DOES THE ANDROID PERMISSION SYSTEM PROVIDE ADEQUATE INFORMATION PRIVACY PROTECTION FOR END-USERS OF MOBILE APPS?

Michael Lane
School of Information Systems, University of Southern Queensland
Queensland, Australia
Michael.Lane@usq.edu.au

Abstract

This paper investigates the Android permission system and its adequacy in alerting end-users of potential information privacy risks in an app. When an end-user seeks to install an app, they are presented with the required permissions and make a supposedly informed decision as to whether to install that app based on the permissions presented. The results from an analysis of ten popular apps indicate a number of permissions that pose potential information privacy risks of which most end-users are likely to be unaware. The Android permission system is complex and difficult for end-users to comprehend and effectively evaluate the potential information privacy and security risks in an app. Most end-users will install the app without evaluating the list of required permissions presented to them. Furthermore there is an inconsistent approach to informing end-users about the privacy policy and terms of use for Android apps. The findings of this paper indicate a need for better decision support apps so end-users can more easily make better decisions regarding privacy and security protection provided by apps. Future research should also examine the free market failure of mobile application market places to provide adequate privacy protection and the need for stronger privacy protection laws.

Keywords
Information privacy, smartphones, android, risks, permission systems, mobile applications.

INTRODUCTION

Smartphones are highly personalised devices which potentially contain a lot of sensitive information about a user (Poremba, 2012; Privacy Rights Clearinghouse, 2012), including personally identifiable information (PII). A smartphone will commonly contain information such as email contacts list, personal photos and videos, credit card details, and so on. This is highly sensitive information and, in many cases, PII (Schwartz & Solove, 2011). The software running on smartphones, including the mobile operating systems and mobile application software commonly known as an "app", pose a number of potential information privacy risks to end-users. By default, the Android mobile operating system (OS) and Android apps require a number of permissions to access system services and information in order to provide required functionality. The Android OS security model has four levels of permissions (1) normal (2) dangerous (3) signature and (4) signature (Android Developer 2012). However, when a user installs an app, the permission requirements for the app (determined by the app developer) are presented to the end-user in a list. Some of these permissions are potentially dangerous and may pose privacy and security risks to the end-user such as sharing of PII with third parties, malicious code and introducing vulnerabilities (Hogben & Dekker, 2010). However, currently it is difficult for the end-user to evaluate privacy and security risks associated with an app based on the permissions presented to them. Hence end-users generally blindly accept the terms of use and privacy policy of an app and the required permissions for the app (Australian Communications and Media Authority, 2011). This paper seeks to show that end-users of smartphones may be exposed to information privacy and security risks through the required permissions of many commonly used Android apps. This paper is structured as follows. First the relevant literature provides the background and context for this study. Then the methodology used in this study is described. Next, the results of the data analysis are presented and discussed. Finally the main conclusions, implications and future directions of this research are presented.

BACKGROUND TO STUDY

Information Privacy

In this paper we use Clarke (2006)'s definition of information privacy: 'as the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves'. Privacy laws are premised on the out dated conceptions of a "reasonable expectation of privacy" which is becoming increasing

more difficult to apply to the protection of personal information in the context of Internet enabled services and applications which can be accessed by a range of Internet enabled devices including smartphones (Stevens, 2011). Privacy laws vary in their protection of personal information according to jurisdiction, European Union being the most progressive in protecting privacy of personal information privacy with their EU data protection directive in comparison to USA which until recently has refrained from regulation to protect the privacy of personal information (Movius & Krup, 2009).

Smartphones

Internet enabled devices such as a smartphone in the future will be the most likely device that many end-users will use to access the Internet and cloud based services (Kar, 2012). With smartphones end-users are continuously connected to the Internet via 3G networks and WiFi networks. Smartphones with significant processing power, memory and storage, have become commonplace with the availability of affordable devices and plans (Bartsch, Sohr, Bunke, Hofrichter, & Berger, 2012). Smartphones are extremely versatile in terms of their functionality, and are used widely beyond the scope of making a phone call for activities such as a contactless wallet, a barcode reader, a satellite navigation system, an email or social network client, web browsing client and a WiFi hotspot (Hogben & Dekker, 2010).

Google data shows that adoption of Smartphones has reached over 50% of the population in six countries, namely Australia, the United Kingdom (UK), Sweden, Norway, Saudi Arabia and the United Arab Emirates (UAE) (Sibley 2012). Furthermore, the adoption rates are particularly high in young adults. This category of user is less likely to understand risks associated with any breaches of their information privacy (see Table 1).

Table 1 Smartphone adoption rate by top six countries and age (Source: adapted from Our Mobile Planet, 2012)

Smartphone Adoption by Country	**Percentages for age and overall**			
	18-29	**30-49**	**>= 50**	**All**
Australia	73	66	28	52
Norway	79	68	33	54
Saudi Arabia	67	56	39	60
Sweden	82	67	25	51
UAE	70	58	37	61
UK	75	69	23	51

This paper focuses on the third risk identified in the Enisa (2010) report, i.e. unintentional data disclosure in the context of the Android operating system. This risk highlights that information privacy and security has become particularly challenging for end-users of smartphones.

Mobile applications (apps)

A mobile application, commonly referred to as an "app," is a type of application software designed to run on a mobile device such as a smartphone or tablet (What is mobile application?). Apps frequently endeavour to provide users with similar functionality to what an end-user might access on their PC or laptop. Initially apps tended to provide limited and specific functionality such as a game, calculator, or mobile web browsing. However apps have increasingly grown and matured into complex, extremely functional, software that greatly extends and utilises the multifunctional capabilities of smartphones and tablets, in a diverse range of application domains (Martin, 2011).

Android marketplace for mobile apps – Google Play

Google Play, as at 27th September 2012, showcased 675,000 apps on the Android OS and is steadily closing in on Apple's App store which boasts close to 700,000 apps on Apple's iOS (Northern Voices Online, 2012) The estimated number of apps downloaded from the Google Play Store has exceeded 20 billion and the Android OS has been installed on more than 400 million devices (Felt, Chin, Hanna, Song, & Wagner, 2011). Google is starting to take information privacy much more seriously now and recently, on 1st March 2012, revised its approach to information privacy by replacing specific privacy policies for over 60 services with one privacy policy (http://www.google.com/policies/privacy/) that provides an overarching framework for data privacy protection for all of the online services it provides, including Google Play market for Android apps. Google has added a field for developers to fill out their privacy policy when submitting an app to the Google Play market, and made the addition of a clear privacy policy a recommended addition for developers. In the future it is

expected that a privacy policy will be explicitly presented to Google Play market customers, allowing them to view a privacy policy before downloading and installing an app.

Android permissions system

Traditional user-based permission systems assign the full privileges of the end-user to all applications (Felt, 2012). Modern platforms such the Android OS for smartphones provide a different set of permissions for each app based on its requirements. The advantage of such an approach is that apps will generally rely on less than full privileges. The Android development platform provides a thriving market for third party apps. However third party apps can pose many risks for end-users in that some third party apps may contain malicious code and/or can introduce vulnerabilities because third party apps have not been developed with security in mind (Chickowski, 2012; Dekker & Hogben, 2011). In order to protect end-users from threats associated with the numerous third party apps that may be installed on a smartphone; the Android OS uses app permissions to control access to security and privacy relevant parts of Android OS APIs (Felt, Egelman, & Wagner, 2012).

Problem with permissions in Android apps

The concept of app permissions is "great in theory" (Hoffman, 2012). The problem is that most Android users have no idea of what app permissions imply for ensuring the security and privacy of the apps they are using. For many users, permissions have unfortunately become like a EULA, something to quickly tap through when installing apps (Northern Voices Online, 2012). This situation is not helped by the way app permissions are presented in a menu list to end-users, without any indication as to the level of information privacy and security risks associated with an app. Apps are a "privacy nightmare" (Rodriguez, 2012). An app can be constantly connected to the Internet, and can upload personal data such as private photos or documents to a remote server without end-user knowledge or consent, as the end-user has often unknowing granted access to these services by blindly accepting the required permissions when installing an app. The Android security model has four levels of permission protection (1) normal (2) dangerous (3) signature and (4) signature or system (Android Developer, 2012). The Android Market displays a prompt for dangerous permissions to end-users during installation. Normal permissions can be viewed once a mobile app is installed but have to be accessed via a dropdown menu. Signature/System permissions are not displayed to users at all (Felt, et al., 2012). Furthermore, studies have shown that current Android developer API's make it difficult for developers to align "least privilege" permission requests with application functionality, even for those developers who wish to do so (Vidas, Christin, & Cranor, 2011).

Android Application Permission Categories

This section discusses each of the main categories and sub categories in terms of what they actually do (Kolobaric, 2011) and how they might impact on an end-user's privacy and security (see Table 2).

Table 2 Categories of Android permissions & potential impact on information privacy/security (source adapted from (Kolobaric, 2011))

Category of permission	Description	Impact on information privacy and security
Services that Cost You Money	Gives an app ability to use services such as calling and texting.	Potentially they can cost an end-user money and can be misused by a malicious app.
Your Messages	Gives an app ability to read and write SMS and MMS messages.	Potential risk to information privacy of end-user
Storage	Allows an app to read/write to SD card or internal memory of the phone	Potential risk to information privacy of end-user
Your personal information	Able to read contact list of account configured in a smartphone Should be treated with caution	Potential risk to information privacy of end-user
Phone calls	Allows an app to read state of phone and identity such as IMEI, IMSI and 64-bit unique ID of phone	
You location	Allows an app to determine an end-user's location, through GPS or mobile networks.	Potential risk to information privacy of end-user if information is shared with third parties
Network communication	Allows an app to access Internet.	Information about an end-user can be shared with third parties without their knowledge

Category of permission	Description	Impact on information privacy and security
System tools	Used by most apps in order to provide required functionality that is part of smartphone system	By modifying system tools app could access sensitive information on smartphone
Hardware Controls	Allows apps to use hardware aspects of a smartphone vibrating smartphone when SMS message is received	
Your Accounts	Gives an app chance to check which accounts are activated to provide user the options to interact with it. It doesn't necessarily approve an app to use account for anything by itself.	

With all of these permission categories, is it realistic that an end-user can evaluate an individual app during its installation to determine whether all of the stated required permissions are really needed for its functional purpose? Given that "Services That Cost Money", to be able to "send an SMS which will incur a cost", or access "Your Accounts", to use "authentication credentials of an account such as a Gmail email account which might compromise personal information" about an end-user, pose potentially significant information privacy and security risk for end-users. In practice most end-users will make a quick decision on whether to install an app based on its functionality and its ratings in the Google Play market. This situation is further complicated by the fact that many "free" apps use Internet and location access permissions for advertising in order to generate revenue, and either deliberately or unintentionally developers create applications with greater permissions than are required for their marketed functionality.

RESEARCH QUESTIONS AND METHODOLOGY

The following research questions are investigated in this study: **R1:** Do Android apps pose information privacy and security risks to end-users? **R2:** Does the Android permission system provide adequate privacy and security protection for end-users of apps?

This research used a case study approach to assess the information privacy risks associated with 10 purposively selected Android apps across the top 10 popular categories. One popular mobile app was selected from each of the top 10 Android market categories as at the 29th September 2012 from the www.appbrain.com web site (See Figure 1 below).

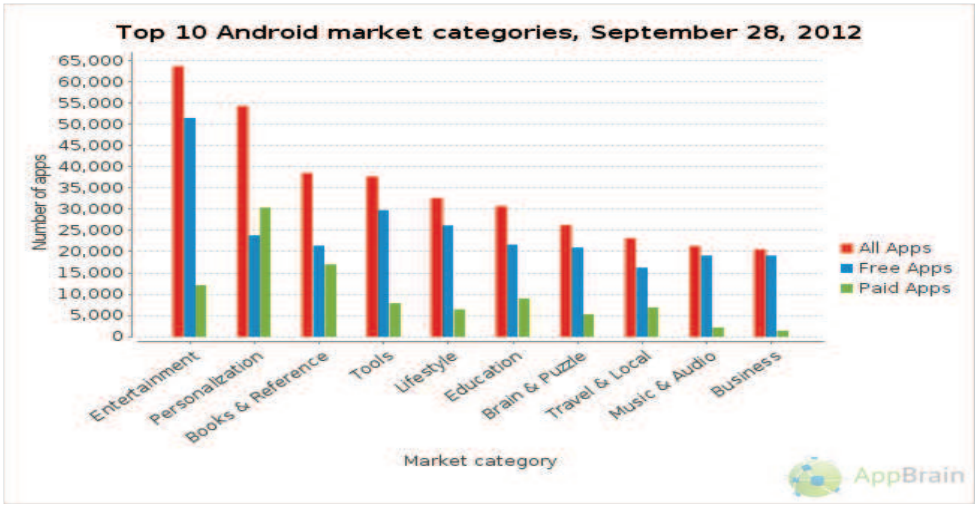

Figure 1

Figure 1. Comparison of Top 10 Android market categories (Source www.appbrain.com/stats/android-market-app-categories)

An overview is provided of the characteristics of each app (app category, number of downloads, download size, average rating). Each app is compared and analysed in terms of any dangerous permissions listed, and whether each app has an official web site and provides a terms of use policy and a privacy policy. Both www.appbrain.com and www.play.google.com were used to identify and analyse dangerous permissions used by each of the 10 apps selected for this research.

DISCUSSION OF RESULTS FROM DATA ANALYSIS OF TEN APPS

Table 3 An analysis of required permissions of ten popular apps (source www.play.google.com and www.appbrain.com web sites).

Permissions	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**No of Permissions**
Your personal information											***7 concerns in total***
read contact data	YC	YC						YC			4 (4 concerns)
write contact data	YC							YC			2 (2 concerns)
Choose widgets		YC									1 (1 concern)
Services cost money											***3 concerns in total***
Directly call phones		YC			YC			YC			3 (3 concerns)
Send SMS											
Your location											***4 concerns in total***
coarse (network-based) location			YC					YC	YC		3 (3 concerns)
fine (GPS) location					YC			YC			2 (2 concerns)
Network communication											1
view network state	Y			Y	Y	Y	Y	Y	Y	Y	8
view Wi-Fi state	Y							Y	Y	Y	4
full Internet access	Y			Y	Y	Y	Y	Y	Y	Y	8
Your Accounts											***3 concerns in total***
View configured accounts								YC			1 (1 concern)
Google Maps								Y			1
Discover known accounts								YC			1 (1 concern)
Manage account list								Y			1
Use authentication credentials of an account								YC			1 (1 concern)
Storage											***0 Concerns in total***
modify/delete SD card / USB contents	Y	Y	Y			Y		Y	Y	Y	7
Phone calls											***0 Concerns in total***
read phone state and identity	Y		Y	Y	Y			Y	Y		6
System tools											**3 concerns in total**
Modify global system settings	YC	YC							Y		3 (2 concerns)
Prevent phone from sleeping		Y				Y		Y	Y		4
Change Wifi state								Y			1
Install shortcuts		Y						Y			2
Disable keylock								Y			1
Automatically start at boot				Y				Y			2
Expand/collapse status bar		Y									1
Retrieve running applications		YC									1 (1 concern)
Set wallpaper		Y									1
Set wallpaper hints		Y									1
Restart other applications		Y									1
Make applications always run		Y									1
Set preferred applications		Y									1
Kill background processes										Y	1
Hardware controls											
Control vibrator		Y					Y	Y			3
Record audio								Y			1
Extra permissions **(can be multiple for an app)**		Y						Y	Y	Y	4
Total	8	16	3	4	5	4	3	23	14	6	***20 concerns overall***

Legend: Category of apps 1.Entertainment 2. Personalisation 3. Books and Reference 4. Tools 5. Lifestyle 6. Education 7. Brain and Puzzle 8. Travel and Local 9. Music and Audio 10. Business; Y = YES permission used in app; C = Concern about dangerous permission used in app identified by www.play.google.com and www.AppBrain.com

Each of the 10 apps listed in Table 3 are discussed in terms of their characteristics, privacy policy and terms of use and permissions concerns.

App1 is a MP3 Music downloader app in the Entertainment category, with over 250,000 downloads, 0.72 MB download size, and over 250,000 ratings with an average rating of 4.46. It has **no official web site** and there is **no link to a privacy policy and terms of use policy**. Google Play lists two dangerous permission that are a concern, **(1) can access contacts (names, phone numbers, emails),** malicious apps may use this permission to send phone contact data to third parties, or to erase or modify phone contact data**; (2) modify global systems settings,** malicious apps may corrupt system's configuration**.**

App2 is an Android home launcher replacement app, Personalisation category, with over 250,000 downloads, 7MB download size, and over 750,000 ratings with an average rating of 4.59. It **does not have a link to a privacy policy or terms of use policy** on its official web site. Google Play lists six dangerous permissions that are a concern, **(1) can access the list of contacts (names, phone numbers, emails)** malicious apps may use this permission to send phone contact data to third parties, or to erase or modify phone contact data **(2) can use SMS services or phone calls which cost money,** allows app to call phone numbers without intervention. Malicious apps may cause unexpected calls on phone bill. **(3) modify global systems settings,** malicious apps may corrupt system's configuration**. (4) Retrieve running Apps,** allows app to retrieve information about currently and recently running tasks. Malicious apps may discover private information about other apps; **(5) Choose widgets**, allows app to tell 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; **(6) Set preferred Apps**, allows app to modify your preferred apps. Malicious apps may silently change apps that are run, spoofing existing apps to collect private data from end-user.

App3 is an Android dictionary app, Books and Reference category with over 250,000 downloads, 2 MB download size, and over 200,000 ratings with an average rating of 4.59,. It has links to a privacy policy and a terms of use policy on its official web site. Google Play list one dangerous permission as an explicit concern **(1) can determine your current location and send it to third party,** access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this permission to determine approximately where end-user is.

App4 is a battery indicator app, Tools category, with over 250,000 downloads, 1.7 MB download size, and over 200,000 ratings with an average rating of 4.68.,. It has a link to the Google Play privacy policy, and a link to the Google hosting project terms of use policy. Google Play does not list any dangerous permission as a concern for this app.

App5 is an online pizza ordering app, Lifestyle category, with over 250,0000 downloads, 15MB download size, and over 85,000 ratings with an average rating of 4.77. It has links to a privacy policy and a terms of use policy on its official web site. Google Play lists two dangerous permissions as an explicit concern **(1) can use SMS services or phone calls which cost money,** allows app to call phone numbers without intervention. Malicious apps may cause unexpected calls on phone bill; **(2) can determine your current location and send it to a third party,** access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this permission to determine approximately where end-user is.

App6 Learn Japanese app, Education category, with over 250,000 downloads, 1.3MB download size, and over 1900 ratings with an average rating of 4.73. It **does not have links to a privacy policy and a terms of use policy** on its official web site. Google Play does not list any dangerous permission as an explicit concern.

App7 is a puzzles app, Games and Puzzles category, with over 250,000 downloads, 7.3MB download size, and over 200,000 ratings with an average rating of 4.55. It does not have an official web site and **does not have links to a privacy policy and a terms of use policy**. Google Play does not list any dangerous permission as an explicit concern.

App8 is GPS map navigation app, Travel and Location category, with over 250,000 downloads, 7MB download size, and over 200,000 ratings and an average rating of 4.37. It has links to Google Play privacy policy and terms of use policy. Google Play lists four dangerous permissions as explicit concerns **(1) can access the list of contacts (names, phone numbers, emails)** malicious apps may use this permission to send phone data to other third parties, or to erase or modify phone contact data**; (2) can discover your accounts and get your email address,** manages accounts lists, allows app to perform operations like adding and removing accounts, and deleting account password. Use authentication credentials of an account, allows an app to request authentication tokens, allows apps to sign into this app using account(s) stored on Android device; **(3) can use SMS services or phone calls which cost money,** allows an app to call phone numbers without intervention. Malicious apps

may cause unexpected calls on phone bill**; (4) can determine your current location and send it to a third party,** access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this to determine approximately where you are. Access fine location sources such as the Global Positioning System on the phone, where available. Malicious apps may use this to determine where you are, and may consume additional battery power.

App9 is a personalised Internet radio app that plays music and comedy, Music and Audio category, with over 250,000 downloads, 1.4MB download size, and over 30,000 ratings with an average rating of 4.5. This app has links to a privacy policy and a terms of use policy on its official web site. Google Play list one dangerous permission as a concern: **can determine your current location and send it to a third party,** access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this permission to determine approximately where end-user is**.**

App10 is an office document app, Business category, with over 250,000 downloads, a 11.3MB download size, and over 29,500 ratings with an average rating of 4.57. This app has a link to a privacy policy on its official web site but does not have a terms of use policy. Google Play does not list any dangerous permission as a concern.

Table 3 shows Android permission categories which grant a smartphone app access to (1) personal information, (2) location information, (3) phone services that are billable such as calls or SMS, (4) end-user account information and credentials, and (5) system tools functionality are potentially problematic. These app permissions may either maliciously or unintentionally expose an end-user to significant information privacy and security risks that of often they will be unaware. Only three of the 10 selected apps did not list any dangerous permissions. Four of the selected apps do not provide privacy policies and/or terms of use policies and if provided these are obscurely located on the official app web site.

CONCLUSIONS AND IMPLICATIONS

The Android permissions system provides a security mechanism to manage the permissions requirements of hundreds of thousands apps. The permission requirements for an app are determined by the app developer and the end-user is presented with a list of required but potentially dangerous permissions when they choose to install an app. The security integrity of this system relies on the end-user being aware of what these permissions actually mean. The reality is that most users will ignore or not understand these permissions and simply install an app. The analysis of 10 popular apps shows there are a number of potential information privacy risks associated with specific permissions required by apps. It should also be noted that the level of privacy concern will also vary across different categories of apps. For instance, the level of privacy concern for an online dictionary app will be much different to a map navigation which might disclose personal information and location information to other third parties. However it is often unclear for end-user perspective as to what information is being accessed by an app and how this app is using information accessed from end-user's smartphone. Thus the complexity of the Android permission system, and the inconsistent and vague approach to informing end-users of the terms of use and privacy policy for an app, means the end-user is at a distinct disadvantage in terms of receiving adequate information privacy protection. This indicates a failure of the free market and the need for stronger privacy protection laws that are unilateral in their jurisdiction given the global nature of the Android app market. There is also a need for better decision support apps so that end-users can more easily make better decisions regarding the privacy and security protection provided by apps when (1) installing an app and (2) on an ongoing basis ensuring that an app is not breaching their privacy and security either through malicious intent, or through an unintentional vulnerability as a result of poor security design.

REFERENCES

Android Developer. (2012). Permissions | Android Developers Retrieved from http://developer.android.com/guide/topics/security/permissions.html

Australian Communications and Media Authority. (2011). Emerging business models in the digital economy - The mobile applications market Retrieved from http://www.acma.gov.au/webwr/_assets/main/lib310665/emerging_business_models.pdf

Bartsch, S., Sohr, K., Bunke, M., Hofrichter, O., & Berger, B. (2012). The Transitivity of Trust Problem in the Interaction of Android Applications. *CoRR, 1204.1458*.

Chickowski, E. (2012). Secure Coding Practices Out The Window With Mobile Apps. *Dark Reading* Retrieved from http://www.darkreading.com/mobile-security/167901113/security/news/232600607/secure-coding-practices-out-the-window-with-mobile-apps.html

Clarke, R. (2006, 20th September 2012). What's 'Privacy'? Retrieved from http://www.rogerclarke.com/DV/Privacy.html

Dekker, M., & Hogben, G. (2011, 9th September 2011). Appstore security: 5 lines of defence against malware Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware/at_download/fullReport

Felt, A. (2012). *Towards Comprehensible and Effective Permission Systems.* PhD Dissertation, UNIVERSITY OF CALIFORNIA, BERKELEY. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-185.pdf

Felt, A., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011, 2011). *Android Permissions Demystified.* Paper presented at the ACM Conference on Computer and Communication Security (CCS) 2011.

Felt, A., Egelman, S., & Wagner, D. (2012). I've Got 99 Problems, But Vibration Ain't One: A Survey of Smartphone Users' Concerns: UC Berkley.

Hoffman, C. (2012). How App Permissions Work & Why You Should Care [Android]. *Makeuseof* Retrieved 29th September, 2012, from http://www.makeuseof.com/tag/app-permissions-work-care-android/

Hogben, G., & Dekker, M. (2010). Smartphones: information security risks, opportunities and recommendations for users: ENISA.

Kar, S. (2012). Booming Mobile Web Access Signals the Death of PCs | SiliconANGLE. Retrieved from http://siliconangle.com/blog/2012/11/07/booming-mobile-web-access-signals-the-death-of-pcs/

Kolobaric, D. (2011). Android and Privacy: Guide to Android Application Permissions. *BrightHub* Retrieved from http://www.brighthub.com/mobile/google-android/articles/91280.aspx

Martin, T. (2011). Will mobile applications become more expensive as functionality increases? Retrieved from http://www.phonedog.com/2011/04/19/will-mobile-applications-become-more-expensive-as-functionality-increases/

Movius, L., & Krup, N. (2009). U.S. and EU Privacy Policy: Comparison of Regulatory Approaches. *International Journal of Communication, 3*, 169-187.

Northern Voices Online. (2012). Google Play Vs App Store: Google Play gets 25 billion app download Retrieved from http://nvonews.com/2012/09/28/google-play-vs-app-store-google-play-gets-25m-app-download/

Our Mobile Planet. (2012) Retrieved from http://www.thinkwithgoogle.com/mobileplanet/en/

Poremba, S. M. (2012). Smartphones and privacy: Are we overreacting? Retrieved from http://www.msnbc.msn.com/id/45743849/ns/technology_and_science-security/t/smartphones-privacy-are-we-overreacting/#.UKHKi4fkvHS

Privacy Rights Clearinghouse. (2012). Privacy in the Age of the Smartphone Retrieved from https://www.privacyrights.org/fs/fs2b-cellprivacy.htm

Rodriguez, A. (2012). Android's Permission Problems *PC World* Retrieved from http://www.pcworld.com/article/251824/androids_permission_problems.html

Schwartz, P., & Solove, D. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review, 86*, 1814 -1894.

Stevens, G. (2011). Privacy Protections for Personal Information Online (pp. 1-15): Congressional Research Service.

Vidas, T., Christin, N., & Cranor, L. (2011). *Curbing Android Permission Creep*. Paper presented at the 2011 Web 2.0 Security and Privacy Workshop (W2SP 2011), Oakland, CA. http://www.andrew.cmu.edu/user/nicolasc/publications/VCC-W2SP11.pdf

What is mobile application? - A Word Definition From the Webopedia Computer Dictionary. Retrieved from http://www.webopedia.com/TERM/M/mobile_application.html