currently app permissions in the Google Play Store do not adequately inform uses of the information being collected about them.

Fixing this issue is not only the interest of the user, but in Google's interest as well. By making permissions more useful for users malicious or harmful apps would be brought to the forefront more quickly as users see apps that are asking for odd permissions. This would make for a more stable app ecosystem that protects users information while allowing the ecosystem to also benefit app developers.

Appendix A- Full List of Permissions

The Permissions below appear in the three categories suggested in Chapter 5 of this study. The number in the parenthesis next to each title represents the number of apps in the sample of 1,300 that asked for the permission. The title and definitional language is taken directly from the Google Play Store as of January 2013.

Permissions that do not collect or Access PII

CHANGE YOUR AUDIO SETTINGS (74)
Allows the app to modify global audio settings such as volume and which speaker is used for output.

CONTROL FLASHLIGHT (46)
Allows the app to control the flashlight.

CONTROL NEAR FIELD COMMUNICATION (37)
Allows the app to communicate with Near Field Communication (NFC) tags, cards, and readers.

CONTROL VIBRATION (388)
Allows the app to control the vibrator.

PREVENT TABLET FROM SLEEPING PREVENT PHONE FROM SLEEPING (474)
Allows the app to prevent the tablet from going to sleep. Allows the app to prevent the phone from going to sleep.

REORDER RUNNING APPS (6)
Allows the app to move tasks to the foreground and background. The app may do this without your input.

CLOSE OTHER APPS (23)
Allows the app to end background processes of other apps. This may cause other apps to stop running.

RUN AT STARTUP (275)
Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the tablet and allow the app to slow down the overall tablet by always running. Allows the app to have itself started as soon as the system has finished booting. This can make it take longer to start the phone and allow the app to slow down the overall phone by always running.

SEND STICKY BROADCAST (56)
Allows the app to send sticky broadcasts, which remain after the broadcast ends. Excessive use may make the tablet slow or unstable by causing it to use too much memory. Allows the app to send sticky broadcasts, which remain after the broadcast ends. Excessive use may make the phone slow or unstable by causing it to use too much memory.

DRAW OVER OTHER APPS (31)
Allows the app to draw on top of other applications or parts of the user interface. They may interfere with your use of the interface in any application, or change what you think you are seeing in other applications.

ACCESS USB STORAGE FILESYSTEM ACCESS SD CARD FILESYSTEM (19)
Allows the app to mount and unmount filesystems for removable storage.

CHANGE SYSTEM DISPLAY SETTINGS (16)
Allows the app to change the current configuration, such as the locale or overall font size.

MAKE APP ALWAYS RUN (7)
Allows the app to make parts of itself persistent in memory. This can limit memory available to other apps slowing down the tablet. Allows the app to make parts of itself persistent in memory. This can limit memory available to other apps slowing down the phone.

SET TIME ZONE (2)
Allows the app to change the tablet's time zone. Allows the app to change the phone's time zone.

INSTALL DRM CONTENT (5)
Allows app to install DRM-protected content.

TEST ACCESS TO PROTECTED STORAGE TEST ACCESS TO PROTECTED STORAGE (889)
Allows the app to test a permission for USB storage that will be available on future devices. Allows the app to test a permission for the SD card that will be available on future devices.

POWER TABLET ON OR OFF POWER PHONE ON OR OFF (10)
Allows the app to turn the tablet on or off. Allows the app to turn the phone on or off.

DISABLE OR MODIFY STATUS BAR (11)
Allows the app to disable the status bar or add and remove system icons.

FORCE TABLET REBOOT FORCE PHONE REBOOT (1)
Allows the app to force the tablet to reboot. Allows the app to force the phone to reboot.

CHANGE WIMAX STATE (1)
Allows the app to connect the tablet to and disconnect the tablet from WiMAX networks. Allows the app to connect the phone to and disconnect the phone from WiMAX networks.

TAKE PICTURES AND VIDEOS
Allows the app to take pictures and videos with the camera. This permission allows the app to use the camera at any time without your confirmation.

PAIR WITH BLUETOOTH DEVICES
Allows the app to view the configuration of Bluetooth on the tablet, and to make and accept connections with paired devices. Allows the app to view the configuration of the Bluetooth on the phone, and to make and accept connections with paired devices.

CONNECT AND DISCONNECT FROM WI-FI
Allows the app to connect to and disconnect from Wi-Fi access points and to make changes to device configuration for Wi-Fi networks.

DISABLE YOUR SCREEN LOCK
Allows the app to disable the keylock and any associated password security. For example, the phone disables the keylock when receiving an incoming phone call, then re-enables the keylock when the call is finished.

TOGGLE SYNC ON AND OFF
Allows an app to modify the sync settings for an account. For example, this can be used to enable sync of the People app with an account.

ACCESS BLUETOOTH SETTINGS
Allows the app to configure the local Bluetooth tablet, and to discover and pair with remote devices. Allows the app to configure the local Bluetooth phone, and to discover and pair with remote devices.

CHANGE NETWORK CONNECTIVITY
Allows the app to change the state of network connectivity.

ALLOW WI-FI MULTICAST RECEPTION

Allows the app to receive packets sent to all devices on a Wi-Fi network using multicast addresses, not just your tablet. It uses more power than the non-multicast mode. Allows the app to receive packets sent to all devices on a Wi-Fi network using multicast addresses, not just your phone. It uses more power than the non-multicast mode.

SET WALLPAPER
Allows the app to set the system wallpaper.

MODIFY SYSTEM SETTINGS
Allows the app to modify the system's settings data. Malicious apps may corrupt your system's configuration.

EXPAND/COLLAPSE STATUS BAR
Allows the app to expand or collapse the status bar.

MODIFY PHONE STATE
Allows the app to control the phone features of the device. An app with this permission can switch networks, turn the phone radio on and off and the like without ever notifying you.

ADJUST YOUR WALLPAPER SIZE
Allows the app to set the system wallpaper size hints.

SET AN ALARM
Allows the app to set an alarm in an installed alarm clock app. Some alarm clock apps may not implement this feature.

GOOGLE MAIL
Allows apps to sign in to Google mail services using the account(s) stored on this Android device.

ERASE USB STORAGE ERASE SD CARD
Allows the app to format removable storage.

Permissions that collect or access user information that is device related, but not PII

DELETE ALL APP CACHE DATA (3)
Allows the app to free tablet storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re-retrieve their data. Allows the app to free phone storage by deleting files in the cache directories of other applications. This may cause other applications to start up more slowly as they need to re-retrieve their data.

ADD WORDS TO USER-DEFINED DICTIONARY (10)
Allows the app to write new words into the user dictionary.

READ GOOGLE SERVICE CONFIGURATION (28)
Allows this app to read Google service configuration data.

RETRIEVE RUNNING APPS (118)
Allows the app to retrieve information about currently and recently running tasks. This may allow the app to discover information about which applications are used on the device.

READ SYNC SETTINGS (49)
Allows the app to read the sync settings for an account. For example, this can determine whether the People app is synced with an account.

READ SYNC STATISTICS (29)
Allows an app to read the sync stats for an account, including the history of sync events and how much data is synced.

MEASURE APP STORAGE SPACE (3)
Allows the app to retrieve its code, data, and cache sizes

VIEW WI-FI CONNECTIONS (410)
Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and name of connected Wi-Fi devices.

VIEW NETWORK CONNECTIONS (918)
Allows the app to view information about network connections such as which networks exist and are connected.

READ BATTERY STATISTICS (12)
Allows an application to read the current low-level battery use data. May allow the application to find out detailed information about which apps you use.

ADD VOICEMAIL (2)
Allows the app to add messages to your voicemail inbox.

PREVENT APP SWITCHES (621)
Prevents the user from switching to another app.

CONNECT AND DISCONNECT FROM WIMAX (64)
Allows the app to determine whether WiMAX is enabled and information about any WiMAX networks that are connected.

USE ACCOUNTS ON THE DEVICE (153)
Allows the app to request authentication tokens.

CREATE ACCOUNTS AND SET PASSWORDS (116)
Allows the app to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords.

ADD OR REMOVE ACCOUNTS (154)
Allows the app to perform operations like adding and removing accounts, and deleting their password.

GOOGLE VOICE (1)
Allows apps to sign in to Google Voice using the account(s) stored on this Android device.

GOOGLE FINANCE (1)
Allows apps to sign in to Google Finance using the account(s) stored on this Android device.

GOOGLE DOCS (3)
Allows apps to sign in to Google Docs using the account(s) stored on this Android device.

GOOGLE SPREADSHEETS (3)
Allows apps to sign in to Google Spreadsheets using the account(s) stored on this Android device.

GOOGLE MAPS (3)
Allows apps to sign in to Google Maps using the account(s) stored on this Android device.

YOUTUBE (2)
Allows apps to sign in to YouTube using the account(s) stored on this Android device.

ACCESS OTHER GOOGLE SERVICES (3)
Allows apps to sign in to unspecified Google services using the account(s) stored on this Android device.

ACCESS ALL GOOGLE SERVICES (1)
Allows apps to sign in to ALL Google services using the account(s) stored on this Android device.

MAKE/RECEIVE INTERNET CALLS (2)
Allows the app to use the SIP service to make/receive Internet calls

MODIFY GMAIL (2)
Allows the app to modify your Gmail, including sending and deleting mail.

SEND GMAIL (1)
Allows the app to send Gmail messages without opening the Gmail app

FULL NETWORK ACCESS (1,085)
Allows the app to create network sockets and use custom network protocols. The browser and other applications provide means to send data to the internet, so this permission is not required to send data to the internet.

DOWNLOAD FILES WITHOUT NOTIFICATION (3)
Allows the app to download files through the download manager without any notification being shown to the

REROUTE OUTGOING CALLS (10)
Allows the app to process outgoing calls and change the number to be dialed. This permission allows the app to monitor, redirect, or prevent outgoing calls.

MODIFY OR DELETE THE CONTENTS OF YOUR USB STORAGE MODIFY OR DELETE THE CONTENTS OF YOUR SD CARD (884)
Allows the app to write to the USB storage. Allows the app to write to the SD card.

ACT AS THE ACCOUNTMANAGERSERVICE (3)
Allows the app to make calls to AccountAuthenticators.

VIEW CONFIGURED ACCOUNTS (18)
Allows apps to see the usernames (email addresses) of the Google account(s) you have configured.

READ GOOGLE SERVICE CONFIGURATION (28)
Allows this app to read Google service configuration data.

MODIFY/DELETE INTERNAL MEDIA STORAGE CONTENTS (5)
Allows the app to modify the contents of the internal media storage.

Permissions that collect PII

CONTACTS DATA IN GOOGLE ACCOUNTS (786)
Allows apps to access the contacts and profile information of account(s) stored on this Android device.

APPROXIMATE LOCATION (NETWORK-BASED) (368)
Allows the app to get your approximate location. This location is derived by location services using network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine approximately where you are.

PRECISE LOCATION (GPS AND NETWORK-BASED) (369)
Allows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi. These location services must be turned on and available to your device for the app to use them. Apps may use this to determine where you are, and may consume additional battery power.

MOCK LOCATION SOURCES FOR TESTING (24)
Create mock location sources for testing or install a new location provider. This allows the app to override the location and/or status returned by other location sources such as GPS or location providers.

ACCESS EXTRA LOCATION PROVIDER COMMANDS (26)
Allows the app to access extra location provider commands. This may allow the app to to interfere with the operation of the GPS or other location sources.

READ YOUR TEXT MESSAGES (SMS OR MMS) (57)
Allows the app to read SMS messages stored on your tablet or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality. Allows the app to read SMS messages stored on

your phone or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality.

RECEIVE TEXT MESSAGES (SMS) (47)
Allows the app to receive and process SMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.

RECEIVE TEXT MESSAGES (MMS) (20)
Allows the app to receive and process MMS messages. This means the app could monitor or delete messages sent to your device without showing them to you.

RECEIVE TEXT MESSAGES (WAP) (3)
Allows the app to receive and process WAP messages. This permission includes the ability to monitor or delete messages sent to you without showing them to you.

READ INSTANT MESSAGES (4)
Allows apps to read data from the Google Talk content provider.

READ GMAIL (6)
Allows the app to read your Gmail.

READ SENSITIVE LOG DATA (12)
Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the tablet, potentially including personal or private information. Allows the app to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.

ADD OR MODIFY CALENDAR EVENTS AND SEND EMAIL TO GUESTS WITHOUT OWNERS' KNOWLEDGE (38)
Allows the app to add, remove, change events that you can modify on your tablet, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge. Allows the app to add, remove, change events that you can modify on your phone, including those of friends or co-workers. This may allow the app to send messages that appear to come from calendar owners, or modify events without the owners' knowledge.

WRITE WEB BOOKMARKS AND HISTORY (18)

Allows the app to modify the Browser's history or bookmarks stored on your tablet. This may allow the app to erase or modify Browser data. Note: this permission may note be enforced by third-party browsers or other applications with web browsing capabilities. Allows the app to modify the Browser's history or bookmarks stored on your phone. This may allow the app to erase or modify Browser data. Note: this permission may note be enforced by third-party browsers or other applications with web browsing capabilities.

READ YOUR WEB BOOKMARKS AND HISTORY (26)
Allows the app to read the history of all URLs that the Browser has visited, and all of the Browser's bookmarks. Note: this permission may not be enforced by third-party browsers or other applications with web browsing capabilities.

RETRIEVE SYSTEM INTERNAL STATE (3)
Allows the app to retrieve internal state of the system. Malicious apps may retrieve a wide variety of private and secure information that they should never normally need.

FIND ACCOUNTS ON THE DEVICE (219)
Allows the app to get the list of accounts known by the tablet. This may include any accounts created by applications you have installed. Allows the app to get the list of accounts known by the phone. This may include any accounts created by applications you have installed.

READ YOUR OWN CONTACT CARD (9)
Allows the app to read personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.

MODIFY YOUR OWN CONTACT CARD (1)
Allows the app to change or add to personal profile information stored on your device, such as your name and contact information. This means the app can identify you and may send your profile information to others.

READ CALL LOG (143)
Allows the app to read your tablet's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge. Allows the app to read your phone's call log, including data about incoming and outgoing calls. This permission allows apps to save your call log data, and malicious apps may share call log data without your knowledge.

READ YOUR SOCIAL STREAM (4)

Allows the app to access and sync social updates from you and your friends. Be careful when sharing information -- this allows the app to read communications between you and your friends on social networks, regardless of confidentiality. Note: this permission may not be enforced on all social networks.

WRITE TO YOUR SOCIAL STREAM (4)
Allows the app to display social updates from your friends. Be careful when sharing information -- this allows the app to produce messages that may appear to come from a friend. Note: this permission may not be enforced on all social networks.

ACCESS GOOGLE PHOTOS DATA (1)
Allows the app to read photo data from Google Photos, including account name, file names, photo IDs, locations where photo were taken, etc.

YOUTUBE USERNAMES (2)
Allows apps to see the YouTube username(s) associated with the Google account(s) stored on this Android device.

READ TERMS YOU ADDED TO THE DICTIONARY (17)
Allows the app to read all words, names and phrases that the user may have stored in the user dictionary.

READ PHONE STATUS AND IDENTITY (527)
Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.

READ SUBSCRIBED FEEDS
Allows the app to get details about the currently synced feeds.

MODIFY YOUR CONTACTS
Allows the app to modify the data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data. Allows the app to modify the data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific contacts. This permission allows apps to delete contact data.

READ CALENDAR EVENTS PLUS CONFIDENTIAL INFORMATION
Allows the app to read all calendar events stored on your tablet, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity.

Allows the app to read all calendar events stored on your phone, including those of friends or co-workers. This may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity.

ACCESS MAIL INFORMATION
Allows the app to access information about your mail.

These apps were included in the third category only because they used the phrases: "not for use by normal apps," "Should never be needed for normal apps," or "malicious app."

Not for use by normal apps:

DISPLAY UNAUTHORIZED WINDOWS (1)
Allows the app to create windows that are intended to be used by the internal system user interface. Not for use by normal apps.

MODIFY SECURE SYSTEM SETTINGS (14)
Allows the app to modify the system's secure settings data. Not for use by normal apps.

MODIFY BATTERY STATISTICS (4)
Allows the app to modify collected battery statistics. Not for use by normal apps

ACCESS CHECKIN PROPERTIES (1)
Allows the app read/write access to properties uploaded by the checkin service. Not for use by normal apps.

MODIFY THE GOOGLE SERVICES MAP (1)
Allows the app to modify the Google services map. Not for use by normal apps.

CHOOSE WIDGETS (5)
Allows the app to tell the system which widgets can be used by which app. An app with this permission can give access to personal data to other apps. Not for use by normal apps.

CONTROL LOCATION UPDATE NOTIFICATIONS
Allows the app to enable/disable location update notifications from the radio. Not for use by normal apps.

Should never be used by normal apps:

CHANGE SCREEN ORIENTATION (13)
Allows the app to change the rotation of the screen at any time. Should never be needed for normal apps.

BIND TO A WALLPAPER (3)
Allows the holder to bind to the top-level interface of a wallpaper. Should never be needed for normal apps.

BIND TO AN ACCESSIBILITY SERVICE (1)
Allows the holder to bind to the top-level interface of an accessibility service. Should never be needed for normal apps.

BIND TO AN INPUT METHOD (1)
Allows the holder to bind to the top-level interface of an input method. Should never be needed for normal apps.

Malicious Apps:

RECEIVE DATA FROM INTERNET (198)
Allows apps to accept cloud to device messages sent by the app's service. Using this service will incur data usage. Malicious apps could cause excess data usage.

DIRECTLY INSTALL APPS (245)
Allows the app to install new or updated Android packages. Malicious apps may use this to add new apps with arbitrarily powerful permissions.

DELETE APPS (1)
Allows the app to delete Android packages. Malicious apps may use this to delete important apps.

ENABLE OR DISABLE APP COMPONENTS (467)
Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important tablet capabilities. Care must be used with this permission, as it is possible to get app components into an unusable, inconsistent, or unstable state. Allows the app to change whether a component of another app is enabled or not. Malicious apps may use this to disable important phone capabilities. Care must be used with this permission, as it is possible to get app components into an unusable, inconsistent, or unstable state.

SEND SMS-RECEIVED BROADCAST (2)
Allows the app to broadcast a notification that an SMS message has been received. Malicious apps may use this to forge incoming SMS messages.

DIRECTLY CALL PHONE NUMBERS (105)
Allows the app to call phone numbers without your intervention. This may result in unexpected charges or calls. Note that this doesn't allow the app to call emergency numbers. Malicious apps may cost you money by making calls without your confirmation.

SEND SMS MESSAGES (50)
Allows the app to send SMS messages. This may result in unexpected charges. Malicious apps may cost you money by sending messages without your confirmation.

EDIT YOUR TEXT MESSAGES (SMS OR MMS) (35)
Allows the app to write to SMS messages stored on your tablet or SIM card. Malicious apps may delete your messages. Allows the app to write to SMS messages stored on your phone or SIM card. Malicious apps may delete your messages.

READ YOUR CONTACTS (163)
Allows the app to read data about your contacts stored on your tablet, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge. Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.

WRITE SUBSCRIBED FEEDS
Allows the app to modify your currently synced feeds. Malicious apps may change your synced feeds.

SET PREFERRED APPS
Allows the app to modify your preferred apps. Malicious apps may silently change the apps that are run, spoofing your existing apps to collect private data from you.

CHANGE/INTERCEPT NETWORK SETTINGS AND TRAFFIC
Allows the app to change network settings and to intercept and inspect all network traffic, for example to change the proxy and port of any APN. Malicious apps may monitor, redirect, or modify network packets without your knowledge.

DIRECTLY CALL ANY PHONE NUMBERS

Allows the app to call any phone number, including emergency numbers, without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services.

Appendix B- App List

The list below is the 1,300 apps included in the sample of this study, it is in alphabetical order.

[root] Mobile ODIN Pro	Action Launcher Pro	All By Myself
[root] Triangle Away	Adam US english voice	Allrecipes Dinner Spinner Pro
100 Doors 2013	Adobe AIR	Alphabet Car
100 Floors Official Cheats	Adobe Photoshop Express	AlpineReplay Ski & Snowboard
10bii FInancial Calculator	Adobe Photoshop Touch	AMA Supercross
12 steps of AA companion	Adobe Reader	Amazing Grocery List
2013 Happy New Year	Advanced Task Killer	Amazon Mobile
2300+ Funny Quotes	Advanced Task Killer Pro	Amazon Mobile (tablet)
2300+ Sex Jokes	ADW.Launcher	Amazon MP3
3D Digital Weather Clock	ADWL Launcher EX	American Airlines
3D Flip Clock & World Weather	AES Xpress	American Express US
40+ Binaurals AmbiScience	AfterFocus Pro	Amo Navi-X
4shared	AirSync by doubleTwist	Amtrak
90Droid Extreme Fitness	Airtight	Ancestry
A Comic Viewer	AirWX Aviation Weather	Android Music Player
A.I.type Keyboard Plus	AIVC (Alice)- Pro Version	Android UPdates, News & Apps
ABC for Kids All Alphabet Free	Akinator the Genie	AndroVid Pro Video Editor
aCar Car Managment, Mileage	Alarm Clock Plus (NoAds)	AndroZip File Manager
AccuWeather for Android	Alarm Clock Xtreme Free	Andy (Siri for Android)
Accuweather Platinum	Aldiko Book Reader Free	Angry Birds
AccuWeather Quick	Aldiko Book Reader Premium	Angry Birds Seasons
Act 1 Video Player	Alien Shapes FULL	Angry Birds Space Premium

Angry Birds Star Wars

Animated Weather Widget & Clock

Anime HD Wallpapers

aniPet Aquarium Live Wallpaper

anMoney PRO Finance

Anomaly

Antivirus Free

Any.DO To-do List & Task Manager

Anywhere Map Aviation GPS

Apex Launcher Pro

Apk Installer

Appy Gamer

Appy Gamer

Aquarium Free Live Wallpaper

Aquarium Live Wallpaper

Asphalt 7:Heat

Astrid Power Pack

Astro File Manager/Browser

ATI RN Mentor NCLEX Exam Prep

Audible for Android

AudioManager (no ads)

AudioManager Pro

Audobon Birds

AVG Mobile Antivirus Security

Aviary Effects: Classic

Aviary Effects: Grunge Pack

Aviary Effects: Nostalgia Pack

Aviary Effects: Tidal

Aviary Effects: Viewfinder

Aviary Frames: Original

Aviary Stickers: Animals

Aviary Stickers: Football

Aviary Stickers: Free

Aviary Stickers: Halloween

Aviary Stickers: Hats

Aviary Stickers: Helmets

Aviary Stickers: Holiday

Aviary Stickers: Mustaches

Aviary Stickers: Space

Baby Care track baby growth

Back Country Navigator Pro GPS

Backgrounds HD Wallpapers

Backup to Gmail

BaconReader for Reddit

BaconReader Premium for reddit

Badoo Meet New People

Badoo Meet New People

Balance My Checkbook

Bank Of America

Barcode Scanner

Barcode Scanner + (Plus)

Battery Boom

BauHaus FlipFont

BB&T Mobile Banking

BBC News

Beat the Traffic

Beat the Traffic Plus

Beautiful Widgets

Bedside (Night Clock)

BeerSmith 2 Lite

Best Buy

Best Wallpapers & Backgrounds

BestRoute Pro

BetterBattery Stats

BeWeather & Widgets Pro

Beyond Podcast Manager

Bible

Bible KJV

Bible Study
Bike Race Free
Bikini.com Lisa Morales supermodel party
Bills
BitTorrent Beta Torrent App
Blackboard Mobile
Bloons TD 5
Blue Skies Live Wallpaper
Box
Brightest Flashlight Free
Brightest LED Flashlight
Brithday Countdown Widget
BSPlayer
Bubble Worlds
Bubbles
BubbleUPnP License
Bump
Business Calender
Business Ringtones
BusyBox Pro
BW Animation Pack
c Pro Craigslist Client
Cabela's Recon Hunt
Caitlin Irish Voice
Calculations 4.0 Pro
CalenGoo
Call Blocker
Call of Duty Black Ops Zombies
Calorie Counter by Fat Secret
Calorie Counter My Fitness Pal
Calvin & Hobbes Search Engine
CamCard
Camcard Business Card Reader
Camera Fun Pro
Camera FV-5
Camera ICS+
Camera Zoom FX
Camera360 Ultimate
Camp and RV Campgrounds Plus
CamScanner Phone PDF Creator
Capital One Mobile
Car Dashboard Pro
Car Finder AR
Car Home Ultra
Car Locator
cardiotrainer pro
Cartoon Network Video
Cashbook Expense Tracker
Cashflow
Catch Notes
CATE CALL AND TEXT ERASER
CBS Sports
CBS Sports Mobile
Ceton Companion Media Center
Chase Mobile
Cheating Spouse? How To Catch
Checkbook Pro
Christmas HD
Chrome
Chrome Beta
Circle Nearby Friends Chat!
Citi Mobile (SM)
Citrix Receiver
Claorie Counter Pro
Classic Text to Speech
Clean Pack for FlipFont
Cleartune Chromatic Tuner
Cleverbot

ClockQ Premium
CLZ Comics
CM10.1 Touchwiz 5.0
CNN App for Android Phones
Coach's Eye
coffee finder pro
Color & Draw for Kids
Color & Draw for Kids HD
Coloring Book for Kids
ColorNote Notepad Notes To Do
Comic Reader Mobi
Comic Strip Maker
Comica
Comicat (comics reader)
ComicRack
Comics Mask Pro
coPilot Live Premium USA
Couch-to-5k
cPro craigslist client droid
Crackle Movies & TV
Craigslist for Android (CLapp)
Craigslist home/apt rental
Craigslist Mobile
Craigslist Mobile Pro
Critical Care ACLS Guide
cUltimate Craigslist Client
Cut the Rope
CVS/Pharmacy
Cyanide & Happiness
D7 Google Reader Pro (RSS)
Daily Ab Workout
Daily Ab Workout Free
Daily Audio Bible
Daily Bible
Daily Funny
Daily Horoscope Holidays
DailyHoroscope
DatPiff Mobile
Days left Widget Pro
DC Comics
Dead Space
Debt Payoff Planner
Deluxe Moon Moon Calender
Devil's Attorney
Diagnosaurus DDx
Dictionary -MW Premium
Dictionary Merriam Webster
Free
Dictionary.com Ad-Free
Dictionary.com Ad-Free
Diet & Food Tracker
Diptic
DIRECTV
DIRECTV Remote Pro
Discover Mobile
Documents to go 3.0
Dog Licker Live Wallpaper
DoggCatcher Podcasts
Dolphin Browser
Domino's Pizza USA
Doodle Jump
Doodle Text! Draw Photo SMS
Dora ABCs Vol 2: Rhyming Words
double Twist Alarm Clock
double Twist Player
Downloader & Private Browser
Dr Panda's Hospital- Vet Game
Dr. Panda's Restaurant Game
Dr. Panda's Veggie Garden
Dr. Seuss's ABC
Dr. Seuss's Sleep Book

Dragon Gem
Draw Something
Draw Something Free
Drawing Cartoons
Drawing Pad
Droid Scan Pro PDF
Droidicon Icon Pack
DroidTV Primetime
Dropbox
Drudge Report
DSLR Controller (BETA)
Ducks Unlimited
Dunkin' Donuts
Dynamic Pads: SwipePad add-on
Easy Battery Saver
Easy Scorecard Pro
Easy Stop Smoking
Easy Tether
Easy Tether Pro
Easy Weight Loss
Easymoney 1.0
EasyNote Notepad To Do lists
eBay Calculator
Edmodo
Electrum Drum Machine/synthesizer
Emoji Keyboard
EMS ACLS Guide
EMS BLS Guide
EMT Tutor NREMT- B Study Guide
Endomondo Sports Tracker Pro
Engagdet
Enhanced Email
Epocratres
Equalizer
eRadar HD: Real-Time and Alerts
ES File Explorer File Manager
ES Task Manager
ESPN College Football
ESPN Fantasy Football 2012
ESPN Mobile App
ESPN Radio
Etsy
Evernote
EveryTrail Pro
eVow Online Dating
eWeather HD, Radar HD, Alerts
Exchange by Touchdown Key
Expedia Hotels & Flights
Extreme Hunting Bundle
Eye in the Sky Weather
ezPDF Reader Multimedia PDF
Facebook
Facebook Messenger
Facedroid Android Facebook
Facetime Plus Trendy
Falcon Pro (for Twitter)
Family Feud & Friends
Family Tracker
Fancy Widgets Unlocker
Fandango Movies
Farm 123 Story Toys Jr.
Fast Burst Camera
Fast Burst Camera
Fast Paleo
FeedR News Reader
FetLife for Android
Fidelity Investments
Fighter Verses

File Manager
Fill and Sign PDF Forms
Fingerprint Scanner
Firefox Browser for Android
Fireworks Live Wallpaper
First Aid
Fitness Buddy
Flashlight
FlightBoard
Flightradar24 Pro
FlightStats for Android
FlightTrack
FlightTrack
FlightView Flight Tracker
Flipboard: Your News Magazine
Flow Free
Fly Delta
FolderSync
Fooducate Healthy Food Diet
Forum Runner
FOX News
Fox Sports Mobile
FOX4 Weather
FoxFi (WiFi Tether) Free
FoxFi AddOn
FoxFi Full Version Key
FPse for android
franco.kernel updater
Free Books & Stories
Free Live TV
Free Movies
FreeCaddie Pro Golf GPS
Fresh Leaves
Friendcast Pro for Facebook
FrostWire
Fruit Ninja
Fruit Ninja Free
Fruit Shoot
FuelLog Car Management
Full classic Movies
full movies online VideoMix
Fun Run- Multiplayer
FunforMobile Ringtones
funnies by ArcaMax
Funny Camera
Funny Facts Free
Funny Jokes
Funny Pictures 1000+
Funny SMS Ringtones
Funny Sound Effects Ringtones
Furby
FxCamera
Galactic Core Free Live wallpaper
Galactic Core Live Wallpaper
Galaxy Pack
Galaxy SII Users Digest
Galaxy Tarot Pro
GalaxyS Go Launcher
GasBuddy Find Cheap Gas
GEICO App
Geocaching
Get Pregnant
Ghost Radar: LEGACY
Glass APEX/NOVA/GO Theme
Glucose Buddy: Diabetes Log
Gmail
GO Keyboard
GO Keyboard Black swan theme
GO Keyboard Emoji plugin
GO Keyboard Neon Theme
GO Keyboard Pink Theme

GO Launcher EX
GO Locker
Go Metro Los Angeles
GO Multiple Wallpaper
GO Power Master (Save Battery)
GO SMS iPhone (iOS) Theme
Go SMS Pro
Go SMS Pro Balloon Theme
Go SMS Pro Dryad Super Theme
GO SMS PRO Pink Zebra Theme
GO SMS Pro Space popup theme
GO SMS Pro WB Pink Zebra
GO SMS Pro Whale Theme
GO SMS Pro WIDE Theme
Go SMS Pro WP7 Theme
GO Weather EX
GO Weather EX
Golf GPS SkyDroid
Golfshot: Golf GPS
Goodreads
goodrx
Google Calender
Google Currents
Google Drive
Google Earth
Google Finance
Google Goggles
Google Maps
Google Maps
Google Play Books
Google Play Magazines
Google Play Movies & TV
Google Play Music
Google Reader
Google Translate
Google Voice
Google Zeitgeist 2012
Google+
Gothic Pack for FlipFont
GoToMeeting
GPS Phone Tacker
GPS Phone Tracker Lite
GPS Staus & Toolbox
Grand Thef Auto III
Granny Smith
Gravy-local events
gReaderPro (Google Reader)
Green Eggs and Ham
Grimm's Snow White
Grocery Gadget Shopping List
Grocery King Shopping List
Grocery Smarts Pro
GrooVe IP
GroupMe
Groupon Daily Deals, Coupons
Gun Club 2
Guns & Destruction
GW Mail
Gymrat Workout Planner
GyroSpace 3D Live Wallpaper
Handcent Emoji Plugin
Handcent SMS
HaxSync 4.x Facebook Sync
HBO GO
HD 12c Financial Calculator
HD Widgets
HDR Camera+
HDW: Tablet weather pack

Headache Diary Pro
Heather scottish voice
Hi-Q MP3 Voice Recorder
Hide It Pro
Hide Pictures in Vaulty
Hide pictures KeepSafe vault
Hill Climb Racing
Hockey Radio
Holo Launcher Plus
Holo Locker Plus
Home Budget with Sync
Home Remedies (Free)
HopStop
Horoscope Plus
Horoscopes
Horoscopes daily
Hotels.com Hotel Booking
Hotmail
HotSchedules
How the Grinch Stole Christmas
How to Draw Easy
How To Sign Language
HP ePrint Home & Biz
HTC SkinGOWeatherEX
Huffington Post for Android
Hulu Plus
Human Anatomy
iAnatomy
iBird Pro
Ibotta
iBP Blood Pressure
ICE: In Case of Emergency
iCorps Pocket Reference
Idyacy Nicole SexyFrench Voice
iFunny :)
iHeart Radio
iLoader for Facebook
IM + Pro
Im excpecting pregnancy app
IMDb Movies & TV
iMediaShare
In Case of Emergency (ICE)
In the Kitchen: Recipes, Chefs
ING Direct
InkPad Notepad - Notes To do
Insight Timer Mediation Timer
InstaFollow For Instagram
Instagram
Instant collage maker
Instant heart rate
Instant Heart Rate- Pro
Instapaper
InstaPicFrame for Instagram
Intuit Gopayment card reader
Inventory Droid
Invoice 2go
iOnRoad Augmented Driving Pro
IP Cam Viewer Pro
iPharmacy Drug Guide
iPhone Messages
iScore Baseball/Softball
iStoryBooks
iSwing Golf Swing Analyzer
iSync for Mac (USB & WiFi)
iSync for PC (USB&WiFi)
iTriage Health
iTunes for Android Sync (wifi)
iTunes to android wireless
iTunes to android wirless pro
IV Drips
IVONA Text-to Speech

J23 Jordan Release Dates
Jamie's 20 Minute Meals
Jefit Pro
Jetpack Joyride
jo-ann
Job Search
Jobs+
Juice Defender battery saver
Juice for Roku
JuiceDefender Plus
JuiceDefender Ultimate
Jump Desktop
JumpStart Preschool 2
Just Me and My Mom
JustReader News Key RSS
JustUnFollow Twitter, Instagram
KakaoTalk Free Calls & Text
Kayak
Kbb.com Car Prices
Keek Social Video
Key Ring Reward Cards
KF FLames Donation
Kick the Boss 2
Kid Mode: Free Games
Kids ABC Letters
Kids ABC Letters Lite
Kids ABC Phonics
Kids ABC Phonics Lite
Kids Animal Piano Free
Kids Animal Piano Pro
Kids Animal Train- First Word
Kids Animals (Children 3 to 9)
Kids Learn to Read
Kids Numbers and Math
Kids Numbers and Math Free
Kids Paint Free
Kids Paintings Coloring Book
Kids reading (preschool)
Kids Shapes (Preschool)
Kids Zoo Animals Sound
Kik Messenger
Kindergarten Kids Math
Kindle
Kingsoft Office 5.2.2
Koi Free Live Wallpaper
Koi Live Wallpaper
Komik Reader
Lab Values + Medical Reference
Lapse It Time Lapse Pro
Launcher 8
LDS Gospel Library
LDS Scriptures App
LDS Tools
Learn Muscles: Anatomy
Ledgerist
Life360 Family Locator
Light Flow LED&Notifcaitons
Light Grid Pro Live Wallpaper
Lightning Bug Beach Pack
Lightning Bug Meditation Pack
LinkedIn
Live ATC for Android
Live TV for Android
Living Social
Locale
Locus Pro
LogMeIn Ignition
Logo Quiz
Lonely Tree Live Wallpaper
Lookout Security & Antivirus
Lose It!
Lotto Results

Lotto Results Premium
love quotes pro
Lumiya
Lustre (adw go apex theme)
Magic Locker Main
Magic Piano
Mall of America Reference
Manga Searcher
Manga Watcher
Manilla Bills and Reminders
MapQuest
MapsWithMe Pro, Offline Maps
Marine & Lakes: USA
Marine Weather Plus by Bluefin
MarineTraffic Ship Positions
Market Update Helper
Marvel Comics
Math Practice Flash Cards
Maverick Pro
MB Notifications for Facebook
Medical Dictionary
Medscape
MeetME Meet New People
Memedroid Pro
Menstrual Calender
Michael Stores
Micromedix Drug Information
Mighty Grocery Shopping
Mileage Tracker
Minecraft Hub (Skin Creator)
Minecraft Pocket Edition
Minecraft Pocket Edition Demo
Minimal MIUI Go Apex
Minimal Reader Pro
Minimals Text
Ministro II
Mint.com Personal Finance
Mirror
Missed It!
mista mixtapes
Mixologist Drink Recipes
Mixology Drink Recipes Free
MixZing Upgrader
MLB.com At Bat
MMA Underground
Mobile Doc Scanner
Mobile Observatory- Astronomy
MoboPlayer
MOG Mobile Music
Money Tab
MoneyWise Pro
Monkey Preschool Lunchbox
Monster Job Search
mooLa! (checkbook & finance)
Moon + Reader Pro
Moon Light GO Weather EX
Moon Phase Pro
Motion Detector Pro Donate
Movie Collection +Inventory
Moviefone
Movies by Flixster
MovieTube: Free Movies
Moxier Mail (Exchange)
MP3 Music Download V8
Mr. Number-Block calls, texts
mSecure Password Manager
MultiPicture Live Wallpaper
Muni Alerts Pro
Muscle Trigger Point Anatomy
Music Volume EQ
Muzy Share photos & collages
MX Mariner Marine Charts

MX Player
MX Player Pro
My Backup Pro
My Beach HD
My Budget Book
My Car Locator
My Coffee Card Pro
My Days Period & Ovulation
My Diet Coach Pro
My Diet Coach Weight loss
My MixTapez
My Movies Pro
My Ovulation Calculator
My Pantry 2
My Pregnancy
My Pregnancy Today
My Tracks
My-Cast Weather
My-Cast Weather Classic
myAT&T
MyCalender
MyCar Locator Free
MyChart
Myibidder Sniper for eBay Pro
MyRadar
Myxer
N.O.V.A. 3 Near Orbit...
NASA App
Naught
Navfree USA: Free SatNav
Navfree: Free GPS Navigation
NAVIGON USA
Navy Feder Credit Union
NBA Game Time 2012-2013
NBC News
Need for Speed Most Wanted
Netflix
NewsRob Pro
Nex honeycomb live wallpaper
Nexercise=fun weight loss
Next Launcher 3D
Nexus Media Importer
NFL
NFL 2013 Live Wallpaper
NFL Sunday Ticket
NFL.com Fantasy Football 2012
NHL Game Center
Nike Training Club
Nike+ Running
Nikon SpotOn Ballistic Match
NIV Bible
NOAA Weather
Nook
Noom Weight Loss Coach
Norton mobile security
Note Everything Pro Add-On
Notification Weather Pro
Nova Launcher Prime
NPR News
Nurses Drug Handbook TR
NYC Subway Embark
NYC Subway Times by MTA [BETA}
NYCMate (NYC Bus & Subway)
NYTimes for Android
OBD DROIDSCAN PRO
Ocean HD
Office Calculator Pro
Office Suite Font Pack
Office Suite Pro 6 +
OfficeSuite Viewer 6

Official eBay Android App
Official Green Bay Packers
Old WootWatcher Donation
Olive Office Premium
On Track Diabetes
One Day at a time
OneBusAway
Onguard Weather Alerts
ooVoo Video Call
OpenTable
Orbitz Hotels, Flights, Cars
Our Daily Bread
Out of Milk Shopping List
Outlook Web Mobile
OverDrive Media Console
pacific/central canad-marine
Package Tracker Pro
Pageonce Money & Bills
Palmary Weather Premium
Pandora internet Radio
Panites x boobs! 2
Pano
Panties x boobs: summer
Panties x Boobs!
Papa John's Pizza
Paper Camera
Paperland Live Wallpaper free
Paperland Pro Live Wallpaper
Paprika Recipe Manager
Paramedic Meds
Paramedic Protocol Provider
Paranoid Android Preferences
Parkmobile
Pattrn
PayPal
PayPal Here
Pediatric EMS
Pen Pack for FlipFont
Perfect Viewer
Perfectly Clear for Android
Period Calender Tracker
Period Tracker
Period Tracker Deluxe
Period Tracker Pro
PGA Tour
Phases of the Moon Pro
Phat Boi FlipFont
Pho.to Lab PRO
Photo Art Color Effects
Photo Collage
Photo Comics Pro
Photo Editor
Photo Editor by Aviary
Photo Editor for Android
Photo Editor Fotolr
Photo Effects
Photo Fun
Photo FX Live Wallpaper
Photo Grid Collage Maker
Photo Sketch
Photobucket Mobile
PhotoWonder
Pic Collage
Picasa Mobile
PicFrame
PicsArt Photo Studio
PicsArt Photo Studio
PicSay Photo Editor
PicSay Pro Photo Editor
PicsPlay Pro
Pill Identifier by Health 5C
Pinger: Text Free + Call Free

Pink Cheetah HD for Facebook
Pink Keyboard
Pinterest
PinterShare Premium
Pix Picture Collage Creator
Pixlr Express
Pixlr-o-matic
Pizza Hut
Plane Finder
Planets Pack
Plants vs. Zombies
Plants Vs. Zombies Comic
Plants vs. Zombies Game Guide
Play to Universal
PlayerPro Music Player
PlayTales Gold
Plex for Android
Plex for Google TV
Plume Premium for Twitter
PNC Mobile
Pocket
Pocket Agent
Pocket Casts
PocketCloud Remote
PocketCloud Remote RDP
PocketMoney
POF Free Online Dating
Pointplus Calculator
Pokedex (donate)
Police Scanner
Police Scanner 5-0
Police Scanner Radio Free
Police Scanner Radio Pro
Police Traps and Speed Cams
Politifact Mobile
PolyClock World Clock
Portable WiFi hotspot
Pose Tool 3D
Poweramp Music Player (trial)
Powerball Scanner
Poynt
Pregnancy Contraction Timer
Pregnancy Test Dr. Diagnosis
Press (Google Reader)
Presto Sound Library Open Beta
Price Check by Amazon
Priceline Hotels & Rental Cars
PrinterShare Mobile printing
Private DIARY
Pro Football Radio
Pro Football Radio & Scores
Pro HDR Camera
Pro Hunting Bundle
Pro Weather Alert
ProBoards
ProCapture camera + panorama
projectMusic Visualizer
Pulse News
Pure Calender widget (agenda)
Pure Grid calender widget
Pure news widget (scrollable)
Push to Kindle
PYKL3 (NEXRAD/TDWR)
QR Barcode Scanner
QR Droid
Quick Manga
Quickoff Pro HD
Quickoffice Pro (Office & PDF)
QuickPic
Race Monitor
Radar Detector
Radar Live Wallpaper

RadarNow!
RadarScope
Rage Comic Maker
Rage Comics
Rage Meme Camera
Rage Reader
Rain Alarm Pro
Rdio
Reader
RealCalc Plus
RealCalc Scientific Calculator
RealPlayer
Reator.com
Recipe Search
Redbox
reddit is fun
Reddit is fun golden platinum
Reddit News
reddit sync pro
redditmag+
RedLaser & QR Scanner
Regions Bank
Relax and Sleep Plus
Remote Desktop Client
Remote for iTunes
RepliGo PDF Reader
Restaurant Weight Loss
RetailMeNot Coupons
Rhapsody
Ringdroid
Ringo Pro: Text & Call Alerts
Ringtone Maker
Ringtone Maker Pro
Robin, the Siri Challenger
RoidRage Comic Maker Pro
ROM Manager
ROM Manager (Premium)
ROM Toolbox Pro
Root Explorer (File Manager)
RootzWiki (Ad Free)
Round Pack for Flipfont
RpnCalc Financial Calculator
RunDouble C25K Pro
Runkeepr GPS Tracker
RunPee
runtastic PRO
Ruzzle
Ruzzle Free
Safeway
Sales Tax Discount Calculator
Sarah UK English Voice
Scanner Radio
Scanner Radio Pro
Scanner911Pro Scanner
ScoreCenter for Android
ScoreMobile: Sports & Scores
ScoutLook Hunting Weather
Scramble With Friends
Scramble With Friends Free
Scratch Draw Art Game
screenshot
Screenshot UX Trial
SD Maid Pro Unlocker
Season Zen HD
Season Zen HD
Seeder
Seesmic Pro
Sense Analog Clock Widget
Sense Analog Clock Widget
Dark
Sense Flip Clock & Weather
SeptaDroid

SeptaDroid Pro
SetCPU for Root Users
Sex Facts
Sex Offenders Search
Sex sounds
SGS3 Easy UMS Support4Dev
Shady SMS 3.0
Shazam
Shazam Encore
Ship Finder
Shopper
Shopping list license
Shopping List Widget
ShopSavvy Barcode Scanner
ShutterFolio for Shutterfly
Sight Words Games & Flashcards
Sign my pad
SimplyNoise
Sirius XM Internet Radio
Sixaxis Controller
Sketch Free
Sketch Guru
Sketch Guru
Sketchbook Mobile
SketchBook Pro for tablets
Ski & Snow Report
Ski Safari
Skout+ Meet, Chat, Friend
Sky Map
Skype Free
Skyvi (siri for Android)
Slacker Radio
Slashtop Remote Desktop
Sleep Deeply
SleepStats
Sleepy Time
SlickDeals Reader Full
SlideIT Keyboard
SlingPlayer for Phones
Smart AppLock Free
Smart Keyboard PRO
Smart Office 2
Smart SWF Player Flash Viewer
Smart Tools
Smart Voice Recorder
Snapchat
Snowfall Free Live Wallpaper
Snowfall Live Wallpaper
Snowmobiling New York State
Soccer Mexican League
Solid Explorer Unlocker
Solunar Fishing & Hunting
Someecards
Songza
SoundCloud
SoundHound
Sounds of Rain Relax your mind
Southwest Airlines
Spanish Translator
sparknotes
SPD Shell 3D
Speaker Boost
Speech Synthesis Data Installer
Speech Synthesis ENGLISH
Speech Synthesis Italian
Speed Anatomy Quiz Free
Speed Bones MD
Speedtest.net
SpeedView Pro
SpeedView: GPS Speedometer
Splash Shopper List Organizer

Splashtop 2 remote desktop

Splashtop Remote Desktop HD

Split Camera: Photo Stories

Sports Wallpaper

SportsTap

Spotify

SQLite Editor

Square Register

Star Chart

Starbucks

Stick It! (Pop-up Player)

Stopwatch & Timer

Storm Shield

Storyline Typewriter FlipFont

Streetview on Google Maps

Stylus FlipFont

Subway Surfers

Sun Rise Free Live Wallpapers

Super Sexy Girls Videos

Super Why!

SuperSU Pro

Superuser Elite

SV-1 SpiritVox "Ghost Box"

SVOX UK English Victoria Voice

SVOX US English Grace Voice

SwiftKey 3 Keyboard

SwiftKey 3 Keyboard Free

SwiftKey 3 Tablet Keyboard

Sygic: GPS Navigation

SymbolsKeyboard & Textart Pro

System ROM Toolbox Pro

System Tuner Pro

Tablet Talk

Tagged Meet New People

Talking Ben the Dog

Talking Ben the Dog Free

Talking Santa

Talking Tom Cat

Talking Tom Cat 2

Talking Tom Cat 2 free

Talking Tom Cat Free

Talking Translator Free

Tango, Text, Voice, Video Calls

Tapatalk Forum App

TapeMachine Recoder

Tapjoy

Target

Task manager

Tasker

Tasks

Tattoos for Men Pro

Taxcaster by TurboTax

Taxi Magic

TD Bank (US)

Team Stream by Bleacher Report

Tech Pack for FlipFont

TED

Temple Run

Temple Run: Brave

Tesla Unread

Text Cutie Instagram Text

Text Me! (Free Texting)

Textfree: Text, Free, Free SMS

Textgram Instagram Text

Textgram Pro

textPlus Free Text + Calls

textPlus Gold Free Text+Calls

Texts From Last Night

The Avengers Iron Man

The Bard's Tale
The Cat in the Hat
The Coupons App
The Game of Life
The Going to Bed Book
The Home Depot
The Lorax
The Night Sky
The Rules of Golf
The Walking Dead Vol. 1
The Walking Dead Vol. 2
The Walking Dead Vol. 5
The Walking Dead, Vol. 4
The Wall Street Journal Mobile
The Weather Channel
Thermometer (free)
This America Life
Thumb Keyboard
Thunderstorm Live Wallaper
Thunderstrom Free Live Wallpaper
Time2Hunt
TimeClock
Tiny Flashlight + LED
tinyCam Monitor Pro
Tip N Split Tip Calculator
Titanium Backup root
Titanium Media Sync
Toddler Coloring Book
Toddler Tapping Zoo
ToMarket Grocery Shopping
TomTom U.S.A.
Top Memory Boosters
Top Rington Downloader
Torque Pro (OBD 2 & Car)
Touch Calender
TouchRetouch
TouchScan (OBD Diagnostics)
Tracing ABC
Trackmaster
Traffic Alert
traffic cameras pro
TransitTimes+ Trip Planner
TransLoc Transit Visualization
Transparent clock & weather
Trapster
TreKing (Chicago)
Trimble Outdoors Navigator Pro
TripAdvisor Hotels Flights
Truck Stops
Truck Stops and Travel Plazas
True Weather LWP
Trulia Realestate
TSF Shell
tTorrent Lite Torrent Client
tTorrent Pro- Torrent Client
Tumblr
Tune Me
TuneIn Radio
TuneIn Radio Pro
TuneSync
TweetCast Pro for Twitter
Tweetings for Twitter
Twin Me!
Twit.TV
Twitter
U.S. Bank
Uber
Ultimate custom widget
Ultimate Food Value Diary 2013
Ultimate Guitar Tabs
Ulysse Speedometer

Ulysse Speedometer Pro
United Airlines
Univision
Univision Deportes
UPS Mobile
Upward Basketball Coach
Urbanspoon
US Military Pay Calculator
US Yellow Pages
USA Today
USAA Mobile
USPS Mobile
Ustream
UTA Tracker+
uTorrent Beta Torrent App
Vault Hide SMS, Pics & Videos
Vaulty Stocks
Verizon Usage Widgets
Vevo
Viber: Free Calls & Text
Video Caller Id
vidtrim pro
Vignette
ViMu Player for Google TV
ViMu Player for Google TV
Virtual Dyno
Visual Anatomy
Visual Anatomy Free
Vitamio Plugin ARMv7 +Neon
Vocre Translate Voice & Text
Voice Grocery Shopping List
Volume+ (Volume Boost)
Voxer Walking Talkie
VPlayer Unlocker
Walgreens
Walmart
Wanelo Shopping
WatchESPN
WatchTV
Water Wallpapers HD Free
WavPlayer
Waze social GPS traffic & gas
Weather
Weather Live
Weather Underground
Weather Widgets
Weather: Local Forecast, Radar
WeatherBug
Weatherbug Elite
Weatherbug Elite
WeatherBug Time &
Temperature Widget
WeatherPro
WebMD for Android
WeChat
Weight Watchers Mobile
Weightwatchers barcode scanner
Wells Fargo Mobile
Whats it worth?
WhatsApp Messenger
When I get Bigger
Where's My Perry?
Wheres My Water
White Noise
Whitepages
WidgetLocker Lockscreen
Widgets for Torque (OBD/Car)
WiFi Connector Library
WiFi Hotspot & USB Tether
Wifi Tether
WiFi Tether Donate
WiFi Tether No Root

Wiki Encylopedia Pro
Wikipedia
Winamp Pro
WIndows 7 GO Launcher
Windows 8 for Android
Wine + List, Ratins & Cellar
Winter Wonderland Live
Wallpaper
WolframAlpha
WomanLog Pro Calender
Word Lens Translator
Word Search
Words With Friends
Workout Trainer
World Weather Clock Widget
Xbox SmartGlass
XDA Premium
XDA Premium HD
XFINITY TV Player
XiaaLive Pro Internet Radio
Xparent Tapatalk Blue
Xparent Taptalk SkyBlue
xScope Browser Pro
Yahoo Mail
Yahoo!
Yahoo! Fantasy Football '12
Yahoo! Fantasy Hockey 2012
Yahoo! Messenger
Yahoo! Sportacular
Yahoo! Weather
Yelp
You Need a Budget
YouTube
YP Local Search & Gas Prices
Zappos
Zedge
Zillow Realestate
Zombies, Run!
Zombies, Run! 5K Training
Zoosk friend, chat, dating

Bibliography

Alastair Beresford and Andrew Rice et al, "MockDroid: trading privacy for application functionality on smartphones," *HotMobile (*2011).

Asian Pacific Economic Cooperation Privacy Framework, *Asian Pacific Economic Cooperation Privacy Framework Privacy Framework,* 2005.

Caimu Tang. "Mobile Privacy in Wireless Networks Revisited." *IEEE Transactions on Wireless Communications* Vol. 7 Issue 3 (2008).

California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, January, 2013.

Chen, Guanling and Farug Rahman, "Analyzing Privacy Designs of Mobile Social Networking Applications," (Paper presented at Institute of Electrical and Electronics Engineers (IEEE) and the International Federation of Information Processing (IFIP) International Conference on Embedded and Ubiquitous Computing, Shanghai, China, December 17-20, 2008).

Children's Online Protection Act of 1998, 15 U.S.C § 6501-6506 (1998).

Clara Mancini et al, "From Spaces to Places: Emerging Contexts in Mobile Privacy," (paper presented at the Proceedings of the 11th International Conference on Ubiquitous Computing, Orlando, Florida, September 30- October 03, 2009).

Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency*, February 1, 2012.

Federal Trade Commission, *Statement of FTC Chairman Jon Liebowitz Updated FTC COPPA Rule*, December 19, 2012.

Federal Trade Commission, *Getting Noticed: Writing Effective Financial Privacy Notices*, October, 2002.

Felt, Porter Adrienne, Erika Chin, Steven Hanna, Dawn Song and David Wagner. "Android Permissions Demystified." (Paper presented at the Conference on Computer and Communications Security, Chicago, Illinois, October 17-21, 2011).

Felt, Porter Adrienne, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin and David Wagner, "Android Permissions: User Attention, Comprehension, and Behavior," (Paper presented at Symposium on Usable Privacy and Security, Washington , DC, July 11-13, 2012).

Howard J. Beales and Timothy Muris, "Choice or Consequences: Protecting Privacy in Commercial Information." *University of Chicago Law Review* 75 (2008), pp 109-135.

Louis D. Brandeis, “The Right To Privacy,” *Harvard Law Review* (1890).

Mill, John Stuart. *On Liberty and Other Essays* (Digireads Books, 2010), pp

National Telecommunications & Information Administration, *Privacy Multistakeholder Process: Mobile Application Transparency*, Updated April 3, 2013.

Nissenbaum, Helen , *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Standford University Press, 2010) PP.

The Nielsen Company, *State of the Appnation*, May 16, 2012, http://www.nielsen.com/us/en/newswire/2012/state-of-the-appnation-%C3%A2%C2%80%C2%93-a-year-of-change-and-growth-in-u-s-smartphones.html.

Rachel Berstein, “Opt-In or Opt-Out?,” Marquette Law School (2011).

The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy*, February, 2012.