Exploring the Implications of Permission Changes and Users' Needs in Google Play Store

by

Adel Alhejaili

Submitted in partial fulfillment of the requirements for the degree of Master of Computer Science

at

Dalhousie University

Halifax, Nova Scotia

April 2016

DEDICATION PAGE

To every member in my family for their love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Smartphones in the recent years have become the ubiquitous devices that offer diverse sets of functionalities and supplant the use of traditional computers. It becomes apart of people's everyday life.

Android uses a permission system that put the burden mainly on users to detect any invasive apps. Past research should when users cannot understand the presented warnings, they tend historically to make poor privacy and security decisions.

This thesis discusses the implication of permission changes, users' needs and concerns on the Google Play Store. I conducted an observation study with semi-structured interviews followed by a post-online questionnaire to seek broader understating of how users interact and select application from the Google Play Store and the factors that they consider when installing an app. How users are currently viewing permissions and are they aware of the existence "Permission Details" Icon. Two classifications were used to analyze the data. Novice versus advanced users and the Westin' metric index.

Our results showed that only 8% of the population was aware of the "Permission Details" Icon. Users are now more aware of permissions than before but still they explanations. We found that the Westin's metric showed a stronger relationship with various security measures better than using the novices versus advanced users' classification based on security courses. We found that the more security courses the users' took, the lower their score in the Westin's metric are. Future work will expand the scope of this thesis to include more diverse populations.

LIST OF ABBREVIATIONS USED

EULA	**End User License Agreement**
TOS	**Terms of Service**
ADV	**Advanced User**
NOV	**Novice User**
UN	**Privacy Unconcerned**
PR	**Privacy Pragmatists**
FU	**Privacy Fundamentalists**

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor Dr. James Blustein for the useful comments, remarks and engagement through the learning process of my Master’s thesis; he has greatly helped me to form my understanding of Human Computer Interaction. Also, I want also to thank Bradly Frankland for his advice about statistical analysis.

I would also like to sincerely thank my beloved family and especially my mother, who has supported me through the entire process and for helping me putting pieces together.

To my wife, Mayyan, who has always been there for me, and to my son Abdullah and to my daughter Amirah, for their patience while I spent much of my time pursuing my master’s degree.

Last but not least, I would like to acknowledge the financial support of Taibah University for the scholarship granted to me for the duration of my master’s degree.

CHAPTER 1 INTRODUCTION

1.1 OVERVIEW

Smartphones in the recent years have become the ubiquitous devices that offer diverse sets of functionalities and “supplant the use of traditional computers”. It becomes apart of people’s everyday life [1,2]. The growth and popularity of using smartphones are constantly increasing [3] According to Statistics Portal, the total units of smartphone shipments globally are expected to reach over 1.44 billion units in 2015 [4]. The current dominant player market is the Android operating system, account for 82.8 % share in the second quarter of 2015 [5].

People are using millions of smartphone apps that are available through different app marketplaces for personal and business purposes [6, 7]. Some of these markets are maintained officially by platform providers such as Apple and Google Play Store; and some are unofficial such as Amazon App Store, APPTISM and AppBrain market[8].

Apple employs a strict vetting app process before any app gets into their App Store. On the other hand, Google Play Store (the official Android App Store) provides a ‘relaxed app submission’ process [9]. What makes Android Operating System popular is that it supports third-party applications markets [7]. Submitting an application to the Google Play Store was easy: all one needed was an anonyms developer account to pay $25 and you could upload your application to the Store. There was “no upfront review process” or approval process to check if the application does what it supposes to do. However, Google for the last several months has put new measures in effect including a launch checklist before any developer can publish their apps to the Google Play Store [10,11].

At the time of writing this thesis, according to AppBrain Stats, Google Play Store includes 1.7 million applications ranging from free and paid apps. Google is still in the lead in terms of the number of downloaded apps by over 190 billion times. According to AppBrain Filter Detection System, the percentage of low quality app is around 12% and these apps are roughly removed from the store once a quarter [12, 13].

Despite the popularity of Android, a recent report by Symantec's latest Internet Security Threat Report stated, "17% of All Android apps were actually malware in disguise". "Malware are programs or apps that are created to do harm such as viruses, worms and Trojan horses". Grayware apps accounted 36% of all Android apps. Despite the fact that these apps are "not malicious by design", still it can "track users' behavior" for targeted ads revenue [14]. Although, Google attempted to limit the increase of malware apps in the past, still their success is limited and its store has vast amount of malware apps [7].

1.2 RESEARCH OBJECTIVES

The main objective of my thesis is investigate the implications of the permissions changes and what uses' need in Google Play Store. Also, looking at the factors that users consider when downloading an application and if they consider permissions or not. Moreover, to look at the changes of the permission group naming between the old and new version of the Android OS. Which one is more appealing to users and easier to perceive. Finally, to look at the differences between of the users under the advance/novice classification as well the Westin's metric classification.

CHAPTER 2 BACKGROUND AND RELATED WORK

In this chapter, I provide an overview of Android Permissions as well as the application installation process, permission understanding and issues. Then, present some of the relevant research on smartphone privacy and warning research.

2.1 ANDROID PERMISSIONS

Android uses a Permission system that put the burden mainly on users to detect any invasive applications. This permission system has two main tasks to protect its users when they download and install applications on their smartphones. First, restrict the ability of apps to "access sensitive hardware resources”. Second, provide assistance to help users make the right decision before they install. The only way that these resources can be accessed by Android apps are when the required permissions are declared in the application “manifest file” after users approve these permissions during the installation process. Android permissions are used to ensure the security of user’s devices resources [15, 16].

Developers use permissions to gain access to the smartphone hardware features such as: accessing location for accurate weather updates, accessing camera to take photos and record videos. When users are searching for an app on the official Google Play Store, they are presented of dozens of applications to choose from. Before they choose an app that seems relevant to their needs; they might play the application video tutorial, read the application text description and look at the app screenshots to understand the features that the app offers. Also, they could read other users reviews, ratings and some would examine the requested permissions. After that, users have two options: whether they accept the permissions and install the app afterward; or they do not install at all. If users accept and grant the requested permissions, and later on if they want to revoke some; they only have to uninstall the app [15, 16].

Android 5.2 defines approximately 150 permissions, categorized into 31 permission groups. However, only 17 permission groups that are most common used permissions will only appear on the installation screen of the new presentation of permissions on Google Play Store. The rest may or may not appear within the application information only. Further details will be discussed later on the Permission Changes section. These permissions fall into four protection levels [7, 17, 18]:

- **Normal:** these permissions are granted automatically at the application installation time to access phone recourses without explicitly asking the user approval. They considered a low-risk permission that cannot cause harm to users.
- **Dangerous**: these permissions can give the application access to the user private data and can control the device. They considered as high-risk permissions that would negatively impact the user. These permissions may be displayed during the installation time to users asking them for confirmation.
- **Signature:** these permissions are granted by the system only if the application that request them has a signed certificate by the people who built the operating system of the application that declared the needed permissions.
- **Signature/System:** Similar to Signature protection level, except that the system only grants permissions if the application has the system image in the Android System. These permissions are only used by the device manufactures and vendors who built the applications in the system image.

2.2 PERMISSION UNDERSTADING

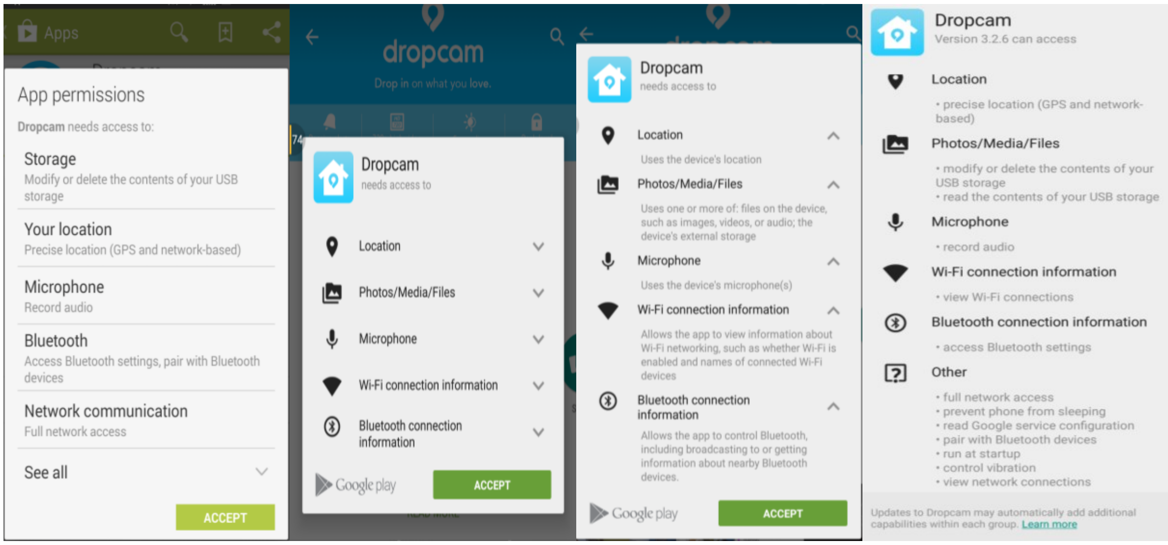
For many years, "Google has been criticized of this approach for various reasons" [18,p.16]. Vidas et al.'s [19] described, "users historically make poor privacy and security decisions" specifically when users cannot understand the presented warnings and be able to act with satisfaction upon these requests. More importantly, Rogers et al.'s [20]. illustrated that it is a complex process to understand the best ways of how the warning information should be presented. Likewise, Hong [21] clearly said it is an open question for researchers to look at "the kinds of information that a display should show", when and where to present the information; is it while the "users are looking for apps" or at the same moment after they have downloaded the app or while using the app or after they have used it.

Another issue to consider is an average user will not be able to comprehend the meaning of approximately 150 permissions [17,19]. Similarly, another study by Liccardi et al.'s [6] found that that only 20% of their participants understood the meaning of each requested permission. Also, users have "misunderstanding of legitimate apps" that used permissions that may appear suspicious but it does not have the ability to transmit personal data outside the phone. Another study by Liccardi et al.'s [16] found that when users are examining permissions during installing an app, this implies that they have "the knowledge of how their phone operates and can differentiate between indifferent permissions (i.e., permissions that are used to interact with the hardware of the phone), permissions that manipulate preferences and information (i.e., that have the ability to write), permissions that can read preferences and information (i.e., permissions that have the ability to read users' information and manipulate them), and network-based permissions (i.e., permissions that allow information exchange via the Internet). Apps come with a multitude of permissions and reading each permission and description in order to understand what they enable can take a lot of effort and/or specialized knowledge". Understanding and reading each permission and its description require from users specialized knowledge and a lot of effort [16]. Moreover, Felt et al.'s [22] study reported that only 17% of their participants had "paid attention" to the requested permission during the application installation process, 42% of participants did not know about "the existence of the permission" screen and only 3% answered correctly the three questions of permissions comprehension. Also, they reported that only 4 participants out of 85 who correctly answered the question of describing the permission “Read Phone State”. This permission “enable the app to detect whether the phone is actively making or receiving a call, provide critical access to the IMEI of the device, the subscriber ID, the serial number of the SIM card” [22]. “Apps do not need users’ IMEI to function” and developers are using it to send the collected data “to ad networks for targeted ads” [23]. Furthermore, Kelley et al.’s [24] study found that users cannot understand the permissions because of “the human-readable-terms” that have been used to describe Android permission before installing an application were: “vague, confusing, misleading, jargon-filled and poorly grouped”. Also, Lin et al.’s [15] reported that the Android permission screens “lack adequate explanation and definitions”. Another serious issue is that some developers by mistake tend to ask for more permissions than its required for the app to work properly, and this is due insufficient documentation [25]. Relatedly, Vidas et al.’s [19] stated that developers were not able to align correctly the required permission to the intended application function because of the documentation issue. Stevens et al. [26] stated that the reason for developers to ask for more permissions is to protect users from experiencing application crashes. Moreover, Wei et al.’s [27] studied the evolution in the Android ecosystem and found “the permission model is becoming more complex and hard to users and developers to understand”. Furthermore, Harbach et al.’s [28] reported that the level of education affects the understanding of “computer warning messages” and their data suggested that on average users’ need at least “10 years of education to understand these messages”.

Lastly, Woyke [23] stated that both Android and Apple OS are in a struggle of how to explain all the things going on inside an app without having too little or too much details”.

2.3 PERMISSION CHANGES AND ISSUES

In June 2014, “Google implemented an extensive update” of its Play Store and changed the structure, presentation of the "permission screen" and the level of the provided details [18]. As shown in Figure 1(a) represents the old view of permissions when users click on the Install button. Some of the permissions headings categories are: Storage, Your Location, Microphone, Bluetooth and Network Communication. If users are interested in looking further for the whole list, they can click on “See all” to reveal them. On the other hand, Figure 1(b) shows the newly refined Permissions Groups (previously called: Permission Headings Categories). Some of the new permissions groups are Location, Photos/Media/Files, Microphone, Wi-Fi connection Information and Bluetooth Connection Information. Moreover, if users want more information, they can click on the arrow symbol to reveal more general details about the requested permissions as you see in Figure 1 (c). [18], [29], [30]



App permissions

Dropcam needs access to:

Storage
Modify or delete the contents of your USB storage

Your location
Precise location (GPS and network-based)

Microphone
Record audio

Bluetooth
Access Bluetooth settings, pair with Bluetooth devices

Network communication
Full network access

See all

Dropcam
needs access to

Location

Photos/Media/Files

Microphone

Wi-Fi connection information

Bluetooth connection information

Dropcam
needs access to

Location
Uses the device's location

Photos/Media/Files
Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage

Microphone
Uses the device's microphone(s)

Wi-Fi connection information
Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

Bluetooth connection information
Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

Dropcam
Version 3.2.6 can access

Location
- precise location (GPS and network-based)

Photos/Media/Files
- modify or delete the contents of your USB storage
- read the contents of your USB storage

Microphone
- record audio

Wi-Fi connection information
- view Wi-Fi connections

Bluetooth connection information
- access Bluetooth settings

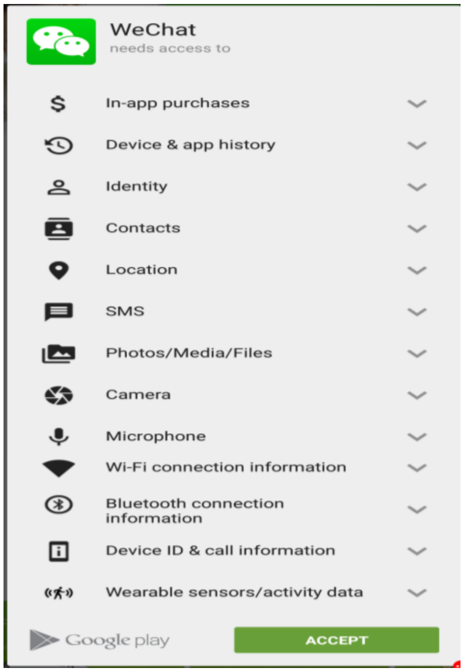
Other
- full network access
- prevent phone from sleeping
- read Google service configuration
- pair with Bluetooth devices
- run at startup
- control vibration
- view network connections

Updates to Dropcam may automatically add additional capabilities within each group. Learn more

Figure 1: (a) on the left: the old view of permissions interface of Google Play Store (until version 4.6.17), (b) on the middle left: the new view of permissions interface until version 5.1, (c) on the middle right: the new interface with general details of requested permissions, (d) on the right: full permission details and “Learn More” blue link [18, 29, 30].

The difference between the two views of permissions interfaces is how they show additional information about what permissions that the app needs. For example, on the old view under the Permission Group for example Storage; you can see in Figure 1(a) the complete list of the actual required permissions under this category. However, instead of describing the actual permissions, the new view only shows general information under the Permission Group Photos/Media/Files that the app is going to use one or more of the files on the device.

Google also reallocated the refined permissions under 17 Groups. When users press the "Install" button on the application page, they can see only 13 groups of permissions that WeChat app requires as Figure 2 shows, in addition to the other three Permission Groups. Also, Figure 1 (d) shows the last permission group called "Other" that covers any other permission that are not corresponded to any of the 17 Permission groups. This group only appears on the new added feature called "Permission Details". Since "users are most likely do not read documentation, they will only know about the screen that followed the "Install" or the "Update" button". As a result, "they will not be able to know the existence of the "Other" permission group" [18].



WeChat
needs access to

In-app purchases

Device & app history

Identity

Contacts

Location

SMS

Photos/Media/Files

Camera

Microphone

Wi-Fi connection information

Bluetooth connection information

Device ID & call information

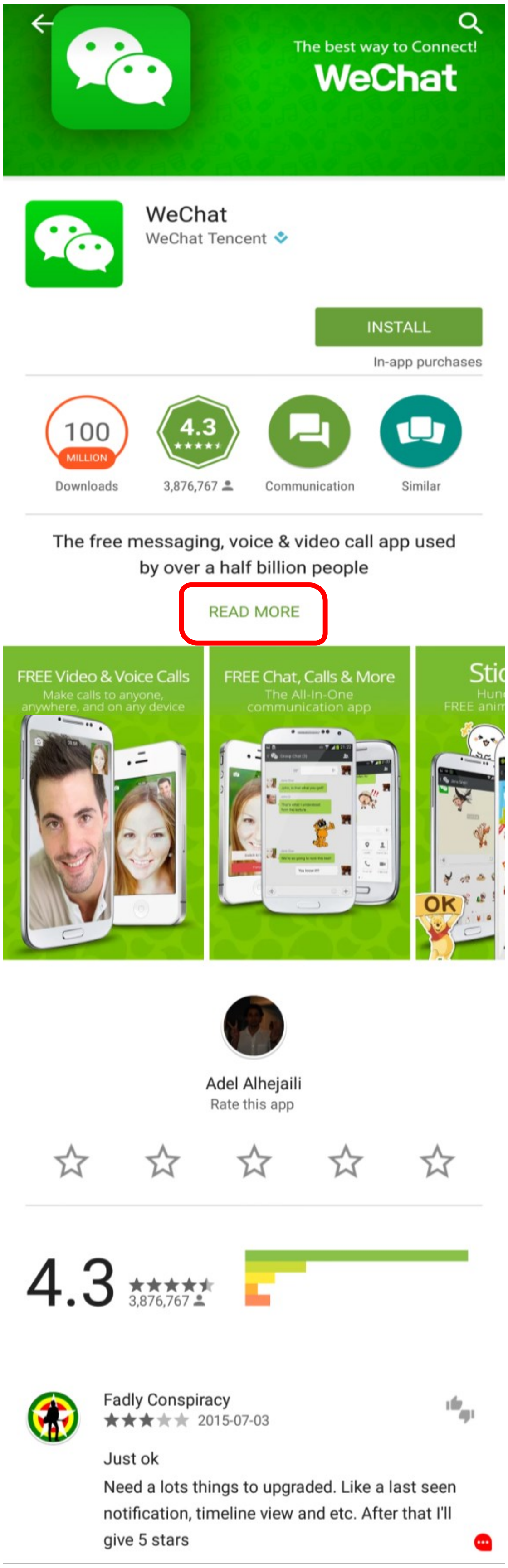
Wearable sensors/activity data

Google play

ACCEPT

Figure 2: WeChat Permissions Groups [6]. The figure only shows 13 groups. "Cellular Data Settings", Calendar" and "Phone" Groups are not shown. The total number of Permission Groups is 17 including the "Other" Group [29].

Users who have concerns about permissions have to take the “complicated access route” to click on “Permission Details” as shown in Figure 3. They have to scroll down to the end of the app description page on the left corner under the heading “Developer” to see the full detailed permissions lists in the form of points and if they want more they can click on blue “Learn More” link, as seen in Figure 1(d). Gerber et al.’s [18] reported “users are not expected to initiate the search process of another screen in order to see the full requested permissions”. If users want to read more about the app or read reviews, the scrolling will be longer. Another way that users can use to check permissions is via the “App Info” under the application settings menu within the app itself [18, 29, 30]. “Google explicitly stated that users are always asked to check the permission changes, however, the changes that have been made only appears under the “Permission Details” link and most users won’t scroll down to look for the full list of permissions”[18]. Akhawa and Felt [31] found in their study that “users rarely click on explanatory links such as ‘More Information’” which is similarly to clicking on “Learn More” link. Also, they stated that “designers should not hide an important detail” in the process of making a decision.



WeChat

WeChat Tencent

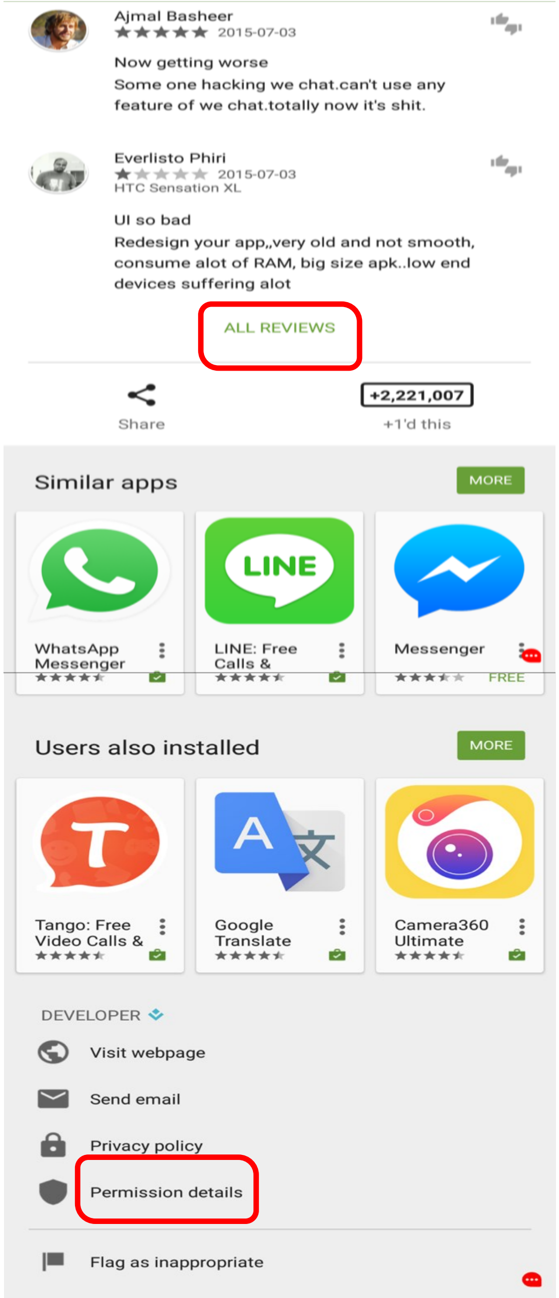
The free messaging, voice & video call app used by over a half billion people

Adel Alhejaili

Fadly Conspiracy ★★★☆☆ 2015-07-03

Just ok

Need a lots things to upgraded. Like a last seen notification, timeline view and etc. After that I'll give 5 stars

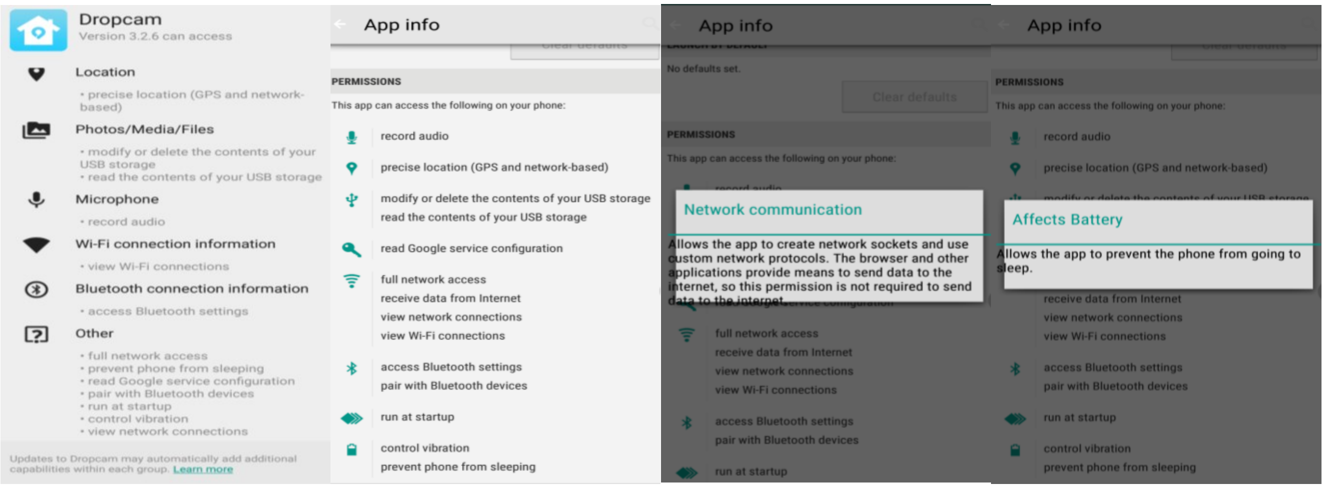

Ajmal Basheer
★★★★★ 2015-07-03

Now getting worse
Some one hacking we chat.can't use any feature of we chat.totally now it's shit.

Everlisto Phiri
★☆☆☆☆ 2015-07-03
HTC Sensation XL

UI so bad
Redesign your app,,very old and not smooth, consume alot of RAM, big size apk..low end devices suffering alot

Figure 3: App Description page on Google Play Store. “Read More”, “All Reviews” and “Permission Details” are circled [30].



Dropcam
Version 3.2.6 can access

Location
- precise location (GPS and network-based)

Photos/Media/Files
- modify or delete the contents of your USB storage
- read the contents of your USB storage

Microphone
- record audio

Wi-Fi connection information
- view Wi-Fi connections

Bluetooth connection information
- access Bluetooth settings

Other
- full network access
- prevent phone from sleeping
- read Google service configuration
- pair with Bluetooth devices
- run at startup
- control vibration
- view network connections

Updates to Dropcam may automatically add additional capabilities within each group. Learn more

App info

PERMISSIONS

This app can access the following on your phone:

record audio

precise location (GPS and network-based)

modify or delete the contents of your USB storage
read the contents of your USB storage

read Google service configuration

full network access
receive data from Internet
view network connections
view Wi-Fi connections

access Bluetooth settings
pair with Bluetooth devices

run at startup

control vibration
prevent phone from sleeping

App info

No defaults set.

Clear defaults

PERMISSIONS

This app can access the following on your phone:

Network communication

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.

full network access
receive data from Internet
view network connections
view Wi-Fi connections

access Bluetooth settings
pair with Bluetooth devices

run at startup

App info

PERMISSIONS

This app can access the following on your phone:

record audio

precise location (GPS and network-based)

Affects Battery

Allows the app to prevent the phone from going to sleep.

receive data from Internet
view network connections
view Wi-Fi connections

access Bluetooth settings
pair with Bluetooth devices

run at startup

control vibration
prevent phone from sleeping

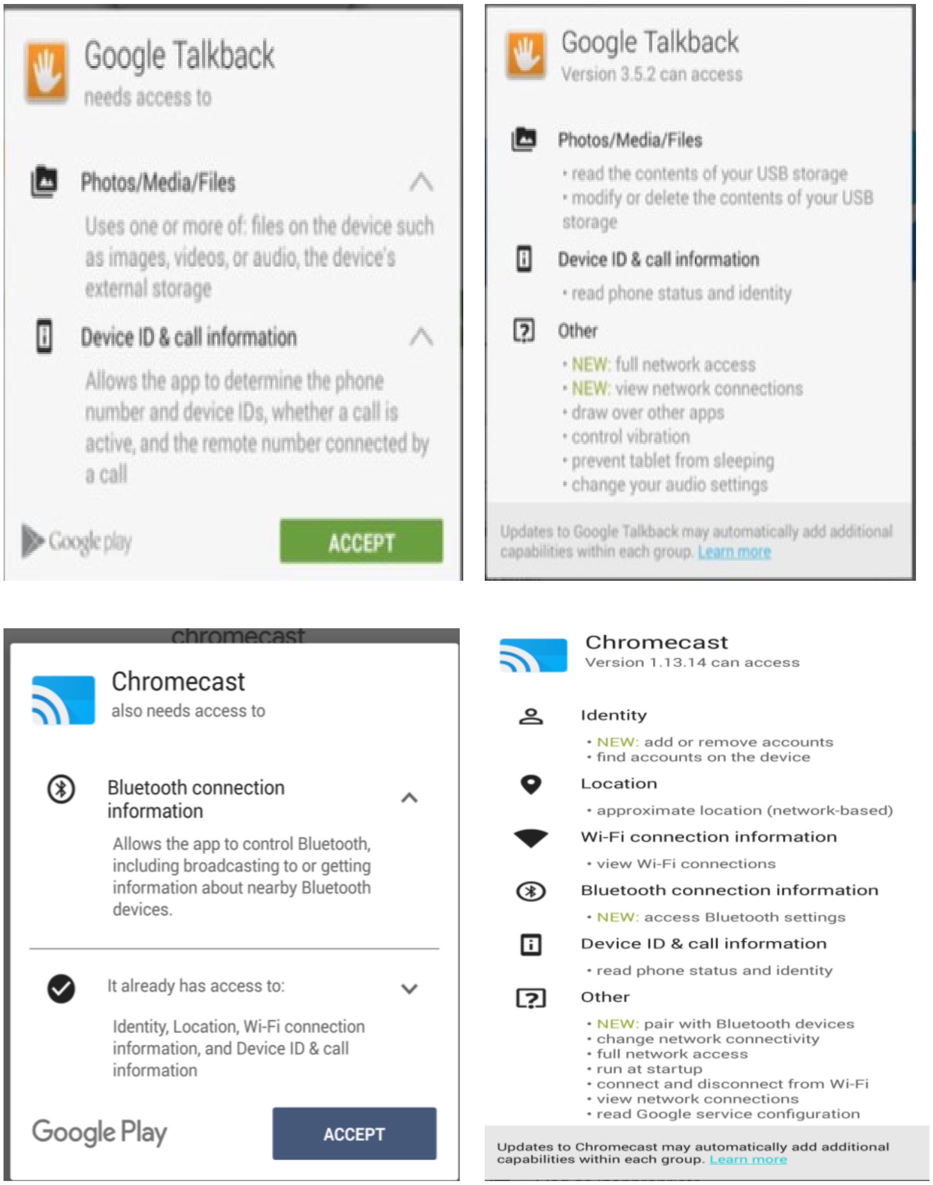
Figure 4: (a), on the left: the new view of the whole list of requested permissions under "Permission Details Icon", (b) on the middle left: the old view of permissions within the application information under settings, (c) on the middle right: the permission group "Network Communication" when users click on "full network access" permission, (d), on the right: the permission group "Affects Battery" appears when user click on the permission "prevent phone from sleeping" for more details [18, 29, 30].

Gerber et al.'s [18] reported the "Unintuitive Permission Allocation Permission Groups" issue. As shown in Figure 4 (a), the permission "access Bluetooth settings" appears under the Permission Group "Bluetooth Connection Information" and the permission "Pair with Bluetooth Devices" appears under the Permission Group "Other". The question is why they did not add the last permission to the same Bluetooth Group.

There are two ways if users want to check permission after they installed the application. Firstly, users have to go back to the Google Play Store and click on "Permission Details" icon. Secondly, users have to select the "Menu Settings", then "Apps" or "Applications Manager" and choose the required app from the list. The permissions are displayed at the bottom of "App Info", as shown in Figure 4 (b). Now users might notice that symbols and the names of the Permissions Groups are different except two to three groups. The presentation of the permissions within the "App Info" is almost identical to the old representation of the Google Play Store as shown in Figure 1(a). For example, the permission "Prevent phone from sleeping" appears on the new interface, as seen in Figure 4(a) under the "Other" group. On the other hand, within the "App Info", it appears under a total different Group called "Affects Battery". Similarly, on the new view of permissions that are related to network communications permissions are spilt into two Permissions Groups", "Wi-Fi Connection Information" and "Other". Also, "full network access" permission appears under the "Other" Group on the new view but when you check the same permission within the "App Info", it appears under the "Network Communication" group. The old views of permissions are well integrated and described. Every permission appears under its corresponded Permission Group. Lastly, the new view shows 17 Permissions Groups, however, the Permission Groups within "App Info" are 31 groups; as shown in Figure 5. Some of these groups will not appear because it depends on the application itself that require extra permission such as: "Private Permission" which is only Signature System Permissions that can only accessed by Manufactures or vendors. As a result, users will have difficult experience to make informed decision [18, 29, 30].

1- "Phone Calls"
2- "Your Messages"
3- "Camera"
4- "Microphone"
5- "Your Location"
6- "Your Personal Information"
7- "Your Social Information"
8- "Your Application Information"
9- "Storage"
10- "Your Accounts"
11- "Network Communications"
12- "Voice Mail"
13- "Development Tools"
14- "System Tools"
15- "Status Bar"
16- "Sync Settings"
17- "Screen Lock"
18- "Alarm"
19- "Bookmarks and History"
20- "Other Application UI"
21- "Affects Battery"
22- "Wallpaper"
23- "Bluetooth"
24- "Audio Settings"
25- "Shortcuts"
26- "Hardware Controls"
27- "Private Permissions"
28- "Display"
29- "User Dictionary"
30- "Calendar"
31- "System Clock"

Figure 5: The complete permissions within the "App Info" [6].



Google Talkback
needs access to

Photos/Media/Files

Uses one or more of: files on the device such as images, videos, or audio, the device's external storage

Device ID & call information

Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

Google play ACCEPT

Google Talkback
Version 3.5.2 can access

Photos/Media/Files
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Device ID & call information
- read phone status and identity

Other
- NEW: full network access
- NEW: view network connections
- draw over other apps
- control vibration
- prevent tablet from sleeping
- change your audio settings

Updates to Google Talkback may automatically add additional capabilities within each group. Learn more

chromecast

Chromecast
also needs access to

Bluetooth connection information

Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

It already has access to:

Identity, Location, Wi-Fi connection information, and Device ID & call information

Google Play ACCEPT

Chromecast
Version 1.13.14 can access

Identity
- NEW: add or remove accounts
- find accounts on the device

Location
- approximate location (network-based)

Wi-Fi connection information
- view Wi-Fi connections

Bluetooth connection information
- NEW: access Bluetooth settings

Device ID & call information
- read phone status and identity

Other
- NEW: pair with Bluetooth devices
- change network connectivity
- full network access
- run at startup
- connect and disconnect from Wi-Fi
- view network connections
- read Google service configuration

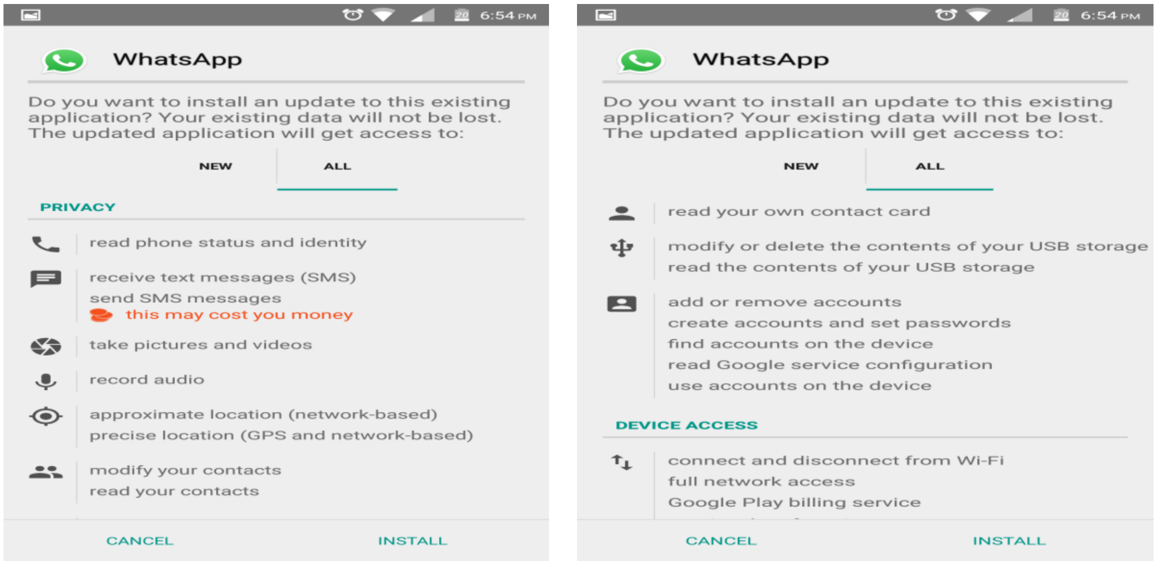
Updates to Chromecast may automatically add additional capabilities within each group. Learn more

Figure 6: (a) on the top left: shows that the app needs to access new permissions under two different Permission Groups after clicking on the Update Button. (b) On the top right: shows the highlighted hint green word (NEW) followed by the added permissions after clicking on "Permission Details". (c) On the bottom left: shows the new requested permissions as well as what already has been accessed by the app after clicking the Update Button. (d) On the bottom right: shows the new added permissions [18, 29, 30].

"Permission Group Agreement" issue reported by Gerber et al.'s [18] that "any app that already granted a set of permissions, may extended the app access to any other permissions within the same group without informing the users".

The previous example shows an issue reported by Gerber et al.'s [18], which is "the complicated access to additional permissions at update". This will affect users and they will not be able to know what the app exactly needs to access. Figure 6 (a) shows that the app needs to access new permissions under two permission groups: Photo/Media/Files and Device ID& Call Information. However, as Figure 6 (b) shows that new added permissions (Full Network Access and View Network Connections) are under the permission group “Other” which they are not related to the new requested permissions Photos/Media/Files and Device ID& Call Information. If users did not click on the “Permission Details” icon at the end of the application description page, they will not be able to make an informed decision because they are not aware of the silently added permissions. Also, Figure 6 (c) shows that the app needs to access permissions under the permission group Bluetooth Connection Information and it shows also what are the permission groups that had already been given access too such as: Identity, Location, and Wi-Fi connection information. On the other hand, Figure 6 (d) shows that if users click on the “Permission Details” icon they will find that there are new requested permissions; (access to Bluetooth settings) which is under the permission group Bluetooth connection Information and (Add or Remove Accounts) under the permission group Identity. The previous example shows that when users click on the “Update” button, they will not see the extra permissions that are silently added to the app without informing users about those changes. Users can accept the new update if they changed the update settings from the Google Play Store to be manual, “otherwise applications can be updated automatically without user’s intervention”.

Another issue is that if users download apps from un-official stores or websites, their experience will be different.



WhatsApp

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

PRIVACY

read phone status and identity

receive text messages (SMS)
send SMS messages
this may cost you money

take pictures and videos

record audio

approximate location (network-based)
precise location (GPS and network-based)

modify your contacts
read your contacts

WhatsApp

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

read your own contact card

modify or delete the contents of your USB storage
read the contents of your USB storage

add or remove accounts
create accounts and set passwords
find accounts on the device
read Google service configuration
use accounts on the device

DEVICE ACCESS

connect and disconnect from Wi-Fi
full network access
Google Play billing service

Figure 7: (a) on the left: shows some permission groups under the category "Privacy". (b) On the right: shows the category "Device Access" [29], [30].

Sometimes the app itself will request the update once you open the app. In this case, the representation of the new required permissions as well as the what has been already granted are identical to the old design of Google Permission of the operating system 4.6 and earlier as seen in if Figure 7 (a &b). Developers tend to ask for more permissions during the update if they need to access more hardware features to add extra app functionalities. For example, if there is a track fitness app that offers certain features but it is still do not have the feature of keep track of how many miles does someone run in a day. So, if the developer wants to add another feature to his app by including collecting data from the phone sensors, he need to request more permissions by pushing them through an update under the permission group "Wearable sensors/activity data".

The new 17 permission groups cannot be seen. Also, two heading categories: "Privacy" and "Device Access" appears only when downloading from any websites. However, these two headings will not be seen if users choose the "App Info" under the "System Settings" and they only see the entire set of permissions.

The last issue reported by Gerber et al.'s [18] is "Impersonal and Harmless-Sounding Permission Description". The current permission descriptions "seems more technical" and impersonal than the old ones. Their example was, "the old explanation said (access to) "Your Location", "Your Accounts" or "Your Personal data"". On the other hand, the naming of the current permission groups" is corresponded to the terms "Location" and "Contacts/Calendar". "A semantic reference to the individual person is clearly avoided so users tend to associate more with functions than with personal privacy". Renaming the permission groups and "making them not personalized", "inexperienced users who are less familiar with technology will tend to underestimate the granted permissions, and not perceive them as applying to themselves and their personal data". This will result in the "tendency to ignore the permission screen completely" [18].

2.4 PERMISSION MAPPING

The first table describes the old and new naming of "Permission Groups" as well as including the most common used permission labels under each group based on extensive observation of the most used applications in the Google Play Store [30]. It also shows a comparison between the two permission designs. As described earlier, the old design has 31 permission groups and the new one has 17 permission groups. To illustrate the comparison, for example, "Device & App History" permission group exists in the current design and it has "Read Sensitive Log Data", Retrieve System Internal State", Read your Bookmarks and History" and Retrieve Running Apps" permission labels. However, on the old design, the previous permissions are found under three different permission groups: "Bookmarks and History", "Your Application Information" and "Development Tools".

Permission Groups (Old view – OS 4.6 & earlier)	**Permission Groups** (New view – OS 5 to 5.9)
Network Communication - Google Play Billing Services	**In-App Purchases** - Google play billing services
Bookmarks & History - Read your web bookmarks and history **Your Application Information** -Retrieve running apps **Development Tools** - Retrieve system internal state - Read sensitive log data	**Device & app history** - Read sensitive log data - Retrieve system internal state - Read your web bookmarks and history - Retrieve running apps
Network Communication - Receive data from the Internet	**Cellular Data Settings** (no specific permissions). Control mobile data connection and received data
Your Personal Information - Read your own contact card **Your Accounts** - Find accounts on the device - Add or remove accounts	**Identity** - Find accounts on the device - Read your own contact card (example: name and contact information) - Modify your own contact card - Add or remove accounts
Your Social Information Similar	**Contacts** - Read your contacts - Modify your contacts
Your Location Similar without the last two	**Location** - Approximate location (network-based) - Precise location (GPS and network-based) -Access extra location provider commands GPS access
Your Personal Information Similar	**Calendar** - Read calendar events plus confidential information - Add or modify calendar events and send email to guests without owners' knowledge
Your Messages Similar	**SMS** - Receive text messages (SMS) - Read your text messages (SMS or MMS) - Receive text messages (MMS, like a picture or video message) - Edit your text messages (SMS or MMS) -Send SMS messages; this may cost you money - Receive text messages (WAP)

Phone Calls - Reroute outgoing calls **Your Social Information** - Read call logs	**Phone** - Directly call phone numbers; this may cost you money - Write call log (example: call history) - Read call log - Reroute outgoing calls - Modify phone state - Make calls without your intervention
Storage - Modify or delete the contents of your USB storage - Read the contents of your USB storage	**Photos/Media/Files** - Read the contents of your USB storage (example: SD card) - Modify or delete the contents of your USB storage - Format external storage -Mount or unmounts external storage
Camera Similar	**Camera** -Take pictures and video - Record video
Microphone Similar	**Microphone** - Record audio
Network Communication - View Wi-Fi connection	**Wi-Fi connection Information** - View Wi-Fi connection
Bluetooth - Access Bluetooth settings	**Bluetooth connection information** - Access Bluetooth settings
NA	**Wearable sensors/activity data** - Body sensors (heart rate monitors)
Phone Calls - Read phone status and identity	**Device ID & Call information** - Read phone status and identity

Alarm **Wallpaper** **Your Application Information** **Affects Battery** **System Tools** **Network Communication** **Bluetooth** **Sync Settings** **Audio Settings** **Other Application UI** **Your Social Information** **Your Accounts** **Screen Lock**	**Other** - Set an alarm - Control flashlight - Adjust wallpaper size - Read your social stream - Write to your social stream - Access subscribed feeds - Send sticky broadcast - Create accounts and set passwords - Run at startup - Prevent phone from sleeping - View network connection - Install shortcuts - Use accounts on the device - Uninstall shortcuts - Change your audio settings -Read Google service configuration - Toggle sync on and off - Modify system settings - Full network access - Pair with Bluetooth devices - Connect and disconnect from Wi-Fi - Read sync settings - Control vibration - Change system display settings - Close other apps - Access mail info - Change network connectivity - Control NFC - Set wallpaper - Email attachment - Draw over other apps - Disable lock screen -Read battery stats

Table 1: Comparison between the naming of the old and new permission groups [7], [29], [30].

The second table shows the old permission groups (previously called "Heading Categories") and their permissions. It includes the most common, observed and related requested permissions to this work through Google Play Store [5,6].

Old Permission Groups	
Phone Calls - Read phone status and identity - Directly call phone numbers - Reroute outgoing calls	**Status Bar** - Expand/collapse status bar
Network Communication - Full network access - Google Play billing service - Receive data from Internet	**System tools** - Send sticky broadcast - Modify system settings - Read subscribed feeds

- View network connections - View Wi-Fi connections - Connect and disconnect from Wi-Fi - Control Near Field Communication - Change network connectivity - Download files without notification - Google Play license	- write subscribed feeds - Access extra location provider commands -Interact across users - Read home settings and shortcuts
Your Messages Similar as **SMS**	**Lock Screen** - Disable your screen look
Your Social Information - Modify your contacts - Read your contacts - Read call log - Write call log - Read your social stream - Write to your social stream	**Hardware Controls** Signature permissions that have direct access to the hardware of the device
Your Personal Information - Read calendar events plus confidential information - Add or modify calendar events and send email to guests without owners' knowledge - Read your own contact card	**Bookmarks and History** - Read your web bookmarks and history - Write web bookmarks and history
Your Application Information - Run at startup - Retrieve running apps- tasks - Close other apps - Make app always rum - Reorder running apps	**Sync Settings** - Read sync settings - Toggle sync on and off - Read sync statistics
Your Accounts - Add or remove accounts - Create accounts and set passwords - Find accounts on the device - Read Google service configuration - Use accounts on the device	**Affects Battery** -Control vibration -Prevent phone from sleeping -Control Flash light
Camera - Take pictures and videos	**User Dictionary** -Read user dictionary -Write user dictionary
Microphone - Record audio	**Bluetooth** **-**Pair with Bluetooth devices **-**Access Bluetooth settings
Your location - Approximate location (network-based) - Precise location (GPS and network-based)	**Wallpaper** - Set wallpaper – Adjust your wallpaper size
Storage - Modify or delete the contents of your USB storage - Read the contents of your USB storage	**Other Application UI** - Draw over other apps
Voice Mail - Add/Write/Read voice mail	**Audio Settings** - Change your audio settings
Development Tools -Modify secure system settings -Read sensitive log data	**Alarm** - Set an alarm

-Retrieve system internal system	
Calendar -Read Calendar -Write Calendar	**Shortcuts** -Install shortcuts -Uninstall shortcuts
Display - System alert window	**System Clock** -Set time -Set time zone

Table 2: Old permission groups and its permissions [7], [29], [30].

2.5 SMARTPHONE PRIVACY

Research studies of users' smartphone privacy concerns have mainly focused in the past on "location tracking and sharing [2]. Even though sharing location is considered as "an important aspect of smartphone privacy", there are only 2 out of 152 permissions that are designated to location. Other work has focused on building tools that help users to be aware of "privacy violation". These tools were built to identify any malicious behavior. Others considered looking into ways of helping users to make an informed decision [22]. Stowaway [25] checks and detects if any Android apps have over privileged permissions. Kelley et al.'s [32] designed Privacy Facts which is build on top of the Android permission system. They displayed under the short app description eight different types of personal information that the app can collect: "personal information, contacts, location, calendar, credit card/financial, diet/nutrition, health/medical and photos". Also, it showed if the app is using advertising libraries and analytics. If any of these information is accessed by the app, there is a checkbox in front of each information type. This presentation helped users to install apps with less permissions. RecDriod framework was designed "to "control permissions in real time and receive recommendations from expert users who use the same apps". This framework has two modes: probation and trusted modes. Users can check which permissions they want to monitor while using the app. When a permissions is requested, the users are shown a pop up message indicating the name of the permission, the RecDroid recommendations and its confidence level ranging from low to high using a color bar and whether the users agree or disagree. Their design helped users to make less false decisions [33]. Kang et al.’s [34] proposed privacy meter framework. It is similar to Kelley et al.’s [32] work in which they put their sliding bar from being safe to dangerous under the short description and screenshots of the app page. They found that when the current “Google’s permission screen was used”, 61% of their participants recommended apps with high privacy risks to their family and friend members. However, using privacy meter dropped the rate to 26%, which showed that it was quick and easy to interpret the potential risks that the may have [34]. The framework by Harbach et al.’s [35] communicated personalized examples of the requested permissions to users by showing them in the real time what is being accessed. For example, if the app needs to access the Storage permission, a photo from the user’s phone is presented during the installation process. Another example, when the app needs to access the location permission, the users is presented with a picture under the Your Location permission group showing the user current location. The researchers found that their framework made participants make “privacy-conscious choices” when deciding to install an app. However, their results also showed that their “approach caused negative affect”, which made participants pay more attention. Much work has been published with regards what users needs. Users are looking for explanations of the used permissions. Justifications are required to bridge the gap between permissions that access phone resources and their intended functionalities [2, 15, 22, 32, 36–42].

2.6 WARNING RESEARCH

Wolteger developer a model of how human process warning messages formalize the steps of how a human experience a warning message and act on that warning accordingly [43].

This model is known as the “Communication-Human Information processing (C-HIP)”. Cranor framework “human in the loop” is based on the C-HIP model, which provides “a systematic approach” for designers to “identify potential causes for human failure”. This framework would help designers to “identify problem areas before a system is built”. Also, it shows how effectively a warning can be communicated and delivered to the end user [44]. Many people for many reasons ignored EULA and TOS warnings. They are similar to the Android permission system. All of the previous warnings types were shown to users during the installation process. “Users’ lack of attention” to the various types of warnings is carried out over other types of “install-time consent dialogs”. Users became habituated to these repeated warnings [45].

CHAPTER 3 METHODOLGY

This chapter describes the method that used to uncover the implications of permission changes permissions and users' needs in the Google Play Store.

3.1 HYPOTHESES

My initial hypotheses were:

Novice users are not aware of the "permission details" icon.
Advanced users are aware of the "permission details" icon.

Novice users will not click on the "permission details" icon.
Advanced users will click on the "permission details" icon.

Novice users will not assign permission label to Permission Group.
Advanced users can and will assign the correct permission label to the Permission Groups.

I tended to test all the above hypothesis During the work of this thesis, however, other hypotheses were formulated during the analysis and it will be discussed later (see Section 4).

3.2 RESEARCH QUESTIONS

I am interested in how different group of users are viewing permissions and if they going to notice the existence of the new added "Permission Details" icon. Can users choose the correct Permission Groups of a given permission Label? Which one is better, the old naming of permission groups or the new one. Where would users go if they want to check for permissions or look for explanation? How would users want the permissions to be presented? What are the changes, complaints and features that users want on Google Play Store? What are the factors the users consider before downloading an app?

3.3 STUDY DESIGN

I followed a two-step procedure to conduct the study. The study procedures were adapted from Felt et al.'s [22], Kelley et al.'s [10], Balebako et al.'s [46] and Egelman et al.'s [47]. Here I give a brief overview of the parts that I adapted from each work.

Balebako et al.'s [46] work was intended to raise awareness of data leaks on smartphones. They provide an interview script that they used during their recruiting. I used the same introduction part of the script but used questions of my own that fit the purpose of my study by focusing on the Android platform.

Egelman et al.'s [47] did an empirical study to test the effectiveness of web browser phishing warnings. One of their research questions was to determine if users would notice a warning indicator. What I did is that I adapted this question to look to see if users notice "Permission Details" icon during the app installation time.

Felt et al.'s [22] was among the first work that looked into the Android permission system (in 2012). They looked at the users' attention, comprehension and behavior in the permission interface of Android version 3.0. That version is the old interface that I cover in Chapter 2. I adapted the idea of doing an explanatory lab study and also the time that is required to do a study was from 30-60 minutes, which is what I did. Moreover, in my work I asked similar question if users notice or consider permissions before installing an app. Furthermore, Felt et al.'s [20] in their online study, they asked participants three comprehension questions by given them a permission label and some possible answers in addition to "None of the above" and "I don't know". They use these two options to detect any false responses. What I did is that I adapted the same criteria with some modifications. The modifications I made are: I did asked participants to choose the right permission group of a given permission label. I also included the "None of the above" and "I don't know" options. In addition, I followed their criteria in scoring the results of the multiple questions by grading accordingly to (all correct, all incorrect, at least one correct, more than one incorrect) as well as scoring the participants scores using the absolute scale of answering the questions without having any extra incorrect answers.

Kelley et al.'s [10] modified the Google store interface and include Privacy Fact section that shows what is the app accessing and shows that to users. I described the Privacy Fact section in section 2.5. Kelley et al.'s did a lab study to test the modified version on of Google store. They used semi-structured interviews, which is exactly what I did. They outline their lab study as: Android introduction, general new smartphone advice, specific new smartphone advice, application-selection task and post task explanation task [10, p.128]. I also used their six scenarios, which I describe in Section 3.3.1.1. I include neither their "Android in the news" nor "malicious activity" parts. I also the same demographic information that they used as can be seen in Section 3.3.1.2.1. However, I did not include the occupation, telephone provider and number of apps that users did use.

3.3.1 Study Overview

The first step is an observation study with semi-structured interview. This step covered the pitfalls that users should avoid while using Android. Also, it covered the application selection task by looking at the steps that users take and the factors they considered while searching for an app. Moreover, it showed users' behavior and decision towards considering permission during the installation process, and if users they were aware of the "Permission Details" icon. Another aspect covered in this step was asking users about the "Auto Update", specifically whether it is on or off and their reasons behind their choice. Also, the interview provided some insights into when users do check permissions and if they were interested to find explanations for the requested permissions and the places that they would use to check them. In addition, it showed users' opinions about the current permission presentation and the changes that they wanted to the permission system and Google Play Store in general.

The second step is filling a post-online questionnaire. This step covered collecting users' demographics, background and Android usage information. It was used also to classifieds participants into two classifications. First, advanced versus novice users based on security courses. Users who did not take any security course are considered novice user. Second, Westin's metric, which divided participants into three groups: Privacy Fundamentalists, Pragmatists and Unconcerned. Moreover, it looked at the stores that users use to search and download apps and if they were willing to try apps from unfamiliar brands and their reasons for doing so. Also, if users were familiar with the term "Android Rooting", what does "App Ops" mean, if users were installing the latest firmware and if they were using any security software and whether they think having such a software is essential to have or not. It also asked participants multiple questions that covered choosing the correct permission group to a given permission label to see whether the old or new naming of permission groups are better.

Together both steps took between 30-60 minutes to complete. To test my hypothesis, I conducted my study during October and November of 2015. For the number of participants, I considered Felt et al.'s [22] study as well as Kelley et al.'s studies [24, 32]. The number of participants in their studies was between 20–25. However, since the collected data is a mix of qualitative and quantitative, Green and Thorogood suggested that 30 or more are needed to get quantitative data [48]. I was looking to recruit 35 participants including Faculty/Staff/students from the Faculty of Computer Science at Dalhousie University. I recruited 26 students. I was not allowed to send any recruiting e-mail message to the Faculty/Staff members due to complaints from them about receiving too many e-mail notices. Participants were recruited through the undergraduate and graduate e-mail lists. Two restrictions were applied to be eligible to participate; the participant's age was at least 18 years old and should own an Android smartphone. All of the Participants signed an informed consent form and received $10 honorarium/compensation for their participation. They were informed of their right to withdraw without penalty at any time during the study.

3.3.2 Demographics

	Age	Education	Phone Model	Android OS	Time Using Android
ID1	18-22	High school	LG e973	**4.4.4 (PacRom)**	2-4 years
ID2	23-30	Master's degree	Samsung S4	I'm not sure	1-2 years
ID3	23-30	Master's degree	MOTO G2	5.x – Lollipop	2-4 years
ID4	23-30	Bachelor's degree	HTC one	5.x – Lollipop	5 years or more
ID5	23-30	Bachelor's degree	Samsung S4	5.x – Lollipop	2-4 years
ID6	23-30	Bachelor's degree	Google Nexus 4	5.x – Lollipop	2-4 years
ID7	23-30	Bachelor's degree	Sony Xperia Z2	5.x – Lollipop	5 years or more
ID8	18-22	High school	Asus Zenfone	5.x – Lollipop	7 months-1 year
ID9	18-22	Some college	Sony	5.x – Lollipop	5 years or more
ID10	23-30	Master's degree	HTC M9	5.x – Lollipop	5 years or more
ID11	18-22	High school	**LG Nexus 5**	**6.0- Marshmallow**	5 years or more
ID12	18-22	High school	Nexus 5	5.x – Lollipop	1-2 years
ID13	31-40	Bachelor's degree	Galaxy Note 4	5.x – Lollipop	2-4 years
ID14	23-30	Bachelor's degree	Nexus 4	5.x – Lollipop	5 years or more
ID15	23-30	Bachelor's degree	Samsung	5.x – Lollipop	2-4 years
ID16	18-22	High school	Samsung Galaxy s5	4.4 – Kit Kat	2-4 years
ID17	23-30	Bachelor's degree	Samsung Galaxy S3	4.4 – Kit Kat	1-2 years
ID18	23-30	Bachelor's degree	Moto X Play	5.x – Lollipop	Less than 6 months
ID19	23-30	Bachelor's degree	**Nexus 5**	**6.0- Marshmallow**	2-4 years
ID20	18-22	High school	LG Nexus 5	5.x – Lollipop	1-2 years
ID21	18-22	High school	Samsung s6	5.x – Lollipop	5 years or more
ID22	18-22	Bachelor's degree	Samsung S5	5.x – Lollipop	2-4 years
ID23	18-22	Bachelor's degree	Samsung grand	4.4 – Kit Kat	1-2 years
ID24	18-22	Bachelor's degree	**Google Nexus 5**	**6.0- Marshmallow (Custom Rom)**	2-4 years
ID25	***	Master's degree	Huawei	I'm not sure	2- 4 years

ID26	18-22	High school	Samsung Galaxy Grand Prime	5.x – Lollipop	1-2 years

Table 3:Basic demographics and Android Information of our lab study. All the information above was self-reported. The age of participant 25 was not disclosed. ID1has a custom ROM. ID11 and ID12 has Android 6.0. ID23 has a custom Android 6 ROM that has the new revised Permission system (Android M).

As shown above, 96% of our participants were males and only one female. Twelve participants were between 18−22 years old, 12 between 23−30, 1 between 31−40 and one was not disclosed. Thirty-four percent were undergraduate, 65% were graduate students. Eleven percent were PhD students, 50% Master's students and one participant has two master's degrees but is currently studying for a bachelor degree in computer science.

3.3.3 Types of Study

3.3.3.1 Observation Study with Semi-Structured Interview

The main goal of the observation lab study was to ask participants semi-structured questions to seek broad understanding of how participants interact and select application from the Google Play Store. Also, looking at the surrounding issues of viewing permissions before and after installing applications. Participants were given a smartphone to perform a set of tasks that will be described later. The semi-structured outlined format was adapted from Kelley et al.'s [32] and Felt et al.'s [22] with some minor modifications (as described above) . It consisted of the following 6 parts:

1- **Interview script:** this script was adapted from Balebako et al.'s [46]. This script was meant to give the participants general information about the study, the interviews were audio-recorded as well as their interactions of the given smartphone and be video-recorded. Also, to ensure that their data was anonymous and their identifying information is stored separately from their comments. Most importantly, I structured them to think aloud while doing the tasks. The complete script can be found in the Appendix A1.

2- **“Android introduction”**: I asked participants some general and basic questions about their experience using their Android phones as well as the reasons behind choosing Android. For example, is it because of the technical features, or they like to look of Android phones, or the apps that Google Play Store provides. This introduction serves dual purpose of creating a welcoming dialog as well as gauge their understating and familiarity of using the Android System.

3- **“General new smartphone advice”**: I then asked participants to think about a hypothetical friend who has just got a new brand smartphone who is less-tech savvy and give him/her a general advice. Also, if there were any “pitfalls that they should avoid” and the “applications that every smartphone user should have”.

4- **“Specific new smartphone advice”**: then I continued the same scenario of their friend but now he/she is asking for their help to find two specific applications that were selected from 6 different scenarios:

a- “Word games for killing time— ‘I really like word games like Scrabble, but it would be great to have a few things on there for when I need to kill time’.”

b- “Nutrition/Health— ‘I keep dieting but an app that helped me keep track of calories would be great’.”

c- “Music— ‘I like to listen to music but don’t have a large music collection myself’.”

d- “Scanning receipts— ‘I frequently have to travel for work, and am so bad about keeping all my receipts together, is there an app that helps me scan in may receipts and save them’.”

e- “Twitter— ‘My friends keep telling me I should use Twitter more, and I do like to follow some celebrities with it, but I don’t just want to use the main Twitter app’.”

f- Flight tracking— ‘I fly a lot, but I still get a bit anxious and I want to be able to track my flights’.”

Then I asked them if they have any specific advice or an application in mind that they would suggest, to their hypothetical friend that matches the above six scenarios. The order presentation of the scenarios was selected randomly without counterbalancing. In the case that a participant had issues with a given scenario (for example, the participant did not understand the scenario or could not think of an answer that they were satisfied with), another of the six scenarios was used. Recall that participants answered at most two scenarios. When participants did not suggest any application, I would ask them about the strategy that they follow to find an application for the chosen scenarios.

5- **Application-selection task:** After verbalizing their suggested application and strategies, I provided them with OnePlus One smartphone operated by a custom Android Lollipop 5.1.1 CyanogenMod, which I said this is your friend's new smartphone. This phone has a built-in application called ScreenCast to video-record users interactions during the tasks. It also shows the areas that where participants touched. During the application search process, I asked participants to use the "think aloud" technique while they using the Google Play Store. Also, I instructed them as well to tell me what they were reading and considering while selecting and installing the two apps. Moreover, I observed what user interface elements they interacted with.

6- **Post-explanation task:** I asked participants a few questions such as: Why they choose the application that they did and what they would have done differently in their life? Also, if participants did not consider or notice permissions during the installation, I asked them for their opinion after the installation task.

I change the experiment while it was in progress by eliminating some aspects that, although they worked in pilot testing, did not work in practice. Specifically, I showed 3 participants the Permissions screen of an application and asked them by verbalizing the term permissions if they considered them before installing an app or after and the reason of that? The reminder of participants were shown the new permission screen (Android OS v.5) but without verbalizing the term permissions to gauge their understanding if they know the exact term of the Permission screen. Some participants did not know what the permission screen mean by saying it is a confirmation screen or “Terms of Service”. Other participants clearly stated that it was a permission screen of what is going to be accessed in the hardware device. However, I discarded this question from the analysis because it did not show any valid results in terms of their permission awareness.

I asked participants if the “Auto Update” is turned on or off and their reasons for doing so. This question is adapted from Sanders et al.’s [34], however, I extended it by also asking participants for the reasons behind their choices.

Moreover, I asked them if they would check the permission changes after receiving an update to see if they are willing to check them or not.

Furthermore, I want to know from where they would get answers if they seek further explanation of permissions where they would go: are they going to look for them within the Google Play Store or they will navigate the Web, online blogs? This question is adapted from Felt et al.’s [22].

Then, I asked them if they could tell me how they want the permissions to be presented to be clearer and easier to understand. Finally, I asked participants if they want to see any changes or features in the near future on Google Play Store. This question would help uncover any issues that bother participants while navigating the store.

3.3.3.2 Post Online-Questionnaire

The online questionnaire was developed using Dal Opinio software [49]. There were a total of 37 questions. Every participant answered 25 questions: twenty-two questions covered collecting demographics, background, and Android usage information; a further three, multiple-choice, questions were selected from a set of 15 questions. The survey software based on participant's ID number did the selection of those three questions. These three questions were about choosing the correct Permission Group to a given permission. These questions were not equally distributed and they were not selected randomly because participants could identify some of the answers from other questions. I assigned the participant ID numbers so that the questions would be consistent with the permission group that the participant had been asked about earlier.

Moreover, this questionnaire helped to differentiate between the different groups of users. The complete questionnaire can be found in Appendix A2.

3.3.2.2.1 Questionnaire Questions

This section describes in details the most important questions that were used.

Participants were asked Q8 to look from which store, would users search and download their applications. They rated them based on their favorite store on a scale of 6 (least important) to 1 (most important) and if_they do not know any of them, they can leave it blank. Users can install applications from official stores such as Google Play Store; or unofficial stores such as AppBrain, Amazon App Store, GetJar, SlideMe and from any websites. The importance of the download source would "influence the availability of the security-relevant information" that users can access before installing applications.

Also, Q9 were asked to put 13 application installation factors into 3 categories: always consider, sometimes consider, and never or rarely consider. They also rate these factors in Q10 that might be considered when downloading applications on a scale of 1 (most important) to 13 (least important). "The self-reported factors that influenced participants' installation decisions were: price, popularity of app, search ranking/sponsored listing, user reviews, expert reviews online (blogs, magazines, etc.), salesperson suggestions in a store (like BestBuy), friends' recommendations, familiarity with brand, ease of installation, screenshots, End User License Agreements and Terms of Services, the application's privacy policy, permissions and "Other" for any additional factors". My goal is to "understand how and why users decides to install applications" so I can identify the most important "key points in the decision process" and what can be done to improve it.

Question 11 were asked to gauge participants' willingness of installing and trying an application from unfamiliar brand or company. The brand name of an application "can act as a security signal" and applications from familiar brands "are less likely to be malware or grayware" [2]. I extended Q11 of the previous work on [2] by asking participants their reason of installing application from unfamiliar brands or company.

Question 14 was previously asked in the interview part but I wanted to give participants more freedom to write down their reasons of turning Auto Update on or off on Google Play Store [34].

Question15 was to look if participants are familiar with the term Android "Rooting". Participants were asked to write what the term means. "Rooting" in Android is an equivalent term to "jailbreaking" in iPhone. It gives you an access for extra features, system settings, allow/deny permissions, different look, and speed enhancements that are locked by the system developer like Google and smartphone manufactures. Only experienced users are able to root their devices because it consists of following multiple steps of unlocking the operating system and then flash a new custom ROM. If anything happens during flashing the ROM, there is a risk of bricking the smartphone, that is, rendering it unable to function or turn on at all. Also, doing that voids the warranty of the phone [50].

Question 16 was to investigate if participants are aware and know if they are running the latest update of the firmware or the operating system.

Similarly, Q17 was to further look into if participants are using any security software in their smartphones and/or PC/laptop or none.

Moreover, Q18 asked participants if they consider using security software are essential [9].

Question 19 asked about a hidden app called App Ops and see if they are aware of what this app can do and what do does it mean. Simply, App Ops is an app that gives the smartphone user the ability to allow/deny application permissions after installing an application. This question is also intended to look if they are using any type of such software.

Question 20 was used to differentiate between advanced and novice users. The criterion was adapted from Bravo-Lillo et al.'s [51] work, which said: "users who took at least one computer security course or privacy graduate course are considered advanced user. Moreover, "past studies found that even lower levels of expertise are sufficient for making significantly better security decisions". Users who did not take any security course are considered novice users [51].

Question 22 was to gauge general understanding of how participants are privacy sensitive; and to do that, Westin index was used [52]. Participants were asked to "rate three statements using a 5-point Likert scale from ("I strongly disagree" to "I strongly agree")". The three statements are:

1- Consumers have lost all control over how personal information is collected and used by companies.

2- Most businesses handle the personal information they collect about consumers in a proper and confidential way.

3- Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Next, I used Westin's metric to classify them accordingly. "Privacy Fundamentalists are participants who agreed (strongly or somewhat) with the first statement and disagreed (strongly or somewhat with the second and third statements". "Privacy Unconcerned are those who disagreed with the first statement and agreed with the second and third statements". The remaining of participants was considered as "Privacy Pragmatists". The Privacy Fundamentalists are considered "at the maximum extreme" regarding their privacy concerns. Also, they are most protective about their privacy. They feel that their personal information should not be acquired and needed by companies/organization and think as individuals that they "should be proactive in refusing to provide information. Moreover, they support strong individual's privacy laws. Privacy Unconcerned "are the consumers with the least protective of their privacy" and they feel that sharing their information with companies may help them to receive benefits. They also think that there are no potential abuses of their information and they do not support expanding the laws and regulations of protecting their privacy. The last group is Privacy Pragmatists who weigh sharing their personal information by looking at the pros and cons of doing so. Also, they evaluate the regulation and laws that are used by companies to see if they can be trusted or not. In addition, after these careful consideration, they may decide if doing that "make sense for them" to share their personal information [52].

The final questions were multiple choices. Participants were presented by a Permission Label such as: Record Audio and then been asked to choose and check all the Permission Categories/Groups that this permission is belong to. I wanted to know how would advanced and novice users do. Can they choose correctly? Are they going to choose the both correct Permission Group of the old view and the current one? Which one seems more appealing to the participants to choose from? Every permission question has two correct answers. Also, the Permission Group "Other" was included in some questions if that permission label was found under it. For example, the permission "Write you Web Bookmarks & History" appears under the permission group "Other" in the current design and in the old design it appears under the permission group "Bookmarks & History". However, the "Read your Web Bookmarks & History" appears in the current design under the permission group "Device & App History" and in the old view appears under the "Bookmarks & History". Moreover, two more options were included to make every question optional and to avoid false responses. It is important to note that, users were shown the permission screen during the post-explanation task to get their feedback about the current design in general. They were asked the permission label questions at the end of the online questionnaire but they were not permitted to look at the permission screen while answering these questions. I believe that showing them the permission screen in the post-online questionnaire could not influence them to answer the permission label questions because there was a time gap between looking at the permission screen and answering the permission labels multiple questions. The participants answered 22 questions before getting to the permission label questions.

Permission Label	Permission Groups/Categories
Write your Web Bookmarks & History	✗Device & App History ✓Other ✓Bookmarks & History ✗None of these I don't know
Read your Web Bookmarks & History	✓Device & App History ✗Other ✓Bookmarks & History ✗None of these I don't know
Read Your Contacts	✗Phone ✓Your Social Information ✓Contacts ✗None of these I don't know
Create Accounts and Set Passwords	✗Your Application Information ✓Other ✗None of these ✓Your Accounts I don't know
Change Your Audio Settings	✗Microphone

	✓Audio Settings ✓Other ✗None of these I don’t know
Connect and Disconnect from Wi-Fi	✓Network Communication ✗None of these ✗Wi-Fi connection Information ✓Other I don’t know
Read Your Own Contact Card	✓Identity ✓Your Personal Information ✗Contacts ✗None of these I don’t know
Find Accounts on the Device	✓Identity ✗Other ✓Your Accounts ✗None of these I don’t know
Read Your Social Stream	✓Your Social Information ✗Device ID & Call Information ✓Other ✗None of these I don’t know
Prevent Phone from Sleeping	✗System Tools ✓Other ✓Affects Battery ✗None of these I don’t know
Read Calendar Event Plus Confidential Information	✗None of these ✓Calendar ✗Your Social Information ✓Your Personal Information

	I don’t know
Google Play Billing Services	✓Network Communication ✗Your Application Information ✓In-app Purchases ✗None of these I don’t know
Read Contents of Your USB Storage	✗Other ✓Storage ✗None of these ✓Photos/Media/Files I don’t Know
Read Phone Status & Identity	✓Phone Calls ✗None of these ✗Identity ✓Device ID & Call Information I don’t know
Read Call Log	✗System Tools ✓Phone ✗None of these ✓Your Social Information I don’t know

Table 4: The complete set of permission labels with the correct Permission Group.

3.3.3 Type of Analysis

This section describes the analysis method that I followed on analyzing both the semi-structured interview and the online questionnaire in details.

3.3.3.1 Aggregation Process

The collected data is a mix of qualitative and quantitative measures. There are four phases that outline the method that I followed to convert the raw data from the two parts of the study into a solid result. I followed the methodology guide from Ranjit Kumar's *Research Methodology* book [53].

Phase 1: I transcribed all the 26 interviews into Excel spreadsheets and Word documents. Also, I downloaded all the raw and statistics data as well as all the reports from the Dal Opinio Software. Also, I identified the broader main themes carefully by going through the descriptive responses given by the participants during the interview. I went through all the data to identify these themes by looking at keywords until I reached a saturation point that give me the ability to assign codes to the themes I had identified.

Phase 2: to classify participants' responses I assigned codes to the identified themes based on how frequently the theme had occurred and the number of counts. Also, all the participants were classified into two groups: novices and advanced users. only participants who took at least one security course, are considered to be advanced users. There were 15 Advanced users and 11 novice users. Then, I used Westin's metric to classifieds the participants. There were three groups: 4 Privacy Unconcerned users, 16 Privacy Pragmatists and 6 Privacy Fundamentalists. We found out the using Westin's metric showed a stronger relationship with various measures of security better than using novices versus advanced based on taking security courses. It showed the real sense of the gathered data.

Phase 3: there were themes or factors found by more than one participant. Some of the themes/factors are left without merging/collapsing the data into other themes. Since there are some factors that did not have enough number of counts to be independent themes, they were grouped into broader theme to represent and make sense of data more accurately. For example, there were 14 pitfalls themes that were reported by participants, I grouped them into three themes that cover all the reported cases: Memory Limitation, Open Source issues and Security Settings. Another example, there were 11 explanation themes that were reported by participants when looking for permission explanations when installing an application. They were grouped into four categories: check within Google Play Store, Google it/Website, Do not Care and Phone Settings. I also added some of the participants' quotes to give and illustrate an example for each theme. Some of the quotes have more than one reported theme/factor.

Phase 4: regarding correcting the multiple questions of choosing the correct permission group of a given permission label, I used what Felt et al. [4] used to score respondents scores. There were two correct choices for each question. One represents the old naming of permission group and the other one represent the new naming. I categorized their responses to: correct, incorrect, at least one correct for the old or new permission group naming, and extra incorrect for the old or new permission group naming. I also followed the same process of classifying them using the novice/advance user metric and then the Westin's metric and reported their scores.

Phase 5: integrate the report results, perform statistical analysis and write final conclusions. I used a simple two-group *t*-test using two codes: 1 for considered and 0 if not considered. Also, I calculate the mean, the standard deviation and correlation (often called Φ-coefficient also known as the phi-coeffient).

The following description is from Howell [54].

For, the correlation, the Pearson correlation calculated when both variables are binary (coded 0 and 1) is functionally the same as the Φ-coefficient. In fact, the coefficient is also the same as the X^2 analysis when the data is presented as a 2×2 contingency table. That is, Φ^2 = N× X^2. Hence, the current analysis is functionally the same as a Φ-coefficient or a X^2 analysis calculated.

The *t*-test of the current data, compares the difference between proportion of participants who endorse each item (answer, action) as a function of group. This is functionally equivalent to a X^2 analysis for group by response ("yes" versus "no"): for two groups, this is a 2×2 X^2. The data fundamentally follows a binomial distribution (number of "yes" versus number of "no" answers, as a function of group). One can use a X^2 or t-test to analyze such data. In statistics, they are very closely related. For use of either the t-test or X^2, there is some discussion in the literature about the necessary sample size, but Howell's review implies that type-I error is not an issue so long as the total sample size exceeds eight. Fundamentally, the goal of this research is to make inferences about the population proportions [54].

3.3.4 Complete List of Questions

This section described an example of the all the asked questions during the observation lab study from the moment the participant arrived. The questions are presented in the following list:

1- Android introduction:
   a- Can you tell me why did you choose to buy an Android Phone? Is it for technical features? The apps or liked the look or others?
2- General new smartphone advice:
   a- What advice they would give to a hypothetical friend, someone less tech-savvy, who has just gotten a brand new smartphone?
   b- What pitfalls they should avoid?
   c- What applications every smartphone user should have?
3- Specific new smartphone advice:
   a- Participants were asked to think about the same friend and this friend is asking them to look for two specific applications.
   b- I asked participants if they have a specific advice or a suggested for the given scenarios.
   c- If they were not sure, I asked them what is their strategy for finding an application for the category would be?
4- Application selection task:
   a- After participants verbalized their suggested application and strategies, I gave them a Google CyanogenMod smartphone saying this is your friend phone.

b- I asked them to think out loud while using Google Play Store.

c- I instructed them to tell me what they were reading and considering while selecting and installing an app.

d- I observed the elements that the participants interacted with.

5- Post-explanation task:

a- I asked participants why they did choose the application that they did?

b- What they would have done differently in their life if they are using their own smartphones?

c- If participants did not consider permissions during the installation, I asked them for their opinion towards permissions after the installation task.

d- Do you check permissions before installing an app or after and why?

e- Is Auto Update on or off and why?

f- Would check the permissions after receiving an update?

g- Where would you go if you want to check for permission or look for explanations? Are they going to look for it within the Google Play Store? Or they will navigate the web or the online blogs.

h- Can you please tell me how would you want the permissions to be presented to you to be clear and easy to understand?

i- What are the changes or features that you want to see on Google Play Store?

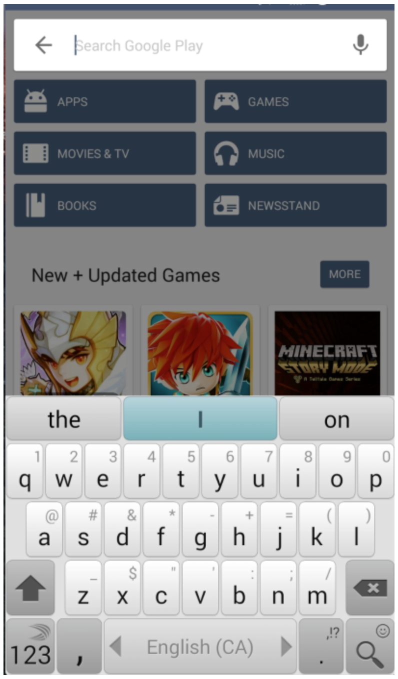
j- Can you please fill up the online questionnaire?

6- The complete list of the questionnaire questions is available in Appendix A2.

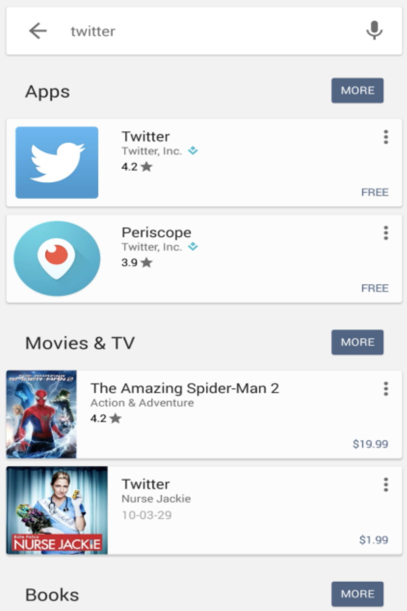
3.3.5 Screenshots of How a User Select an App

This sections shows a complete walkthrough steps that one of the participants took to install an app. It shown as follows:

1- Participant opened the Google Play Store.



2- Used the search bar to write twitter


twitter

Apps MORE

Twitter
Twitter, Inc.
4.2 ★
FREE

Periscope
Twitter, Inc.
3.9 ★
FREE

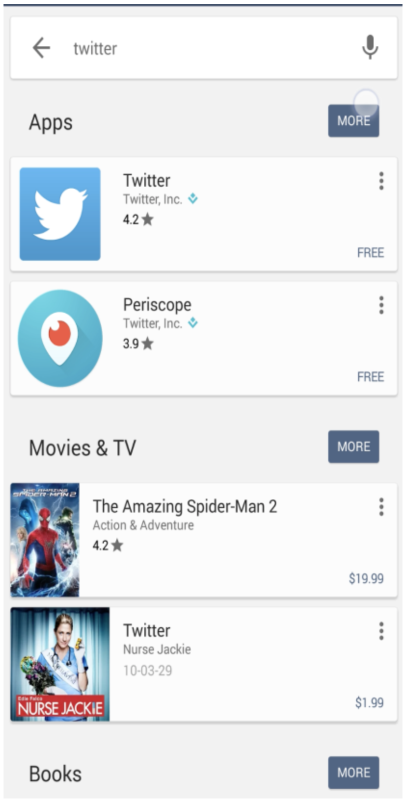
Movies & TV MORE

The Amazing Spider-Man 2
Action & Adventure
4.2 ★
$19.99

Twitter
Nurse Jackie
10-03-29
$1.99

Books MORE

3- If I do not want to use the main Twitter app, I press the more button instead of going to the official one.



twitter

Apps MORE

Twitter
Twitter, Inc.
4.2 ★
FREE

Periscope
Twitter, Inc.
3.9 ★
FREE

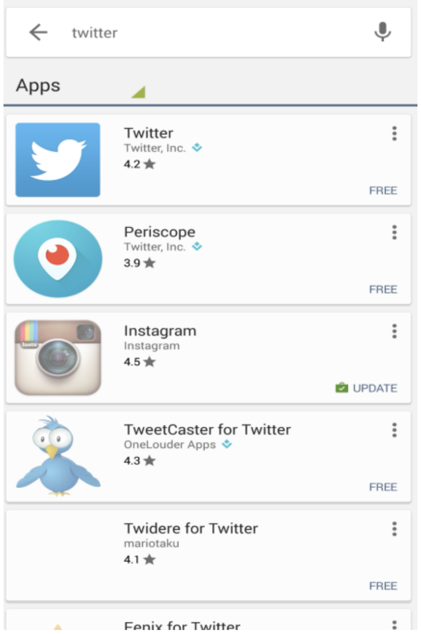
Movies & TV MORE

The Amazing Spider-Man 2
Action & Adventure
4.2 ★
$19.99

Twitter
Nurse Jackie
10-03-29
$1.99

Books MORE

4- After pressing the "more" app button, then I can scroll down to see some other options such as: Periscope or TweetCaster for Twitter.



twitter

Apps

Twitter
Twitter, Inc.
4.2 ★
FREE

Periscope
Twitter, Inc.
3.9 ★
FREE

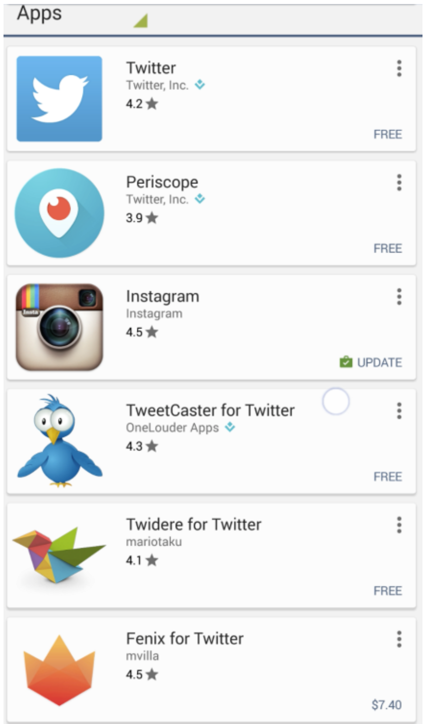
Instagram
Instagram
4.5 ★
UPDATE

TweetCaster for Twitter
OneLouder Apps
4.3 ★
FREE

Twidere for Twitter
mariotaku
4.1 ★
FREE

Fenix for Twitter

5- So, I will look at the TweetCaster because it has 4.3 rating which is pretty high.



Apps

Twitter
Twitter, Inc.
4.2 ★
FREE

Periscope
Twitter, Inc.
3.9 ★
FREE

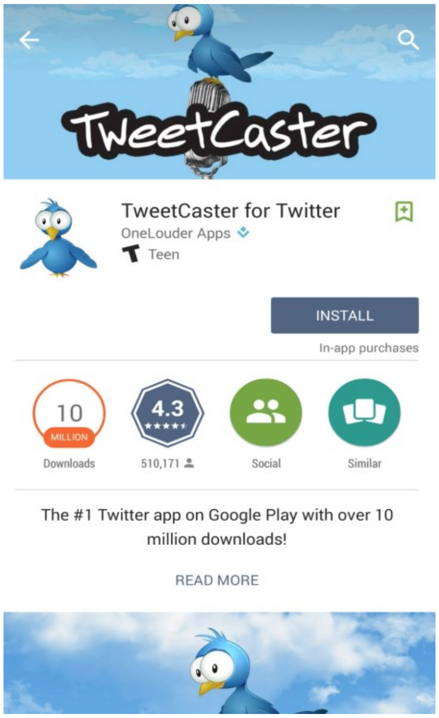
Instagram
Instagram
4.5 ★
UPDATE

TweetCaster for Twitter
OneLouder Apps
4.3 ★
FREE

Twidere for Twitter
mariotaku
4.1 ★
FREE

Fenix for Twitter
mvilla
4.5 ★
$7.40

6- After clicking on the TweetCaster for Twitter.



TweetCaster for Twitter
OneLouder Apps
Teen

INSTALL
In-app purchases

10 MILLION
Downloads

4.3 ★★★★★
510,171

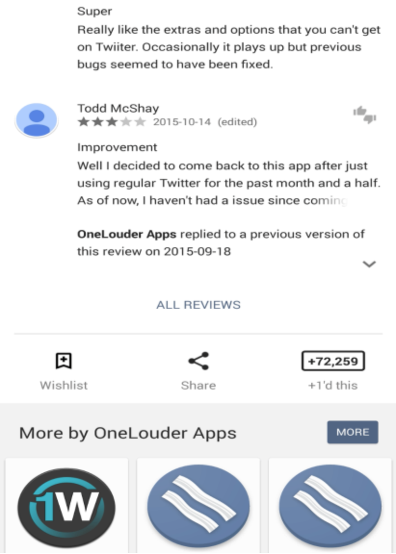
Social

Similar

The #1 Twitter app on Google Play with over 10 million downloads!

READ MORE

7- I can see from the number of downloads it is quite popular, it is 10 million downloads, and now I'm looking through reviews and most of the people seems to like it. I don't usually read all the reviews.



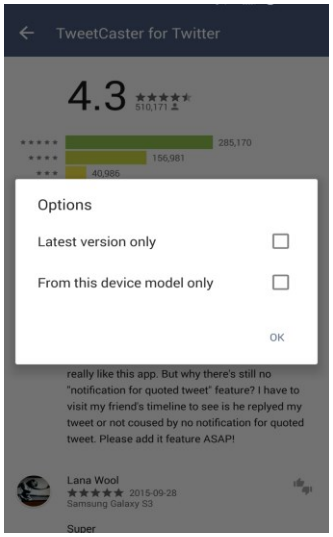
Super
Really like the extras and options that you can't get on Twiiter. Occasionally it plays up but previous bugs seemed to have been fixed.

Todd McShay
★★★☆☆ 2015-10-14 (edited)

Improvement
Well I decided to come back to this app after just using regular Twitter for the past month and a half. As of now, I haven't had a issue since comin

OneLouder Apps replied to a previous version of this review on 2015-09-18

8- Usually what I do is I press all the "All reviews button" and from review sorting option and press latest version only and check that because sometimes people are not really happy with the application because of the recent update that they did not like and if I'm downloading it now, I want to make sure that I'm looking at the reviews of what I'm downloading. Also, sometimes I check "From this device model only" because sometimes your phone is not compatible with the app and you want to know that beforehand.



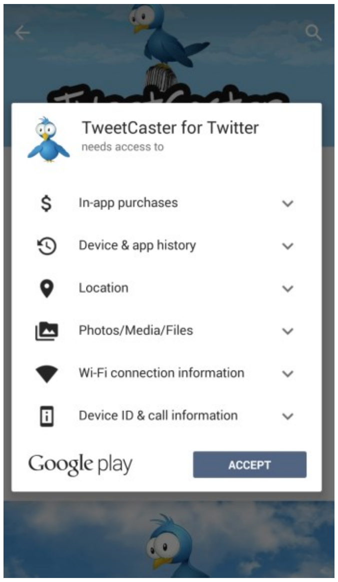
Options
Latest version only □
From this device model only □

really like this app. But why there's still no "notification for quoted tweet" feature? I have to visit my friend's timeline to see is he replyed my tweet or not coused by no notification for quoted tweet. Please add it feature ASAP!

Lana Wool
★★★★★ 2015-09-28
Samsung Galaxy S3

Super

9- Then, I would install the app. The participant immediately clicked “Accept” to begin installation of the app.



TweetCaster for Twitter
needs access to

In-app purchases
Device & app history
Location
Photos/Media/Files
Wi-Fi connection information
Device ID & call information

CHAPTER 4: RESULTS

In this section, since the results of both parts are related, they will be described and integrated together in proper section that represents them. I discuss the results of how would users interact and select application from the Google Play Store and the surrounding issues of viewing permissions and what users' needs and concerns. With regards to the reported themes/factors, each of them are analyzed using two classifications: one is based on Westin's metric and the second is the advanced/novice users'. Also, for some issues I did use both classifications to interpret the results. Moreover, no classifications were used when there is no enough data. Using Westin's metric added a higher level of abstraction of the results. It is important to note that, I described the majority of results using the first classification. I did not go into details using the advanced/novice classification because of it did not represent the data as it should be and it was a failure.

4.1 HYPOTHESIS TESTING

I discuss the results of my hypotheses in general. Later on I discuss them in detail under the proper section. One of my research questions was if users are aware of the added "Permission Details" icon which is located at the end of the app page. It appeared that only two users (ID7 and ID8) comprising 8% of the population) were aware of "Permission Details". They also clicked on it to find more about the required permissions. There was not enough data to test all the subsequent hypotheses. Neither of them did click on the "Learn More" link that appears at the bottom of the "Permission Details" icon. ID7 and ID8 were both aware of the "Other" permission group, which is hidden from the permission screen during the application installation process. As stated earlier, this permission group only appears under the "Permission Details" icon. The previous finding validates what Akhawa and Felt [31] reported in their study that "users rarely click on explanatory links" and "designer should not hide important details" in the process of making a decision. Also, these finding are supported by Gerber et al. [18] report in which they stated that users who have concerns about permissions have to take "the complicated access route" to click on "Permission Details" icon and "users are not expected to initiated the search process of another screen in order to find" the full list of the requested permissions.

4.2 WESTIN'S METRIC CLASSIFICATION

Under this classification, I looked into the factors that participants considered when downloading an application during the application selection task.

4.2.1 Factors Considered when Downloading an App

Table 5 shows the factors considered by participants' when downloading an application. Generally, there were some similarities among some factors such as: looking at reviews, rating, reading the full app description, checking the app features, avoid app with ads and if they knew the app.

What was interesting that, the Privacy Fundamentalists are not concerned about the application cost (r=–0.5). Also, with regards to the reasonable permissions, the Privacy Fundamentalists and the Pragmatists do care and look at the permissions when installing an application (r=0.3). This shows clearly the Privacy Unconcerned group do not care about their personal information. For example, ID10 stated: *"I would say what permissions it needs and I see what it needs. It needs access to Photos/Media/Files and Camera which both make sense to me. I would "accept that". Where if it needs something like accessing my contacts. Or something, then I would be little more suspicious what is trying to do and why. If I saw something like that, I would go back. Read through the description carefully".* More interestingly, some of the participants related permissions to the concept of the features that the application has. ID14 stated*:" I don't accept directly. I'll look for what this app is going to access. If I'm comfortable. Yeah pretty comfortable of letting the app accesses all these features on my phone".* ID5 read the permission screen and said this is fine and he hit accept.

He further explained the reason for looking at permission saying: “I *was just checking permissions whether is the app is asking for Kernel permissions”.* The Kernel permissions give the access to the Android Operating System and it can brick the phone. ID1 (Privacy Fundamentalist), ID12 and ID23 (Privacy Pragmatists) stated that the required permissions are needed for the application to work without having limitation and they will not be able to tell what sort of things this application requires.

Another surprising results was that 33% of the Fundamentalists group were aware of a quick shortcut to go directly to the reviews section without scrolling down. What they did was, they clicked on the rating icon as Figure 8 shows.

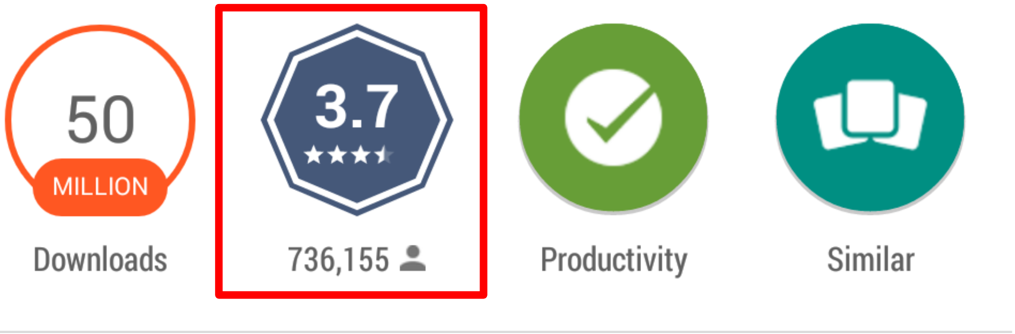


Figure 8: Ration icon appears above the short app description.

Factors Considered	Mean UN	Mean PR	Mean FU	SD UN	SD PR	SD FU	*r*
1-Blue Sign	0.25	0.06	0.33	0.50	0.25	0.52	0.153
2- Rating	1.00	0.56	0.67	0.00	0.51	0.52	-0.228
3-Number of Downloads	0.75	0.31	0.83	0.50	0.48	0.41	0.070
4- Popular	0.25	0.44	0.67	0.50	0.51	0.52	0.210
5-Reviews	1.00	0.75	1.00	0.00	0.45	0.00	0.029
6-Number of Reviews	0.25	0.19	0.33	0.50	0.40	0.52	-0.033
7-Rating Icon	0.00	0.00	0.33	0.00	0.00	0.52	0.473
8-Read Full Description	0.25	0.44	0.33	0.50	0.51	0.52	0.082

9-Read Short Description	0.25	0.06	0.17	0.50	0.25	0.41	-0.025
10-Features	0.25	0.25	0.17	0.50	0.45	0.41	-0.038
11-New Section/Updated version	0.00	0.06	0.17	0.00	0.25	0.41	0.227
12- Latest App version/When it's Updated	0.25	0.00	0.17	0.50	0.00	0.41	-0.020
13- Reasonable Permissions	0.00	0.50	0.50	0.00	0.52	0.55	0.345
14-Free	0.75	0.25	0.00	0.50	0.45	0.00	-0.488
15-Similar Apps	0.25	0.31	0.17	0.50	0.48	0.41	-0.042
16- Negative Reviews	0.50	0.38	0.33	0.58	0.50	0.52	-0.055
17-Find my Solution	0.00	0.25	0.00	0.00	0.45	0.00	-0.029
18-Google it	0.00	0.13	0.00	0.00	0.34	0.00	-0.020
19- Screenshots	0.75	0.38	0.50	0.50	0.50	0.55	-0.064
20-App Logo	0.00	0.25	0.17	0.00	0.45	0.41	0.134
21-Avoid Ads	0.25	0.25	0.17	0.50	0.45	0.41	-0.038
22-Knew the App	0.25	0.13	0.17	0.50	0.34	0.41	-0.029
23-Quick Install	0.00	0.19	0.00	0.00	0.40	0.00	-0.025
24-Categories	0.25	0.06	0.17	0.50	0.25	0.41	-0.025
25-Install/Try it	0.50	0.38	0.00	0.58	0.50	0.00	-0.332

Table 5:Factors considered by participants when installing an application. UN (Privacy Unconcerned), PR (Privacy Pragmatists) and FU (Privacy Fundamentalists). *r* (correlation).

Another interesting result was that none of the Privacy Fundamentalists and Unconcerned would use Google to find more about the app. Also, the Privacy Unconcerned group did not consider looking at the App Logo to install an app. Twenty-five percent of the Privacy Pragmatists and 17% of the Privacy Fundamentalist would consider looking at the App Logo. ID8 stated: *"Yeah it looks professionally. Especially. If it has the look of that it was designed by a graphical designer. Something like that. They have been more committed on their applications than some odd screenshots".*

Moreover, none of the Privacy Fundamentalists would install the app and try it without looking at app description page.

Also, the percentage of viewing negative reviews was slightly higher among the Privacy Unconcerned than the other two groups. ID 5 stated why he would look at the one or two stars' reviews: *"The 5 stars I can assume that he is a friend of someone.*

He might just give it. These guys who hate him or are the true to these reviews. Other ways they have to have a proper reason to give it one star".

Surprisingly, 19% of the Privacy Pragmatists group would install the application from the Three Dots Menu as Figure 9 shows. This menu is found when the search results are presented to the user. It is located on the top right corner of the application result. What it means is that these users would install the application from this option without even open the application page.

The blue Diamond sign was another interesting factor that was considered by some participants in both groups. As you can see in Figure 9, Google gives this sign to the top developers and it appears beside the developer name or the company. They stated that if they see this blue sign, they would directly install the application without looking at anything else.

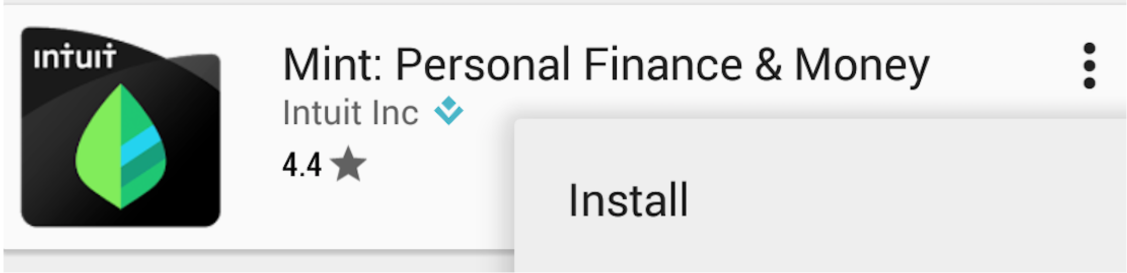


Figure 9: The Three Dots Menu (top right corner) and the Blue Diamond Sign beside the company name Intuit Inc.

ID 14 stated*: "if there is a blue sign. I don't read through the contents that available in the description. Straight away I'll install it*". Another reason stated by ID 14: "*This blue sign indicates trusted application. So Google Particularly give this blue sign for best applications that are available in a particular field. So I would choose an application that has a blue sign other than the other application".*

The previous results were found from the lab study. However, Q9 asked users to put 13 factors into 3 categories: always consider, sometimes consider, and never or

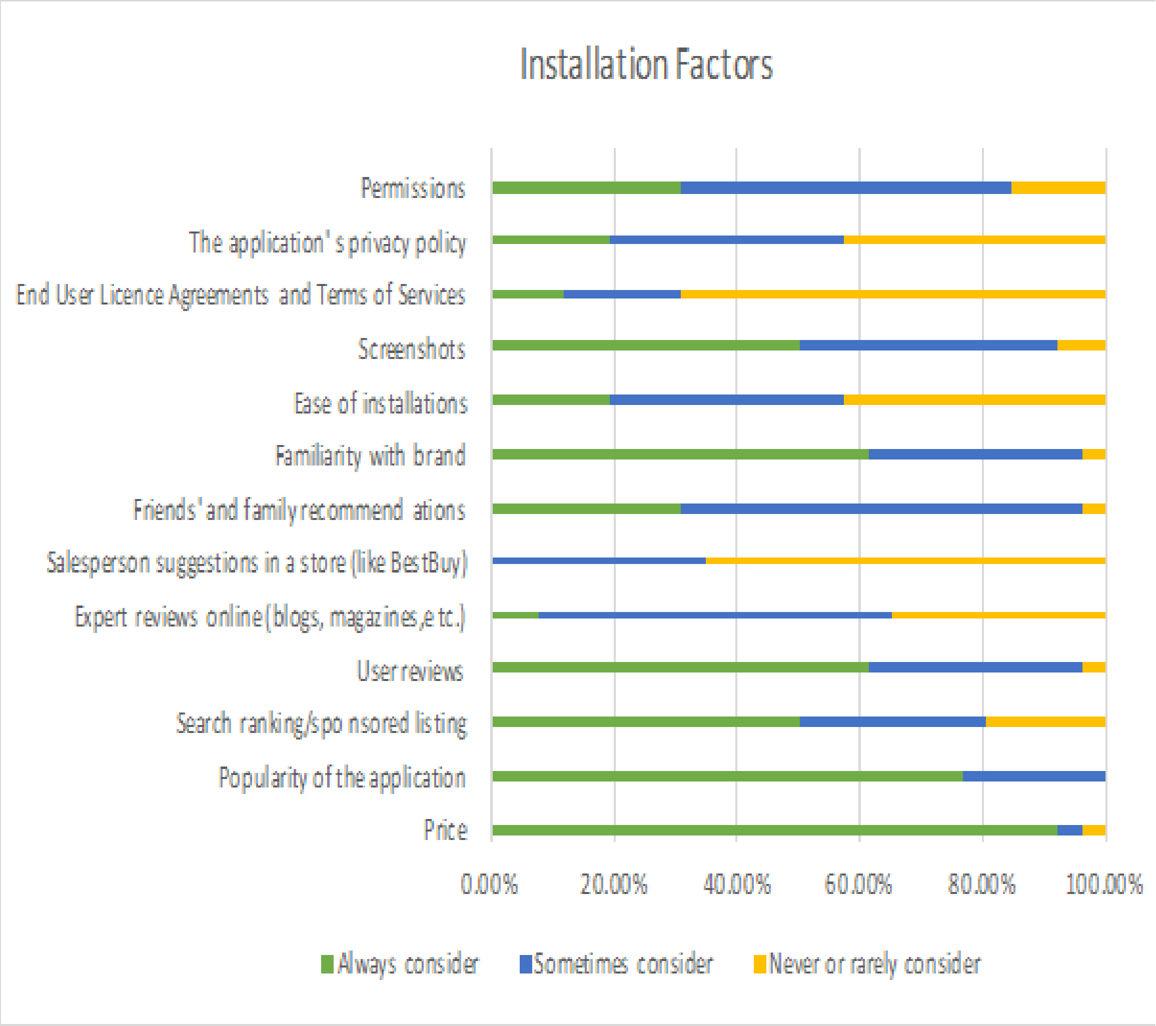


Figure 10: Installation factors.

rarely consider. Similarly, the same factors were given to users to rank them (from the least important is 13 to the most important is 1). These questions were adapted from Chin et al.'s [2]. As Figure 9 shows, 92% of participants always consider the price which is similarly reported by Chin et al.'s [2].

Almost 80% of users always consider the popularity of the application. Ninety percent of participants chose "always or sometimes consider" user reviews. Moreover, the familiarity of the brand influenced 61% of users. With regards to permissions, 53% stated that they sometimes consider them when installing an application. Sixty-nine percent and 42% of participants never or rarely consider reading End User License Agreement and Terms of Service and The Application's Privacy Policy as well. These findings are in line with Chin et al.'s work [2].

4.2.2 Attention to Permission

As stated earlier that the Privacy Unconcerned are the least group that care about their privacy and security and this finding was validated by the Westin's metric. When they were asked when to check for permissions, only one form the Privacy Unconcerned group would check before. This happened because the participant was asked directly, however, when installing the application during the application selection task, he did not consider that. Eight participants of the Privacy Pragmatists group do check permission before installing the application but only two of them would check during the update. Four participants from the Privacy Fundamentalists would check before and only two would check during the update. Minority of the Privacy Fundamentalists and Pragmatists stated that that they do not check permissions because the application is popular. For example, ID13 stated: *"if the app seems popular and its rate is high and well known and recommended. I don't spend much time to review that, it means trusted. Most of the apps are trusted and popular. I don't care about this screen".* Similarly, ID23 stated: *"I will not spend my time looking at that. I'll just simply hit the button so I can get it and see the features. That is the most important thing for me, not the acceptance. Because there is no option. There is only one. If you want to download that application, you have to accept. Why should I think about it?"*

ID5 was one of the participants of the Privacy Pragmatists group. The participant stated why he does not check permission during the update by saying: "*I don't check for update. Permissions are more or less are the same. I have that app in my phone because I need it. Otherwise I wouldn't have installed it. If I don't really need an app or I feel suspicious about it, I just uninstall it, I don't wait for the update.* He further stated that what he checks during the update is if there any changes in the user interface and the functionality.

4.2.3 Security Courses

When we used the Westin's metric index, we found that 75% of Privacy Unconcerned, 44% of Privacy Pragmatists and 17% of the Privacy Fundamentalists are classified as advanced users. All the users who are Privacy Fundamentalists are novices except one.

Using Westin's metric showed stronger relationship with various measures of security better than using the novices versus advanced users based on security course. Surprisingly, the more security courses the users have, the lower their score in the Westin's metric are (r= – 0.3). This metric showed us the real sense of the data.

4.2.4 What Users Think about Current Permission Presentation (OS v.5 5.9)

Users were asked about their opinions of the permission presentation and if they want to make any changes that they think might be helpful.

Table 6 shows that the 75% of the Privacy Unconcerned and 63% of the Privacy Pragmatists thought the current design is useful. However, only 33% of the Privacy Fundamentalists thought it was useful. One other hand, none of the Privacy Unconcerned group want the permission presentation to be complicated in terms of having control of permissions.

Permission Presentation	**Mean UN**	**Mean PR**	**Mean FU**	**SD UN**	**SD PR**	**SD FU**	***r***
1- Special Cases	0.25	0.13	0.67	0.50	0.34	0.52	0.28
2- Want Explanations	0.50	0.38	0.67	0.58	0.50	0.52	0.20
3- More Control/Personalize it	0.00	0.25	0.17	0.00	0.45	0.41	0.13
4- Useful	0.75	0.63	0.33	0.50	0.50	0.52	-0.22

Table 6: What both groups' thinks about the permission presentation and what they need.

In terms of explanations, users among all the groups wanted them to be short and why they need that permission and for which reason.
ID 1 (Privacy Fundamentalist) stated: *"Not very much details about it. More details would be useful and short explanations. Do not have option to deny certain permissions".* This particular user has a custom ROM installed on his device and he is using an application called AF Wall, which gives him the ability to deny the Internet permission to applications. Another quote regards making the permissions more personalized is reported by ID3 (Privacy Pragmatist): *"place the things that are much more of people interests/depends on people choice and more information about In-App Purchases"* permission group. Similarly, ID11 (Privacy Pragmatist) stated the permission presentation is fine but he said *"give a list of In-app purchases so I'll know what I might need to pay in advance. As for, at times I might download an app. That it requires a crucial part. If I want to use that crucial part then I'll have to pay for that specific thing and I don't like that happen to me after I downloaded the app. Suppose this app if I want to get HD feature for the scanner and I wanted it and I don't know maybe they are asking for something else to pay then If I knew that it requires me to pay then I won't download it"*. Moreover, ID18 (Privacy Pragmatist) wanted minor changes and provides a short explanation and do not make them too large because users will not read the whole thing. The participant also wanted more information about the Location permission and to be specific like *" Does it track you at the moment or does track your GPS location".*

One the other hand, ID10 (Privacy Pragmatist): was under the Special Cases, the participant stated: *"I like the old presentation. Used to be better. Gave more exact details. What the permissions were but I imagine that is not the case for everybody"*. The old view presentation of permission (Android OS 4.6 & earlier) as stated earlier by Gerber et al.'s [18] is well integrated and well described and this particular participant point of view validates that. Gerber et al. work was describing the general difference between the changes of old view and the new one and their work did not involve any users. Our work is built on Gerber et al. Also, ID10 (Privacy

Unconcerned) stated: *"it is up to the application developer to add that and Google wouldn't have that feature for the application developer so on so forth".* Similarly, ID20 said: *"I like it, it gives an overview. It collapses. It gives overview what it is using and if you are curios about specific one you can click on it. And check it out. I think it might be nice. If the developer of the app put an explanation here too because here this is a pre-set explanation to what it is using like Call Information* (part of the Device ID & Call Information permission group)*; allows the app to determine the phone number and device Id but that still doesn't say why the app needs to know that. So that might be a better way to do it if the developer can actually explain what are they using it for whereas in the case you kind of makes you need to download the app and see what it does before you understand why it's using these permissions".* Moreover, ID26 (Privacy Fundamentalist) said that he does not like the permission description because it is generic. He gave an example of the Microphone permission. The description says record at any time. He explained his frustration that the he will be recorded at any time without being aware. He said: *"I think it should be specific options for the distributor of the applications to choose from to explain what they are going to be doing with it. Instead of saying using the Microphone at anytime you can prompt or whatever because you know on Skype you are using the Microphone when you answering a call. So it should be there a modified version of that. A description for such a situation. The generic description is kind of giving you a general idea what is going on. It is not really very specific".* Tian et al.'s [55] work was on the iPhone IOS, which showed that how developers are describing their permission access. iPhone developers have Plist files, which give them the ability to write a purpose string description of the reason of requesting the permission access. In the Android permission system, this feature is not supported. They also found the mostly of the Specific Benefit/Purpose is most usable option instead of the least favor one which is the generic purpose which is what is being currently used in the Android system. What the participants mentioned earlier validates Tian et al.'s work. Shih et al.'s [56] research was to "understand what affects people's privacy preferences in smartphone applications" with regards to "the application name and the purpose of the data collection". They found that when there is no purpose was given, "participants were more willing to disclose data". Also, when a vague purpose was given, "participants became more privacy-aware and were less willing to disclose their information". However, when specific purposes were shown to participants, "they were more willing to disclose their information" because they think that is beneficial to them in terms of functionalities.

ID25 (Privacy Fundamentalist) questioned the used symbols that represent each permission group if they were universal symbols. She said, *"Icons/symbols are kind of weird. The Identity, I'm not sure if that is a universal symbol for Identity. The location you can see that on Google map and stuff like that. Camera is universal. Wi-Fi is kind of a weird symbol. Everything is in black and white, which is kind of odd because they have colors".*

Surprisingly, ID16 (Privacy Pragmatist) stated that he wanted to place the permission screen under the Reviews or under the Read More sections. This is really interesting because the "Permission Details" icon is already located at the end of the application page and the participant is not aware of that which validates what Gerber et al.'s [18] and Akhawa and Felt [31] stated in their work. When I asked further for his reasons to change the permission screen location under the reviews section, he said *"actually if I want to read the comments I'll expand it"*. He still did not give a reason and when I asked the participant again, he said, *"mostly because permissions will be the least interesting part*". I think the reason of his request due that he did not consider looking at the permission screen during the application selection task.

4.2.5 Where do Users go to Look for Permission Explanation

Users were asked where they would go if they want to look for permission explanations.

Look for explanations	Mean UN	Mean PR	Mean FU	SD UN	SD PR	SD FU	r
1-Within Google Play Store	0.50	0.31	0.67	0.58	0.48	0.52	0.08
2- Google it/Website	0.00	0.31	0.33	0.00	0.48	0.52	0.12
3- Don't Care	0.50	0.44	0.00	0.58	0.51	0.00	-0.33
4- Phone Settings	0.25	0.06	0.00	0.50	0.25	0.00	-0.27

Table 7: Users responses regards looking for explanations.

As can be seen in Table 7, 67% of the Privacy Fundamentalists, 50% of the Privacy Unconcerned, and 31% of the Privacy Pragmatists would look for explanations for permissions within the Google Play Store.

Surprisingly, the Privacy Fundamentalists group was the only group who care about finding an explanation whether if it is with the Store itself or using Google. On the other hand, none of them would check for explanations within the phone settings.

What was interesting was that none of the Privacy Unconcerned group would look for explanations within the app description (Read More section).

Nineteen percent of all the groups would find an explanation in the application in the reviews section. Felt et al.'s [22] reported that 24% of their participants relied on the reviews to look for explanations for the requested permissions. Also, Felt et al.'s [22] described that users' reviews were used to "convey privacy and security information during installation" and users reviews "can warn people about undesirable or privacy–invasive applications". Similarly, They stated that some of their participants considered online news articles that looked into application permissions [22]. However, Wagner and Ha work looked at what users write about in the reviews and if they discuss any topic regarding the privacy and security of an application. They found that only "1% of the reviews mentioned application permissions" and the "majority focused on the quality of applications" [42]. What that means is when users look for an explanation it is almost impossible to find that in the review section which is going to put burden on users. ID6 stated: *"I check the* *reviews and see the description. And what are they using and what they need those permissions for and if I think there is a genuine reason behind it, then I'll install it. If I did not like that I wouldn't install it and I'll go for alternatives".* Another quote by ID26 *"if you are not sure about the permissions. What you can do is to check the Read More section. Often times they'll actually explain what are these permissions for, not always though but you can usually find explanations implicitly like for example, this application wants access to the camera"*. The participant opened the permission screen to show me what he means and looked carefully and slowly then said "*so if you look in the description. It's got a barcode scanner so that's a feature of the application, which would require the camera. There is actually an actual explanation why they need it which you know kind of mitigates any sense that they might be just thrown that permission in there for some shitty reason but. It is always possible that they can do whatever they want. This kind of how permission works. You are taking the risk"*.

As stated earlier, justifications are required to bridge the gap between the requested permissions that access the phone resources and the intended functionalities.

4.2.6 Checking Reviews

Users in general looked at the positive reviews to see what others has said about the application which many encourage them to install the application. Also, looked at the negative ones to see what kind of issues other users run into.

ID 10 said one of the reasons to check reviews is that he sometimes does not know what he wants necessarily from using the application. The participant said *"I know I want this kind of app and I do not know what kind of features I might wanted to have like in this case, maybe something that I thought of it's really important and the reviews usually bring that up front for me".* Another important reasons reported by ID26*: "no application has you know all around perfect reviews. If it is popular I find the negative reviews to determine what they didn't like about it. Sometimes there problems that are more legitimate than others like almost all the time the problems that people have with applications are specific to their phones and not to the* *application like it doesn't work at all, like it because it crashes all the time maybe because the phone is not Prime or something like that"*. What he meant that there are some compatibility issues with regards to specific phone models that other users may be not aware of. This issue is reported also by ID1. However, this participant was the only one participant who chose from the review section; the sorting options; the latest version only and from this device only during the application installation task to see if there are certain issues that are specifically related to the used phone before installing the application.

4.2.7 Users' Need Changes/Features in Google Play Store

Users were asked if they want to see any changes or features in the near future on Google Play Store. This would help uncover any issues that bother users while navigating the store. The results showed that all the Privacy Fundamentalist, all the Unconcerned group and only half of the Privacy Pragmatists group want the Google Play Store to be more organized. Both of the Privacy Fundamentalists and Unconcerned groups did have concerns in the Google Play Store. Forty-three of the Privacy Pragmatists did not have any concerns and they think the current design is fine.

ID2 (Privacy Fundamentalist) described his frustration when searching for apps by not finding the real apps that he is looking for. He wanted the change the current presentation of the Google Play Store to be similar to the Apple iPhone App. The participant said that there are many similar apps that looks like Twitter or other apps and if Google cannot delete these similar apps, at least ask these developer or companies to change their apps' icons. He can find the real Twitter app in the Apple IPhone App Store without any difficulties. Similarly, ID8 (Privacy Fundamentalist) said: "*Front page could be done little better. I feel like just, a lot of information. A lot of it really varies. New users would be confusing, Overwhelming at times. And sometimes I find it little bit hard like to find better less known apps. I mean I realize just from how it's work. I have to go to a website. Here is an app that is pretty good but if I don't know it by name, it is hard to find. Go to website to find best 25 apps for something"*. ID15

(Privacy Pragmatist) wanted one more tab for new users which consists of mandatory and essential apps. ID1(Privacy Fundamentalist) said that he wants to see the list of the apps in the Top Free tab without showing any games.

ID4, ID5 and ID24 described that Google should block spam/malicious apps and check on apps before uploading to Google Play Store to make the store more secure. ID3 and ID15 were frustrated because they receive too many updates. ID3 said: *"it's not a good experience that I face everyday when I go home and connect to the Internet: oh nine apps are ready to update. I don't want to everyday to my apps to be updated. If I'm using this app regularly again and again, pop me up with the message that you are using this app again and again, there is a new update but if I'm using an app once in a month, just don't bother me".*

Surprisingly, ID6 and ID7 stated that the apps in the first page of Google Play Store should not be random, it should be related to our interests. This feature is already available in the store. The reason can be that there is a lot of information in the store and this implies that users are not fully aware of the features that the Google Play Store provides.

On the other hand, ID14 is a registered developer. The participant wanted to put back the 5 stars' ratings. Now, the rating is shown as the exact number of the app rating in a range of (1 to 5) followed by one-star symbol. He thinks that the current rating is *"invisible, weak and do not look nice".*

ID11 lived in the Middle East and he wants an option to change the country in the Google Play Store. He explained his reason by saying: "*many times it depending on which country you are in. They will update your suggested application by the top applications by the country you are living in. So I want a feature that you can change the country. Let's say if I'm in the middle east then I would get apps suggested apps by the people who download app in the middle east but most of the apps might be native to their language but not to me. It would be difficult for me to go through the list. Looking for apps that are probably popular in the US or Canada".*

Finally, ID20 wants some changes in the reviews section. The current one always shows you the recent comments. He wants to incorporate the same experience of most online shopping websites by adding more sorting options such as: the most helpful reviews and the most critical reviews. He said" *I mean the most recent ones are often useful for an app but you want to see the most critical reviews to see what actually is good or bad about the app".* This is another example of not knowing what the current Google Play Store has. The most helpful sorting option is already available.

4.2.8 Participants Permission Groups Matching Scores

Table 8 records only the percentage of the respondents' answers. The scoring was done manually as can be seen in Table 8. The total number of questions was 78 questions. Twelve questions for the Unconcerned, 48 for the Pragmatists and 18 questions for the Fundamentalists.

Unconcerned 12 Questions		Pragmatists 48 Questions		Fundamentalists 18 Questions	
Correct (2)	4-33%	Correct (2)	9-18%	Correct (2)	10-55%
Correct (1)	8-66%	Correct (1)	32-66%	Correct (1)	5-27%
Incorrect (0)	0	Incorrect (0)	7-14%	Incorrect (0)	3-16%
Correct old	11-92%	Correct old	26-54%	Correct old	15-83%
Incorrect old	1-8%	Incorrect old	22-45%	Incorrect old	3-16%
Correct New	5-41%	Correct New	24-50%	Correct New	10-55%
Incorrect new	7-58%	Incorrect new	24-50%	Incorrect new	8-44%
Extra old inc	2-16%	Extra old inc	7-14%	Extra old inc	5-27%
Extra new inc	0	Extra new inc	5-10%	Extra new inc	4-22%

Table 8: The score percentage of each category.

Table 8 shows the 55% of the Privacy Fundamentalists answered correctly some of the questions. The Privacy Unconcerned group answered at least one correct of the old naming followed by the Privacy Fundamentalists by 83%. The percentage of the Privacy Fundamentalists with regards to choosing at least one correct answer of the new naming was slightly higher the other two groups. Both the Unconcerned and the Fundamentalist perceived the old naming of permission better than the

Pragmatists. These finding prove to some extent the work of Gerber et al. [18] when they stated, that old permission naming's are well described and integrated. All the three groups perceived the new naming of permission groups. However, the Privacy Pragmatists scored almost the same score regarding the old and new naming. They like both permission presentations.

On the absolute scoring scale without having extra incorrect answers; both ID24 (Unconcerned) and ID6 (Pragmatist) answered correctly 2 questions out of 3. Three from the Fundamentalists and the Pragmatists groups answered one question correctly. Only one participant from the unconcerned group got a correct answer.

In some cases, the old naming was better than the new naming and vice versa. For example, as Table 9 shows, the old naming was better in the permission label questions: 1,2,4,5,6 and 9. They were perceived better than the new naming. For example, all the four participants chose the old "Bookmarks & History" permission group for the Permission label: "Read you Web Bookmarks & History", which was better than the "Device & App History" new permission group. On the other hand, the new naming was better for the permission label questions: 3,12 and 15. The permission label: "Google Play Billing Services" is a perfect example the represents this category. Ten participants chose the new naming of "In-app Purchases" permission group and only 4 chose the old naming, which is "Network Communication". Clearly, this shows that new one represents the given permission label very well. Permissions label questions 8, 11 and 13 were perceived equally in both the old and new naming. For example, both "Storage" old permission group and "Photos/Media/Files" new group were equally chosen for the "Read Contents of Your USB Storage" permission label.

Only two participants choose the hidden "Other" permission group. This permission group covers any other permission's that are not related to any of the 17 permission groups. I think the reason for their choices is that they thought there are other permission groups that can be corresponded to the permission label question.

Finally, some of the previous findings validate what Gerber et al. [18] stated in their work and some contradicted it because it shows that some participants did like the old naming, some the new ones and some did like both. So, we conclude that our hypotheses were rejected and there is no enough data to do further analysis.

Permission Label	N	Permission Groups/Categories	Responses	
1-Write your Web Bookmarks & History	3	✗Device & App History	0	0%
		✓Other	0	0%
		✓Bookmarks & History	3	100%
		✗None of these	0	0%
		I don't know	0	0%
2-Read your Web Bookmarks & History	4	✓Device & App History	1	25%
		✗Other	0	0%
		✓Bookmarks & History	4	100%
		✗None of these	0	0%
		I don't know	0	0%
3-Read Your Contacts	4	✗Phone	2	50%
		✓Your Social Information	1	25%
		✓Contacts	4	100%
		✗None of these	0	0%
		I don't know	0	0%
4- Create Accounts and Set Passwords	3	✗Your Application Information	1	33.33%
		✓Other	0	0%
		✗None of these	0	0%
		✓Your Accounts	3	100%
		I don't know	0	0%
5- Change Your Audio Settings	10	✗Microphone	6	60%
		✓Audio Settings	10	100%
		✓Other	1	10%
		✗None of these	0	0%
		I don't know	0	0%
	3	✓Network Communication	2	66.67%

6- Connect and Disconnect from Wi-Fi		✗None of these	0	0%
		✗Wi-Fi connection Information	3	100%
		✓Other	0	0%
		I don’t know	0	0%
7- Read Your Own Contact Card	8	✓Identity	4	50%
		✓Your Personal Information	3	37.5%
		✗Contacts	6	75%
		✗None of these	0	0%
		I don’t know	0	0%
8- Find Accounts on the Device	9	✓Identity	6	66.67%
		✗Other	0	0%
		✓Your Accounts	7	77.78%
		✗None of these	0	0 %
		I don’t know	1	11.11%
9- Read Your Social Stream	6	✓Your Social Information	5	83.33%
		✗Device ID & Call Information	2	33.33%
		✓Other	1	16.67%
		✗None of these	0	0%
		I don’t know	0	0%
10- Prevent Phone from Sleeping	4	✗System Tools	4	100%
		✓Other	0	0%
		✓Affects Battery	0	75%
		✗None of these	0	0%
		I don’t know	0	0%
11- Read Calendar Event Plus Confidential Information	5	✗None of these	0	0%
		✓Calendar	4	80%
		✗Your Social Information	4	80%
		✓Your Personal Information	4	80%
		I don’t know	0	0%
12- Google Play Billing Services	10	✓Network Communication	4	40%
		✗Your Application Information	5	50%

		✓In-app Purchases	10	100%
		✗None of these	0	0%
		I don’t know	0	0%
13- Read Contents of Your USB Storage	2	✗Other	0	0%
		✓Storage	1	50%
		✗None of these	0	0%
		✓Photos/Media/Files	1	50%
		I don’t Know	1	50%
14- Read Phone Status & Identity	3	✓Phone Calls	2	66.67%
		✗None of these	0	0%
		✗Identity	3	100%
		✓Device ID & Call Information	3	100%
		I don’t know	0	0%
15- Read Call Log	4	✗System Tools	1	25%
		✓Phone	4	100%
		✗None of these	0	0%
		✓Your Social Information	1	25%
		I don’t know	0	0%

Table 9: The percentage of respondents’ answers.

4.2.9 Users’ Concerns using Android

During the interview, participants were asked to give a general advice for their hypothetical friend who has just got a new brand smartphone. Also, if there are any “pitfalls” that other users should avoid when using the Android platform.
Examples of the reported memory limitation issues are: users have to consider the size of the RAM before buying an Android smartphone, avoid the multitasking and overloading the phone, and always close a running task or install a killer task manager app. Open source reported issues are: as stated earlier that anyone can upload any apps, Google Play Store is not restrict as iPhone App Store, third-party apps, less trustworthy stores, shady apps, avoid viruses and malware and install trusted antivirus apps.

Some participants described that the security settings are quite difficult and confusing for novices and some of these settings can mess up the phone. For example, ID21 reported that he rooted his phone partially because his phone was locked and the participant wanted to remove pre-installed useless apps. Also, the participant was very frustrated that he is no longer receiving any system update and he is still in the process of figuring out a way to un-root his device. 83% of the Privacy Fundamentalists group stated that, users in general should not enable the developer mode and also avoid rooting their devices. Enabling the developer mode allows third party apps downloaded from the Internet to be installed, which may affect their phones. All the groups reported that every user should always backup and sync their data on the cloud and restrict the use of data usage. Finally, the number of individuals endorsing each pitfall is small; we do not want to over interrupt the data.

4.3 ADVANCED/NOVICE USERS CLASSIFICATION

Under this classification, I looked into the factors that participants considered when downloading an application during the application selection task. It is important to note that because Bonferroni correction lowers the acceptable p-level (for α=0.05, i.e., 5% chance of a Type-I error) to 0.001 (from 0.05), none of the tests that were calculated indicated significant differences. I described the results in general without going into details since the results of this classification did not represent the data as it should be and it was a failure.

4.3.1 Factors Considered when Downloading an App

Table 10 shows the number of factors that participants considered when downloading an application. Generally, there were some similarities between both groups when installing an application such as considering: Rating, Number of Downloads, Application Popularity and Reviews. Other factors were slightly higher by novice users such as: reading the full application description and looking at application screenshots.

Both groups were looking to see if the required permissions are reasonable.

Factors Considered	Mean Nov	Mean Adv	SD Nov	SD Adv	*p*
1-Blue Sign	0.20	0.09	0.41	0.30	0.47
2- Rating	0.60	0.73	0.51	0.47	0.52
3-Number of Downloads	0.47	0.55	0.52	0.52	0.71
4- Popular	0.47	0.45	0.52	0.52	0.95
5-Reviews	0.87	0.82	0.35	0.40	0.75
6-Number of Reviews	0.20	0.27	0.41	0.47	0.68
7-Rating Icon	0.13	0.00	0.35	0.00	0.22
8-Read Full Description	0.47	0.27	0.52	0.47	0.33
9-Read Short Description	0.13	0.09	0.35	0.30	0.75
10-Features	0.27	0.18	0.46	0.40	0.63
11-New Section/Updated Version	0.13	0.00	0.35	0.00	0.22
12- Latest App Version/When it's Updated	0.07	0.09	0.26	0.30	0.83
13- Reasonable Permissions	0.60	0.18	0.51	0.40	0.03
14-Free	0.20	0.36	0.41	0.50	0.37
15-Similar Apps	0.27	0.27	0.46	0.47	0.97
16- Negative Reviews	0.53	0.18	0.52	0.40	0.07
17-Find my Solution	0.13	0.18	0.35	0.40	0.75
18-Google it	0.07	0.09	0.26	0.30	0.83
19- Screenshots	0.53	0.36	0.52	0.50	0.41
20-App Logo	0.20	0.18	0.41	0.40	0.91
21-Avoid Ads	0.33	0.09	0.49	0.30	0.16
22- Knew the App	0.13	0.18	0.35	0.40	0.75
23-Quick Install	0.00	0.27	0.00	0.47	0.03
24-Categories	0.07	0.18	0.26	0.40	0.38
25-Install/Try it	0.20	0.45	0.41	0.52	0.18

Table 10: Factors considered by participants when installing an application.

4.3.2 Attention to Permissions

Earlier, I described that novice users were looking to see if the permissions are reasonable. During the app selection task, 73% of the advanced users and only 27% of the novice users did not consider permissions. Twenty percent of the novices took a quick glance at the permission screen and 40% of them took longer time deciding.

Despite the fact that some participants do not check permission for various reasons, still, these finding showed that users are now more aware of permissions than before because 80% of both groups did look if the requested permissions are reasonable. As reported in 2012 by Felt et al.'s [22] earlier, that only 17% of their participants had "paid attention" to the requested permission, and 42% were not aware of "the existence of the permission screen". Another reason for this finding is, all the participants are Compute Science students, which could imply the higher percentage of permission awareness.

With regards the time that participants took installing an app, novice users took longer time to install an application. On the other hand, when users were asked when to check permissions, three advance users check before installing an application but none of them would check permission on during the update. Ten novice users check permissions before but only 4 of them would check on update.

4.3.3 What Users Think about Current Permission Presentation (OS v.5 to 5.9)

Table 11 shows that the majority of each group thinks that the permission presentation is useful. Also, 53% of the novice users and 36% of the advanced users want some sort of explanations of the requested permissions.

Permission Presentation	Mean Nov	Mean Adv	SD Nov	SD Adv	*p*
1- Special Cases	0.33	0.18	0.49	0.40	0.41
2- Want Explanations	0.53	0.36	0.52	0.50	0.41

3- More Control/Personalize it	0.13	0.27	0.35	0.47	0.39
4- Useful	0.60	0.55	0.51	0.52	0.79

Table 11: What both groups' think about the permission presentation and what they need.

4.3.4 Where do Users go to Look for Permission Explanation

Table 12 shows where would users go to look for explanations.

Where to look for explanation	Mean Nov	Mean Adv	SD Nov	SD Adv	*p*
1-Within Google Play Store	0.47	0.36	0.52	0.50	0.62
2- Google it/Website	0.33	0.18	0.49	0.40	0.41
3- Don't Care	0.27	0.45	0.46	0.52	0.34
4- Phone Settings	0.00	0.18	0.00	0.40	0.09

Table 12: Users responses regards looking for explanations.

Almost half of the novice users and 36% of the advanced users would check for explanation within the Google Play Store. Also, both groups stated that they would use Google or the application website to find more about permissions. Again, the percentage of novice users is slightly higher than advanced users.

What is most interesting is that 45% of the advanced group and 27% of the novice group do not care about finding explanations. More importantly, 18 % advanced users were looking for explanation under the Phone Settings Menu. This reflects their expertise in knowing their phone settings very well. As described earlier in Chapter 2, if users want to check permissions, they have to go to the Menu Settings and select Apps or Application Manager options. Then, choose an application and the permissions are shown at the bottom of App Info page. It is quite complicated to navigate the phone settings to find the APP Info and the organization of the settings in Android are sometimes different because every smartphone manufacture has their own Android user interface.

4.3.6 Users' Need Changes/Features in Google Play Store

The results showed that both groups want the Google Play Store to be more organized. A few stated that they do not have any concerns at all and they like the current one.

4.3.7 Participants Permission Groups Matching Scores

Table 13 The total number of questions was 78 questions. Forty-five questions for novice users and 33 questions for advanced users. In general, 29% of both groups correctly answered some of the given questions without having extra incorrect answers. Fifty-seven percent gave at least one correct answer from two answers, and 12% of the population gave incorrect answers. The percentage of both novice and advanced users who got at least one correct answer of the old naming of permissions' group was 67%. Fifty percent got at least one correct answer of the new naming of permissions. Only 17% got chose extra incorrect answer of the old naming of permissions categories and 11% chose extra incorrect answer of the new naming.

Novice- 45 Questions		Advanced - 33 Questions	
Correct (2)	15- 33%	Correct (2)	8-24%
Correct (1)	23- 51%	Correct (1)	22-67%
Incorrect (0)	7-15%	Incorrect (0)	3-9%
Correct old	24-53%	Correct old	28-85%
Incorrect old	21-46%	Incorrect old	5-15%
Correct New	29-64%	Correct New	10-30%
Incorrect new	16-35%	Incorrect new	23-69%
Extra old inc	7-15%	Extra old inc	7-21%
Extra new inc	7-15%	Extra new inc	3-9%

Table 13: The score percentage of each category.

These results clearly show that the 85% of advanced users have perceived the old naming of permission groups in compare to 30% of the new naming. Advanced users preferred the old naming of permission groups.
Sixty-nine percent of advanced users chose incorrect answers of the new naming compare to 35% of novices.

On the absolute scoring scale without having extra incorrect answers; both ID6 (novice) and ID24 (advanced) answered correctly 2 questions out of 3. One question was answered by four novice users: ID11, ID14, ID20 and ID25. Similarly, from the advanced group ID2, ID3 and ID18 answered one question correctly.

Finally, some of the previous findings validate what Gerber et al.'s [18] stated in their work and some contradicted it because it shows that some participants did like the old naming, some the new ones and some did like both. So, we conclude that our hypotheses were rejected and there is no enough data to do further analysis.

4.3.8 Users' Concerns using Android

Both groups similarly mentioned the memory limitation issues. However, the percentage of advanced users concerns regards the open source vulnerabilities and the security settings were higher than novices.

4.4 BOTH CLASSIFICATIONS

In this section, I described the results in general and by using both classifications.

4.4.1 Latest Firmware/Security Software/App Ops

Participants were asked if their devices running the latest firmware. More than half of participants reported that their firmware is up to date. Twenty-three of them stated their OS is not updated. Quite surprising that 15% of participants do not know whether or not they upgrade to latest firmware. Also, I asked participants if they use any security software on their smartphone or PC/Laptop. What is interesting is that 78% of participants have security software on their PC/Laptop but only 23% have it on their smartphones. This finding is in line with Mylonas et al. [9] work that stated, "smartphone security software is poorly adopted". Only 24.5% of their sample has them.

Question 18 asked participants if they consider security software essential. Forty-six did not consider them essential.

Moreover, Q19 was asked to see if participants know what does App Ops means. As stated earlier in the Chapter 2, this app allow/deny permissions. Only 2 participants defined it correctly. Ninety-two percent did not know what does it mean. One participant thought it was something related to Ads.

Security Software	**Mean UN**	**Mean PR**	**Mean FU**	**SD UN**	**SD PR**	**SD FU**	***r***
Smartphone	0.00	0.25	0.33	0.00	0.45	0.52	0.275
PC/Laptop	0.75	1.00	1.00	0.50	0.00	0.00	0.355
None	0.25	0.00	0.00	0.50	0.00	0.00	-0.355
Essential	0.00	0.56	0.83	0.00	0.51	0.41	0.598

Table 14: Security software adoption in each category and if they are essential

There was no relationship between the advanced and novice users with regards to installing security software on their devices and if it essential. They both have the same percentage. However, Table 14 shows that when Westin's metric was used, participants from the Pragmatists and Fundamentalist groups similarly considered having security software on their smartphone. All the three groups have security software on their PC/Laptop. The Privacy Fundamentalists have a less percentage of having security software in their PC/Laptop. ID24 from the Unconcerned group reported that he does not have any security software. What was really interesting that 83% of the Fundamentalist and 56% of the pragmatists do consider security software essential (r=*.598)*. On the other hand, the Unconcerned group thinks that security software is not essential to have.

When advanced and novice users were asked if they installed the latest firmware, 82% of advanced users and 47% of the novice user stated affirmatively of installing it. This shows that advanced users are aware of the phone settings.

Lastly, Westin' metric was used to see if there are any differences among the three groups with regards to installing the latest update. I thought that the Privacy Fundamentalist percentage would be higher than the other two groups. However, as Table 14 shows that only 17% of Fundamentalists did install the latest firmware, which is surprising (*r=–. 507)*. Installing latest firmware updates any security or privacy issues. More importantly, all the Unconcerned group did install the latest firmware. Furthermore, 50% of Fundamentalist and 19% of Pragmatists stated that they did not install the latest firmware.

What was quite shocking was that 33% of the Fundamentalists and 13% of Pragmatists did not know about whether or not if they have installed the latest firmware. It seems that the Privacy Unconcerned group care more about installing it than the other two groups.

Latest Firmware	Mean UN	Mean PR	Mean FU	SD UN	SD PR	SD FU	r
Yes	1.00	0.69	0.17	0.00	0.48	0.41	-0.507
No	0.00	0.19	0.50	0.00	0.40	0.55	0.432
Don't know	0.00	0.13	0.33	0.00	0.34	0.52	0.181

Table 15: Respondent's answers.

4.5 NO CLASSIFICATION

In this section, I report the rest of the results without using any type of classifications because when I did further analysis, I could not find any relation or correlation between the different groups.

4.5.1 Unfamiliar Brands/App Stores

Question 14 was asked to gauge participants' willingness of installing and trying apps from unfamiliar brand or company. The brand name of an app "can act as a security signal" and apps from familiar brands "are less likely to be malware or grayware". I adapted this question from a previous work [2] and I extended its scope by asking participants about their reasons of installing apps from unfamiliar brands.

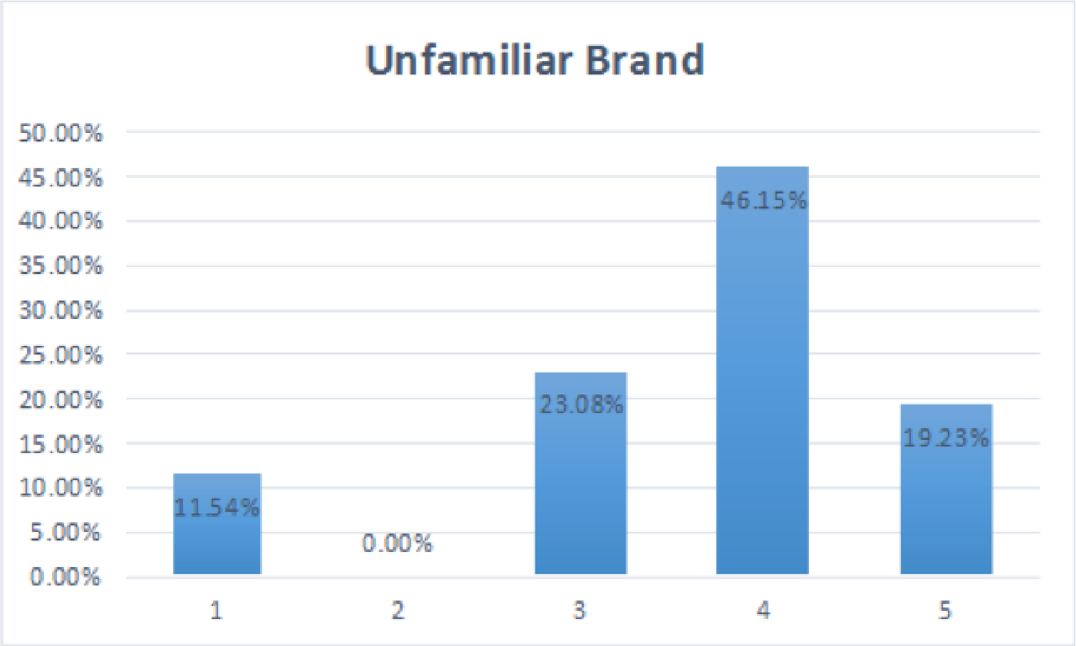


Figure 11: The willingness of participants to try applications from unfamiliar brands, on a scale of 1 (least likely) to 5 (most likely).

Figure 11 shows that 65% of participants are likely to try apps from unfamiliar brands and these results are in line with Chin et al. [2] study that reported 70% of their participants are willing to try that. Table 16 showed the reasons given by participants.

Reasons	% Of Participants
Good reviews	26
Spam/malware/affect my phone/fear of data loss	11

Start-up companies make good apps/upcoming brand	8
Get familiar later	8
Discover & test new apps/open minded to try/take the risk	15
Necessity of the app	8
Like the app, brand is not important/useful/free	11
Care about popularity not the brand/if it become popular	8
Brand/name/app icon are good and believable	4

Table 16: Reasons for trying or not trying apps from unfamiliar brands.

Question 8 was to look the app stores that users would use to search for and install apps. Google Play store is the official app store for the Android platform. Figure 12 shows that the dominant used store is the Google Play Store, which is similar to what Chin et al.'s [2] found. The second source was using Websites.

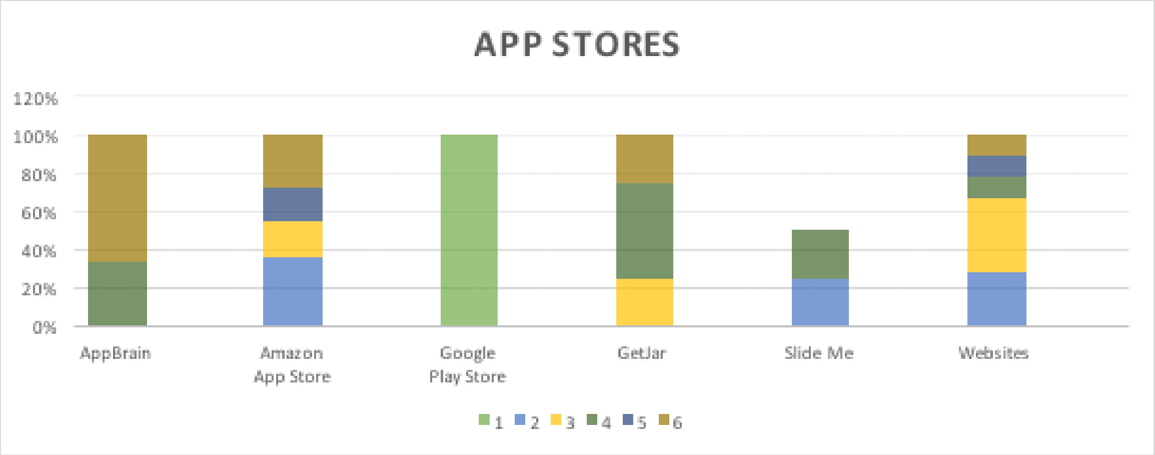


Figure 12: Breakdown of some of the available App Store downloads sources on a scale of 1 (the most important) to 6 (the least important).

4.5.2 Auto Update

Participants were asked during the application selection task whether they enable the Auto Update on the Google Play Store or not and their reasons for doing so. I adapted this question from Sanders et al.'s [34] work and I extended it by including participant's reasons. However, a recent work reported various reasons for enabling/disabling the Auto Update and I compared my results to their work. I also used some of their used codes to represents my similar results. The same question was asked during the post-online questionnaire to give participants' the freedom to writing. In general, 54% of the study participants reported enabling the Auto Update and 46% chose to do it manually. Table 17 and Table 18 describe the reasons in details.

Reasons For Automatic Updates	**Number of Participants (%)**
Get relevant updates/Fix bugs or issues	3-11
Don't want to update it manually/no time	6-23
Auto Update is safe	1-4
Never bothered about it	1-4
Only with Wi-Fi	3-11

Table 17: Reasons for automatic updates.

Reasons For Manual Updates	**Number of Participants- %**
Update only trusted apps/Certain apps	3-11
In case of app's permission change/like to know more about it	3-11
Annoying notification notices/more control	3-11
Data usage	1- 4
Memory Limitation	1- 4
Horrible updates	1- 4

Table 18: Reasons for manual updates.

These reported results showed that users concerns are divers. Similar results found in a recent work by Tian et al.'s [55] in which they stated "users like to engage in decision making for app updating by being aware of updates and making decisions they think they are reasonable".

Three participants showed higher level of update awareness. They stated that if there were a change of permissions, the app would not be updated until the users approve it. ID16 explained his frustration when he cannot stop updating some apps. It updates automatically without his consent and does not like that. This case applies to some of the pre-installed apps such as: Google Play Store. ID 15 stated: *"updates usually takes place by itself without user intervention, so I will not check it or it does not make me to check it once again".* These two examples show that some participants still have some misconceptions and they do not understand how the auto update works.

More importantly, three participants were aware of a feature in the store, which is, disabling the auto update but they can make some apps update automatically. Doing that requires a good knowledge of the Google Play Store. It takes six steps to do it. A user has to open the Google Play Store>Menu>my apps>select the app you want to modify>press on the three dots menu which is located in the upper-right corner of the store screen>check the auto update.

4.5.3 Knowing the Android Rooting Term

This question was to asked because I wanted to know whether participants are familiar the term. Seventy percent of participants stated that they knew the term and they showed high level of understanding when they described it. I thought the percentage would be higher since this work pole was only from the Faculty of Computer Science.

CHAPTER 5: DISCUSSION

In this section, I discuss some of the results without over reporting. Also, discuss the recent Google announcement of introducing Android M and N as well as sheds some light about its revised permission system. Moreover, I discuss various interesting findings and the limitation and challenges of my work.

5.1 ANDROID M AND N

During working on my thesis, Google announced a new version of Android M 6.0. It was announced last year in the summer and then was given to the developer in beta preview. It was released officially on the end of September 2015. Google Nexus devises was the first to get the update. M stands for Marshmallow.

The Android M has more fine-grained permission system. Apps are no longer ask for permission during the installation process. Users will be asked to grant some of the permissions while using the app. They can revoke any permission at any time without causing the app to crash. However, if the app asks to grant the Microphone permission, a pop up notification will ask the user to allow or deny it [57]. It is similar to what App Ops does which was released back in the Android 4.3 as a hidden app but then removed by Google in Android 4.4. With the releasing of Android M, now the users are back in control of the requested permissions. Apps need to be updated to support the latest API that supports the new permission system. If the app is supported, disabling permission will not cause the app to crash. On the other hand, if the app is not updated yet and users try to disable some of the permissions. A dialog will appear stating that “this app was designed for an older of Android, denying permission may cause it to no longer function as intended” [58] . The new permission groups are: Calendar, Camera, Contacts, Location, Microphone, Phone, SMS and Sensors. According the Android Police website [59], the Internet permission is no longer under any of the previous permission groups. That means users cannot even find a way to revoke the Internet permission even if they go the

Menu Settings. There is no method to do so. The Internet permission in the Android M is located under the Normal Protection level. Any permission under this level is granted at the install time despite the fact that the Internet permission is considered in the previous API as a dangerous permission. For example, if there is an app that "manage the address book: access to the Contacts permission group is obviously necessary, but access to the Internet is not necessarily needed". In this case, "would have to trust the app developer" by not sending their app data to a server [59]. Derks described that the "real reason for not including a revocable Internet permission is advertising". Google Play Store has many free apps that "rely on the Internet to download and display advertisement". Derek further explain that" if every user could turn off the Internet access, ad-supported apps would lose their only method of monetization, which would seriously discourage developers" [7], [30].

During my study, three participants had the Android M operating system installed because their devices were Google Nexus. I asked each participant to show me their Google Play Store to see if they have the new revised permission system. Two of them had the same current permission system that shows the permissions that it needs before accepting and downloading the app. The third participants had the new revised permission system because he installed it as a custom rom from XDA developer website. At that time, the version of Google Play Store was 5.9. Now it is 6.2. I could not do further checkups on the participant's devices to see if they have it or not. One participant was aware of the permission changes because he installed a custom rom.

Apps that control and revoke permissions are available in the Google Play Store but most of them requires rooting the device which most of the users are not willing to do because as stated earlier in the background that they will lose their warranty. CyanogenMod is an example of a custom rom that is built on Android. They have their own version of APP OPS called Privacy Grade. This app gives users the ability to allow/deny certain permissions [7].

More importantly, according to Google developer website[60], the distribution of the Android operating system is that only 2.3% of the current devices has Android 6.0

Marshmallow. Seventeen percent had Lollipop 5.5 and 19% Lollipop 5.1. Surprisingly, 34.3% had the Android KitKat 4.4 and 22% Jelly Bean 4.1.x. That means that users are more likely not to get an update to the new Android M [57]. Apple iPhone devices receive faster updates in comparison to Android. One of the reasons that Android devices do not get latest updates very quickly is that there are many vendors like Samsung, LG, HTC and Motorola. Each company has their own modified version of the interface. Another reason is that Apple pushes their updates on the go without the interference of phone carriers [61].

Finally, Google also announced Android N on the 17th of March 2016. It is available now for developer in the preview mode. It added more features such as: multi-window mode and new notification mode [62].

5.2 HOW TO PRESENT PERMISSIONS

During the study, I asked participants how they want the permissions to be presented in order to be easier and clear to understand. I wanted to get some insight from the participant's point-of-view. Rogers et al. [20] described that understanding the best ways of "presenting warning information is a complex undertaking" process. Hong [21] stated that developing a "better displays that can summarize the privacy behaviors of an app" is a good opportunity research. Also, he further explained and asked, "what kinds of information should a display show?" Do they place these displays while "users are searching for apps", or right before they install an app, or as they use the app or after they install it. All of the previous work that developed and designed tools to help users make informed decisions were based on the design of developers or designers, not the end-users. Potzsch [63] described the importance of "the choice of words and descriptions" from the perspective of "ordinary people, not from computer specialists. Also, "it is not sufficient to rely on expert opinions about what may be useful to display and to inform people". Similarly, Adams and Sasse [64] described the importance of understanding the perception of the "target group" to design usable applications. The "level of technical knowledge" differs among the "majority of people" since they are not all considered experts [64]. Moreover, Gould and Lewis stated, "users diversity is underestimated". They further explain that designers rely on their expertise when designing and they do not realize the difference between them and users. Designers do not think about the difficulties that users may have [65].

I speculated from the previous studies that may be Google could include end users in the stages of designing any permission systems. As described earlier in the results chapter, users did like the current permission presentation. However, they want some sort of explanations why permission is needed and for which purpose. One of the participants stated that the given permission description is generic and Google should give developers or the distributors such a features that give them the ability to state clearly why this permission is being asked. Another participant questioned the used symbols on the permission screen if they all are universal. The previous example shows, to some extent, why it is important to include end-users in the design of the permission-acceptance process.

5.3 USERS TRUST

ID5 stated that he lost his trust in Google Play Store because anyone can upload any application. He heard a few years back that someone repackaged the Angry bird game and attached a malware. He said*" people were downloading the game thinking it was a game but it was actually draining the battery in the background"*. He further said" *Angry Birds is a big franchise so if some could take that game and repackaged it, there is no guarantee that someone will do it for other games".* The game asked for more permissions and it is difficult for users to detect the infections [66]. Similarly, ID19 stated that *"be careful on what you download, maybe there is a malware, usually people think that everything on Google Play Store is safe but that is not true, some people can have some viruses in that".* ID16 reported that he would check more for some apps because he encountered an issue. He heard about the True Caller app and said "*it is accessing the contacts and it is given all the contact information, in this case,* *this type of app, which is publically available and it is collection the data".* ID25 stated looking at the permission screen every time. I asked her why? She said: "*I mean people gave up too much personal information. When someone gives you something for Free, they are not given you something for Free".* They collect your data and clean it to sell it to somebody else. She further explains *"there is nothing in life that's Free and I understand that but what I'm giving up for it to be Free. It has to be something that I'm willing to give up".* Moreover, she said: "this is how you lose your identity". She reported that *"anybody who works for an any app who has a level of security now has access to all my personal information. I don't like that".* Furthermore, she said: *"I become a lot aware of where everything led and if people are making money of me, I want to know why and I want to make sure that I have control over that".*

This shows that some users are becoming more aware of the application that they hear about or use and they weigh their benefits from using an app despite their willingness to give up their personal information in return.

5.4 WARNING MESSAGES

Two participants referred seeing the permission screen to the EULA (End User License Agreement or TOS (Terms of Services). ID25 stated: *"everything you download from the Internet has one of these screens where you accept what they are planning to do".* ID22 said his reason of accepting the permissions requested by saying "*I'm just giving you an example of some software. If you install some software. Even if there is permission like lots of bunch of lines there written. We don't go through that. We just hit and check the accept mark and go through it. It is just the same thing; we are just accepting the licenses whatever it is and proceeding further".* Similarly, ID26 explained what he thinks about the permission by saying "*really this is like a shrunken privacy agreement. This is not the real privacy agreement of the application but it is like a summarization of it and most of people don't read privacy agreement because it is too long and legally. I honestly, t is unfair to the consumer because it is obviously meant to be like that. It is legally binding and it is hard to understand and at the same time it is also usually hidden away. They make it as difficult to understand as*

possible and you know consider a popular application. Facebook more than 1 billion downloads. I'm sure that a lot of people are barely read the beginning. They should be making them as simple as possible".
These are some of the reasons that warning messages why warning messages were ignored which add to what I mentioned already in Chapter 2 and 4.

5.5 WHAT'S INTERSETING

The pole of this thesis was from the Faculty of Compute Science. I thought that more participants would click on the "Permission Details" icon. Only two participants were aware of its existence. Some may say changing something can be better but I think this is not the case, this is the opposite. These hidden information should be presented in a way that can users notice it. This validates the findings from previous work [26], [31].

One might think that users who took security courses are more aware of the permissions. However, novices got higher percentage than advanced users. It is quite surprising that 19% of the Privacy Pragmatists group users would install apps quicker using the Three dots menus (see Figure 9). This means that these participants would install the application using this option without even opening the app page. On the other hand, neither of the Privacy Unconcerned and the Fundamentals considered that.

Another interesting result, is that none of the Privacy Fundamentalists would install the app and try it without looking at app description page.

With regards to the factors that users considered when downloading an app, some participants reported looking at the Blue Sign diamond symbol. That symbol acted as clue or trigger of installing any app without looking at what permissions it requests. Some participants stated that Google give this particular sign to the top developers. They also stated, if Google trusted those developers so we do trust these apps. It is important to note that the participants' view of the Blue Sign does not necessarily mean that they ignore looking at permissions.

I looked also into the old and new naming of permission groups, I based my hypotheses on Gerber et al.'s work [18]. They stated that old naming are well integrated and well described. However, with groups partitioned according to Westin's metric, both the Unconcerned and Fundamentalists groups scored higher when using the old naming. The Pragmatists scored almost the same percentage in both namings (statistically there was no difference).

Westin's metric presented interesting results. It also validated the various measure of security that were considered by participants when installing apps and deal with the Android platform in general. Again, as I stated earlier that taking security courses do not make participants more aware of what is going on. Our finding showed that the more security coursers the users have, the lower their score in the Westin's metric are. Taking security courses did not change the users' perspective regarding the three Westin's metric statements that looks into: consumers losing their control over their personal information, how businesses handle their personal data and the existing laws and organizational practices of protecting consumer's privacy.

5.6 THE FAILURE OF THE ADVANCED/NOVICE CLASSIFICATION

The results that used the classification into advanced or novice were counter-intuitive and seemed to contradict the results using the more established Westin metrics. These results could indicate something very interesting and unusual, however there is a simpler explanation. The classification was based on whether a participant had formal training in computer security, however all of the participants were computer science students so they can be assumed to be more aware of technical issues of security than members of the general population, and furthermore the security courses might not be about practical applied matters since there are several mathematically-based courses, such as cryptography, that fit the description of a “security course”. Therefore, I completely disregard the results that use the advanced/novice classification but I am leaving the details in this document as a warning to future researchers.

5.7 The Applicability of using Westin’s Metric

Westin’s metric three sets of questions are being used widely into the surveys to investigate how users’ behavior and attitudes towards privacy. Felt et al.’s [22] and Chin et al.’s [2] use the metrics in their work. More importantly, Buchanan et al.’s [67] validated the use of Westin’s metric by using it to compute the correlation among users’ privacy behavior and concerns about the Internet.

5.8 LIMITATIONS AND CHALLENGES

It is important to note that some of the collected user’s data are self-reported which might be subjective. Also, our dataset pole was limited and biased because all the participants were from the Faculty of Computer Science. They were considered as well-educated participants. Moreover, as I stated earlier that I was not able to send the recruiting email to the Faculty/Staff members due to complaints from them about receiving too many e-mail notices.

While doing the study, I noticed that some of the participants did not pay attention and read the questionnaire questions carefully. Maybe they were tired from doing the both parts of the study in one setting. Question 10 was a clear example of that. It asked participants to rank 13 factors from. It was presented in a table as can be seen in the Appendix A2. Despite the fact the great features and the ease of use that Dal Opinio had, I wish if it had supported selecting the factors from the list and drag them into another list accordingly. What I found is that some participants did the opposite and some ranked multiple factors as the most important. Because of that I could not use the collected data for that question (namely, Q10). The word choices for that question was difficult for users to differentiate what does the question really mean and how should it be answered. Some participants thought it is ranking instead of rating. I now think that a better way of asking this kind of questions is by asking about the frequencies of how participants did select a factor to install an app. This would give a better indication of the things that users would consider when installing an app. Furthermore, writing custom questions and format can be time consuming. There is no doubt that it is fairly easy to do survey on but it definitely needs to upgrade its features/capabilities.

The permission label matching questions were not equally distributed and they were not randomly selected because some of the answers will be identified if it was selected randomly. Participants will notice that.

Finally, I reflect on some cases that I could have done differently. I would have not included overlapping questions. Also, divide the study session into two sessions to avoid user's fatigue. Moreover, use another survey software that has more features. Transcribing the collected data of the audio and video recording were time-consuming process. For later work, I would consider using qualitative software's that are designed to such analysis.

5.9 MAIN FINDINGS

I described the reported findings of this thesis by showing the percentage followed by the actual number of participants who considered a particular factor or area. The total number users in each classification is: 11 advanced 16, 11 novices, 4 Privacy Unconcerned, 16 Privacy Pragmatists and 6 Privacy Fundamentalists. The findings are described as the following list:

5.9.1 Permission Detail Icon

- 92% (24) of users were not aware of the "Permission Details" Icon.

5.9.2 Reasonable Permissions

- All the Privacy Fundamentalists group were not concerned about the app cost.
- 50% (3) of the Privacy Fundamentalists and 50% (8) of the Privacy Pragmatists do care about viewing permissions.

5.9.3 Quicker to Install an App

- 19% (3) of the Privacy Pragmatists users were quicker to install an app without opening the app page. They used the Three Dots Menu shortcut.
- The entire Privacy Fundamentalists group would not install and try the app directly.

5.9.4 Security Courses

- The more security courses the users have, the lower their score are in the Westin's metric index are. It showed stronger relationship with various measures that were investigate.
- Taking security courses does not mean necessarily making users more aware of what is going on in terms of security and privacy.

5.9.5 Using Google to Find more about an App

- None of the Privacy Fundamentalists and Unconcerned groups would use Google to find more about an app.

5.9.6 Considering App Logo

- The Privacy Unconcerned group did not consider looking at the App Logo before installing an app.
- 25% of the Privacy Pragmatists and 17% of the Privacy Fundamentalist would consider looking at the App Logo.

5.9.7 Security Settings

- 83% (5) Privacy Fundamentalists were worried about the security settings.

5.9.8 Permission Presentation and Explanations

- The Privacy Unconcerned would not look for permission explanations.
- The Privacy Unconcerned thinks the current permission presentation is useful and they do not wanted it to be complicated.

5.9.9 The Differences Between the Old and New Naming of Permission Groups

- 92% (11 out of 12 questions) of the Privacy Unconcerned and 83% (15) of the Privacy Fundamentalists do like the old naming of permission groups but 54% (26 out of 48 questions) of the Privacy Pragmatists.
- 41% (5 out of 12 questions) of the Privacy Unconcerned, 50% (24 out of 48 questions) of the Pragmatists and 55% (10 out of 18 questions) of the Fundamentalists perceived the new naming of permission groups.

5.9.10 The Adoption of Security Software

- Security software was highly adapted in the PC/Laptop platform among all the classified groups.
- Security software was poorly adapted in smartphones. This finding is found too in the work of [9].
- The entire Privacy Unconcerned group did not install any security software.
- 60 % (5) of the advanced and 45% (9) of the novices do think that the security software is essential.
- The Privacy Unconcerned does not think that security software is essential.

5.9.11 Installing the Latest Firmware

- Minority of the Privacy Fundamentalists group did not install the latest firmware and 30% of them do not know about it.
- The entire Privacy Unconcerned group and also the majority of the Pragmatists group did install the latest firmware.

5.9.12 Auto Update

- Some users have misconceptions about the Auto Update and some showed superior knowledge of the Auto Update by knowing how to turn it on automatically for certain app and manually for other apps.

CHAPTER 6 CONCLUSION AND FUTURE WORK

In this thesis, I reported the implications of the permission changes in the Android permission system and what users need in Google Play Store.

I followed a two-steps procedure to conduct the study. Two classifications were used: the advanced users versus novice users based on taking security courses and Westin's metric index.

The categorization into novice/advanced does not seem to apply. I think this is because the results actually contradict the definitions. This could be because the definition of advanced was having taken security course but some of the security courses are almost all mathematics, which is not the same type of security that we intended to assess. Therefore, my conclusions are based solely on the classification of Westin's metric.

Eight of the population was aware of the "Permission Details" Icon. The experimental participants paid attention to many factors when downloading an app. Despite the fact the population pole was from the Faculty of Computer Science, still, there are various issues and misconceptions that were uncovered while users are using the Google Play Store. Gerber et al.'s [18] showed that old naming was better but that was not the case, users among all the classified groups have shown to some extent that they understand those permission groups. What I also found that both naming's work in certain cases. All of these finding is based on the users scores.

Google has to make some changes to regain users' trust. Transparency, for example might be needed to address user's privacy and security concerns.

FUTURE WORK

What was interesting that the computer science students they think they know more, which led them experiencing negative effect. Also, maybe they became habituated from seeing the warnings more often. There is a gap between what users think they know and what they need to know. Despite the fact that taking security courses did not change the perspective of some users regards how their personal information is collected. This gap needs to be addressed by educating the users.

I want to expand this work to a general audience and more divers population to see if the general public is more concerned about their privacy and security. Also, I want to consider doing heuristics by including the aspect of how users' "cultural roots" and background affect their app choices [65]. Moreover, do further analysis by creating mental models of the steps that users take before they make their final app installation decision.

REFERENCES

[1] A. Mylonas, "Exploring the user's exposure to security and privacy threats in the smartphone ecosystem,". January, p. 291, 2014.

[2] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," *Proc. Eighth Symp. Usable Priv. Secur. - SOUPS '12*, no. 1, p. 1, 2012.

[3] A. Mylonas, D. Gritzalis, B. Tsoumas, and T. Apostolopoulos, "A qualitative metrics vector for the awareness of smartphone security users," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8058 LNCS, pp. 173–184, 2013.

[4] Statista, "Global smartphone shipments forecast 2010-2019," 2015. [Online]. Available: http://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/. [Accessed: 10-Jul-2015].

[5] IDC, "Smartphone OS Market Share, 2015 Q2." [Online]. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp. [Accessed: 12-Jul-2015].

[6] I. Liccardi, J. Pato, D. Weitzner, H. Abelson, and D. De Roure, "No technical understanding required: Helping users make informed choices about access to their personal data," *Proc. 11th Int. Conf. Mob. Ubiquitous Syst. Comput. Netw. Serv. - MOBIQUITOUS '14*, vol. 1, pp. 140–150, 2014.

[7] M. Thesis and C. Science, "Fair Privacy : Improving Usability of the Android Permission System," no. August, 2015.

[8] S. Hill, "Tired of Google Play? Check out these alternative Android app stores."

[9] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, vol. 34, pp. 47–66, 2013.

[10] P. G. Kelley, "Designing Privacy Notices : Supporting User Understanding and Control Designing Privacy Notices."

[11] Developers, "Launch Checklist," 2015. [Online]. Available: http://developer.android.com/distribute/tools/launch-checklist.html. [Accessed: 14-Jul-2015].

[12] "AppBrain. Number of Android Apps." [Online]. Available: http://www.appbrain.com/stats/number-of-android-apps. [Accessed: 10-Aug-2015].

[13] App Annie, "App Annie Index: Market Q3 2015," 2015. [Online]. Available: http://blog.appannie.com/app-annie-index-market-q3-2015/. [Accessed: 14-Oct-2015].

[14] Symantec, "Internet Security Threat Report," vol. 20, no. April, p. 119, 2015.

[15] J. Lin, "Expectation and Purpose : Understanding Users ' Mental Models of Mobile App Privacy through Crowdsourcing," pp. 501–510, 2012.

[16] I. Liccardi, J. Pato, and D. J. Weitzner, "Improving Mobile App Selection through Transparency and Better Permission Analysis," no. 2, pp. 1–55, 2013.

[17] Google, "Manifest Permission." [Online]. Available: http://developer.android.com/reference/android/Manifest.permission.html. [Accessed: 10-May-2015].

[18] P. Gerber, M. Volkamer, and K. Renaud, "Usability versus privacy instead of usable privacy," *ACM SIGCAS Comput. Soc.*, vol. 45, no. 1, pp. 16–21, 2015.

[19] T. Vidas, N. Christin, and L. F. Cranor, "Curbing Android Permission Creep," *IEEE Web 2.0 Secur. Priv. Work.*, 2011.

[20] W. A. Rogers, N. Lamson, and G. K. Rousseau, "Warning Research: An Integrative Perspective," *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 42, no. 1, pp. 102–139, 2000.

[21] J. Hong, "Research Issues for Privacy in a Ubiquitously Connected World," pp. 1–20, 2014.

[22] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," *SOUPS '12 Proc. Eighth Symp. Usable Priv. Secur.*, pp. 1–14, 2012.

[23] E. Woyke, *The Smartphone ANATOMY OF AN INDUSTRY*. 2013.

[24] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, “A conundrum of permissions: Installing applications on an android smartphone,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7398 LNCS, pp. 68–79, 2012.

[25] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, “Android permissions demystified,” *Proc. 18th ACM Conf. Comput. Commun. Secur. - CCS ’11*, p. 627, 2011.

[26] R. Stevens, J. Ganz, V. Filkov, P. Devanbu, and H. Chen, “Asking for (and about) permissions used by android apps,” in *IEEE International Working Conference on Mining Software Repositories*, 2013, pp. 31–40.

[27] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos, “Permission Evolution in the Android Ecosystem,” *ACSAC ’12 Proc. 28th Annu. Comput. Secur. Appl. Conf.*, no. April 2009, pp. 31–40, 2012.

[28] M. Harbach, S. Fahl, T. Muders, and M. Smith, “Towards measuring warning readability,” in *Proceedings of the 2012 ACM conference on Computer and communications security - CCS ’12*, 2012, p. 989.

[29] “Google Play Help, Reivew permission on app download screens.” [Online]. Available: https://support.google.com/googleplay/answer/6014972?hl=en-CA. [Accessed: 10-May-2015].

[30] “Google Play Store.” [Online]. Available: https://play.google.com/store?hl=en. [Accessed: 05-Apr-2015].

[31] D. Akhawe and A. P. Felt, “Alice in warningland: a large-scale field study of browser security warning effectiveness,” *Proc. 22nd USENIX Secur. Symp.*, pp. 257–272, 2013.

[32] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as part of the app decision-making process,” *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, p. 11, 2013.

[33] B. Rashidi, C. Fung, and T. Vu, “RecDroid: A Resource Access Permission Control Portal and Recommendation Service for Smartphone Users,” *ACM MobiCom Work. Secur. Priv. Mob. Environ.*, pp. 13–18, 2014.

[34] J.Kang, H.Kim, Y.G. Chenong and J.H.Huh, "Visualizing Privacy Risks of Mobile Applications through a Privacy Meter", in ISPEC: The 11st International Conferences of Information Security Practice and Expereince, Beijing, China, Springer, May 2015

[35] M. Hettig, E. Kiss, J. Kassel, S. Weber, M. Harbach, and M. Smith, "Visualizing Risk by Example : Demonstrating Threats Arising From Android Apps," pp. 2–3, 2013.

[36] D. Barrera, P. C. Van Oorschot, and A. Somayaji, "A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android," *Security*, no. 1, pp. 73–84, 2010.

[37] A. R. Beresford, A. Rice, and N. Skehin, "MockDroid : trading privacy for application functionality on smartphones Categories and Subject Descriptors," *HotMobile '11 Proc. 12th Work. Mob. Comput. Syst. Appl.*, pp. 49–54, 2011.

[38] I. Leontiadis, C. Efstratiou, M. Picone, and C. Mascolo, "Don't kill my ads! Balancing Privacy in an Ad-Supported Mobile Application Market," *Hotmobile 2012 13th ACM Sigmobile Work. Mob. Comput. Syst. Appl.*, pp. 2:1–2:6, 2012.

[39] T. Matsudo, E. Kodama, J. Wang, and T. Takata, "A proposal of security advisory system at the time of the installation of applications on Android OS," *Proc. 2012 15th Int. Conf. Network-Based Inf. Syst. NBIS 2012*, pp. 261–267, 2012.

[40] B. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-rotaru, and I. Molloy, "Android Permissions: A Perspective Combining Risks and Benefits," *Symp. Access Control Model. Technol.*, pp. 13–22, 2012.

[41] S. Rosen, Z. Qian, and Z. Mao, "Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users," *Data Appl. Secur. Priv.*, pp. 221–232, 2013.

[42] D. Wagner and A. G. Play, Do Android users write about electric sheep? examining consumer reviews in Google Play. In Consumer Communications and Networking Conference (CCNC), 2013 IEEE, pages 149–157. IEEE, 2013.

[43] M. Silic and J. Barlow, "Warning! A Comprehensive Model of the Effects of Digital Information Security Warning Messages," pp. 1–32, (2015)

[44] L. F. Cranor, "A Framework for Reasoning About the Human in the Loop," *Proc. 1st Conf. Usability, Psychol. Secur.*, pp. 1:1–1:15, 2008.

[45] A. P. Felt, "Towards Comprehensible and Effective Permission Systems," *UC Berkeley Diss.*, 2012.

[46] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "'Little Brothers Watching You': Raising Awareness of Data Leaks on Smartphones," *SOUPS '13 Proc. Ninth Symp. Usable Priv. Secur.*, pp. 12:1–12:11, 2013.

[47] S. Egelman, L. F. Cranor, and J. Hong, "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," *Proceeding twenty-sixth Annu. CHI Conf. Hum. factors Comput. Syst. - CHI '08*, p. 1065, 2008.

[48] J. Green and N. Thorogood, *Qualitative Methods for Health Research*. 2009.

[49] "Dal Opinio Software." [Online]. Available: https://surveys.dal.ca/opinio/admin/folder.do. [Accessed: 10-Jun-2015].

[50] W. Gordon, "Everything You Need to Know About Rooting Your Android Phone," 2013. [Online]. Available: http://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone. [Accessed: 05-Aug-2015].

[51] L. Bauer, C. Bravo-lillo, L. Cranor, and E. Fragkaki, "Warning Design Guidelines,", Pittsburgh, PA: Carnegie Mellon University. 2013.

[52] P. Kumaraguru and L. Cranor, "Privacy indexes: A survey of westin's studies," *Sch. Comput. Sci. Carnegie Mellon Univ.*, vol. Tech. rep., no. December, pp. 1–22, 2005.

[53] R. Kumar, *Research Methodology*. 2011.

[54] D. Howell, "Statistical methods for psychology," *books.google.com*, p 284-286, 2009.

[55] Y. Tian, B. Liu, W. Dai, B. Ur, P. Tague, and L. F. Cranor, "Supporting Privacy-Conscious App Update Decisions with User Reviews," *Proc. 5th Annu. ACM CCS Work. Secur. Priv. Smartphones Mob. Devices*, pp. 51–61, 2015.

[56] F. Shih, I. Liccardi, and D. J. Weitzner, "Privacy Tipping Points in Smartphones Privacy Preferences," *Proc. 2015 ACM Conf. Hum. factors Comput. Syst.*, pp. 807–816, 2016.

[57] Google, "Android 6.0 Marshmallow." [Online]. Available: http://developer.android.com/about/versions/marshmallow/index.html. [Accessed: 10-Jan-2016].

[58] R. Hooly, "CAREFUL WHAT YOU WISH FOR Using App Permissions in Android M." [Online]. Available: http://www.androidcentral.com/using-app-permissions-android-m?utm_source=related&utm_medium=module&utm_campaign=next. [Accessed: 15-Dec-2015].

[59] C. Toombs, "Android M Will Never Ask Users For Permission To Use The Internet, And That's Probably Okay." [Online]. Available: http://www.androidpolice.com/2015/06/06/android-m-will-never-ask-users-for-permission-to-use-the-internet-and-thats-probably-okay/. [Accessed: 10-Dec-2015].

[60] Google, "Platform Versions Used." .2015. [Online]. available: http://developer.android.com/about/dashboards/index.html. [Accessed: 15-Dec-2015].

[61] R. Ritchie, "Switch to iPhone for years of free software updates," 2015. [Online]. Available: http://www.imore.com/switch-iphone-years-free-software-updates. [Accessed: 15-Dec-2015].

[62] O. Hamwi, "Android N: everything you need to know." [Online]. Available: https://www.androidpit.com/android-n-release-date-news-features-name. [Accessed: 17-Mar-2016].

[63] S. Pötzsch, "Privacy Awareness: A Means to Solve the Privacy Paradox?," *Futur. Identity Inf. Soc.*, vol. 298, no. 216483, pp. 226–236, 2008.

[64] A. Adams and M. A. Sasse, "Privacy in multimedia communications: protecting users not just data," in *People and Computers XV — Interaction without Frontiers*, 2001, pp. 49–64.

[65] J. D. Gould and C. Lewis, “Designing for Usability: Key Principles and What Designers Think,” *Commun. ACM*, vol. 28, no. 3, pp. 300–311, 1985.

[66] C. Joo, Seolwoo, Hwang, “Mobile banking vulnerability: Android repackaging threat,” 2012. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2012/05/mobile-banking-vulnerability-android-repackaging-threat. [Accessed: 01-Mar-2016].

[67] T. Buchanan, C. Paine, A. N. Joinson, and U. D. Reips, “Development of measures of online privacy concern and protection for use on the Internet,” *J. Am. Soc. Inf. Sci. Technol.*, vol. 58, no. 2, pp. 154–165, 2007.

[68] L. Dogruel, S. Joeckel, and N. D. Bowman, “Choosing the right app: An exploratory perspective on heuristic decision processes for smartphone app selection,” *Mob. Media Commun.*, vol. 3, no. 1, pp. 125–144, 2015.

APPENDIX A1: App Selection Tasks Interview Script & Questions.

Interview Script

Welcome to my study. My name is Adel. Thank you for coming. I need to read this script to everyone so I know that they have heard the same basic information. Before I begin, let me tell you some important information about the study. I will be recording what is said in this interview as well as the video recording of the smartphone that you will use, but everything will be anonymous. Your name and identifying information will be stored separately from your comments. The study will take approximately one hour.

Please think out loud as you go through the tasks. That is, tell us what you are thinking as you go. My goal is to evaluate the Google Play Store; not you. Everything you say, including confusion and questions, is very valuable to us.

Imagine that a family member or friend has just acquired an Android. They would like your advice on which applications they should install. [I will select from the scenarios and give them a printed copy]. Please take a minute to choose someone and tell me his or her relationship to you.

Android Introduction:

I will ask participants basic questions about their Android experience to create a welcoming start and understand their familiarity with the system.

- Can you tell me why did you choose to buy an Android Phone? Is it for technical features? Apps or liked the look or other?
  Live wallpaper, customizable, widgets.

General new smartphone advice:

- What advice they would give to a hypothetical friend, someone less tech-savvy, who has just gotten a brand new smartphone
- What pitfalls they should avoid?
- What applications every smartphone user should have?

Specific new smartphone advice:

I will continue the scenario, asking my participants to think about the same friend, but that friend is now looking for two specific applications:

- Word games for killing time- “ I really like word games like Scrabble, but it would be great to have a few things on there for when I need to kill time”.
- Nutrition/Health- “ I keep dieting but an app that helped me keep track of calories would be great”.
- Music-“ I like to listen to music but don’t have a large music collection myself.”
- Flight tracking: - “ I fly a lot, but I still get a bit anxious and I want to be able to track my flights”.

- Scanning receipts: " I frequently have to travel for work, and am so bad about keeping all my receipts together, is there an app that helps me scan in may receipts and save them?"
- Twitter- "My friends keep telling me I should use Twitter more, and I do like to follow some celebrities with it, but I don't just want to use the main Twitter app."

I will then ask them if they have any specific advice or application they would recommend for each category. If they weren't sure, I will ask them what their strategy for finding an application for the category would be.

Application-selection task:

After verbalizing their suggested application and strategies I will provide them with a Google CyanogenMod smartphone, which I will say this is your friend's new phone. During this application search process, I will ask participants to think aloud while they while using the Google Play Store. Also, I will instruct them as well to tell me what they were reading and considering while selecting and installing the two apps. Moreover, I will observe what user interface elements they interacted with.

Post-explanation task:

Why they choose the application that they did and what they would have done differently in their life?

If participants did not consider permissions during the installation, I will ask them for her or her opinion after the installation task.

Do you check permissions before installing an app or after and why?
Is Auto Update on or off and why?
How would you check the permission changes after receiving an update?

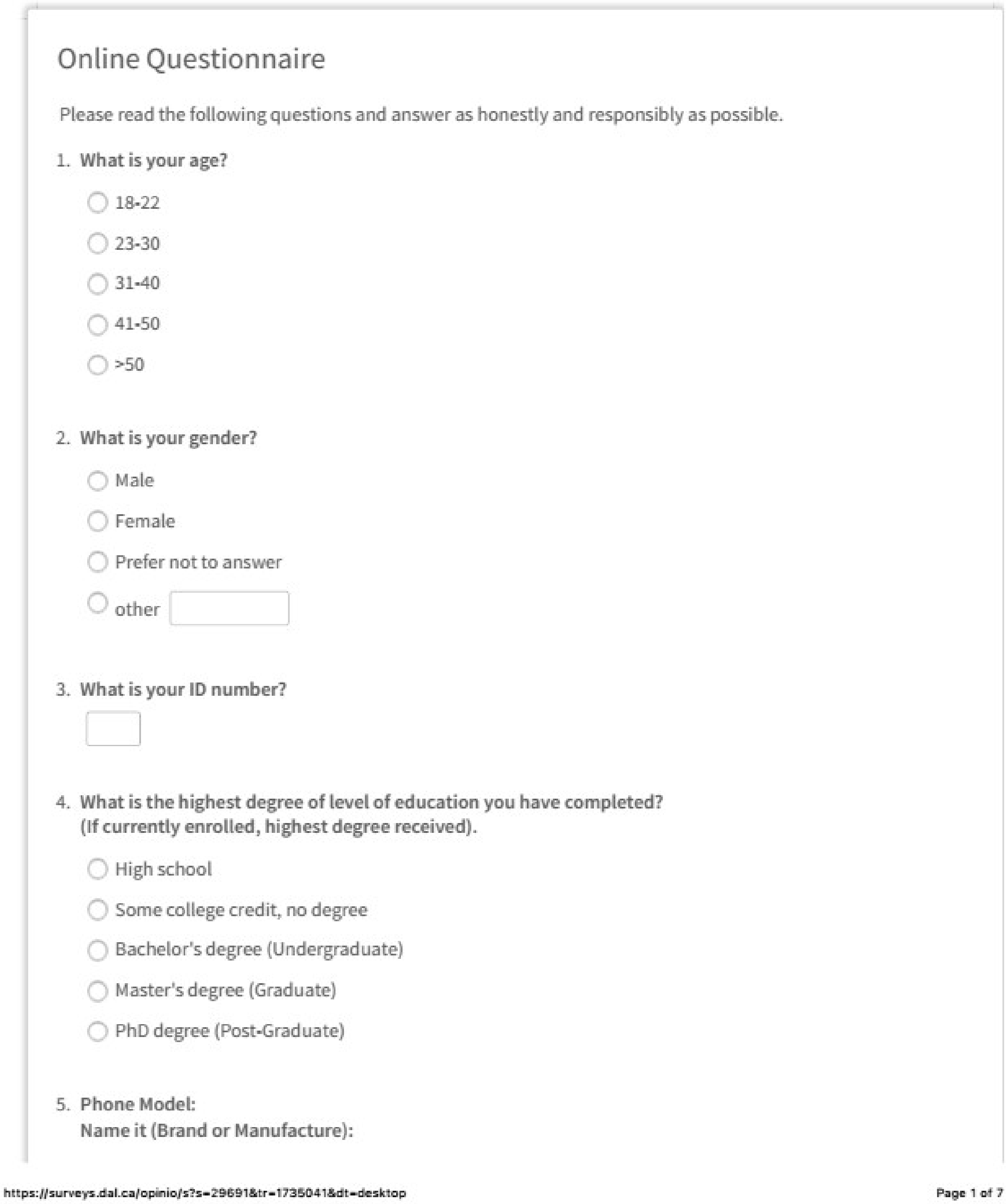
Where would you go if you want to check for permissions or look for explanations? Are they going to look for it within the Google Play Store? Or they will navigate the web, online blogs.

Can you please tell me how would you want the permissions to be presented? To be clear and easy to understand.

What are the changes or features that you want to see on Google Play Store?

Finally, can you please fill an online questionnaire?

APPENDIX A2. Online Questionnaire



Online Questionnaire

Please read the following questions and answer as honestly and responsibly as possible.

1. **What is your age?**

   ○ 18-22

   ○ 23-30

   ○ 31-40

   ○ 41-50

   ○ >50

2. **What is your gender?**

   ○ Male

   ○ Female

   ○ Prefer not to answer

   ○ other ▭

3. **What is your ID number?**

   ▭

4. **What is the highest degree of level of education you have completed? (If currently enrolled, highest degree received).**

   ○ High school

   ○ Some college credit, no degree

   ○ Bachelor's degree (Undergraduate)

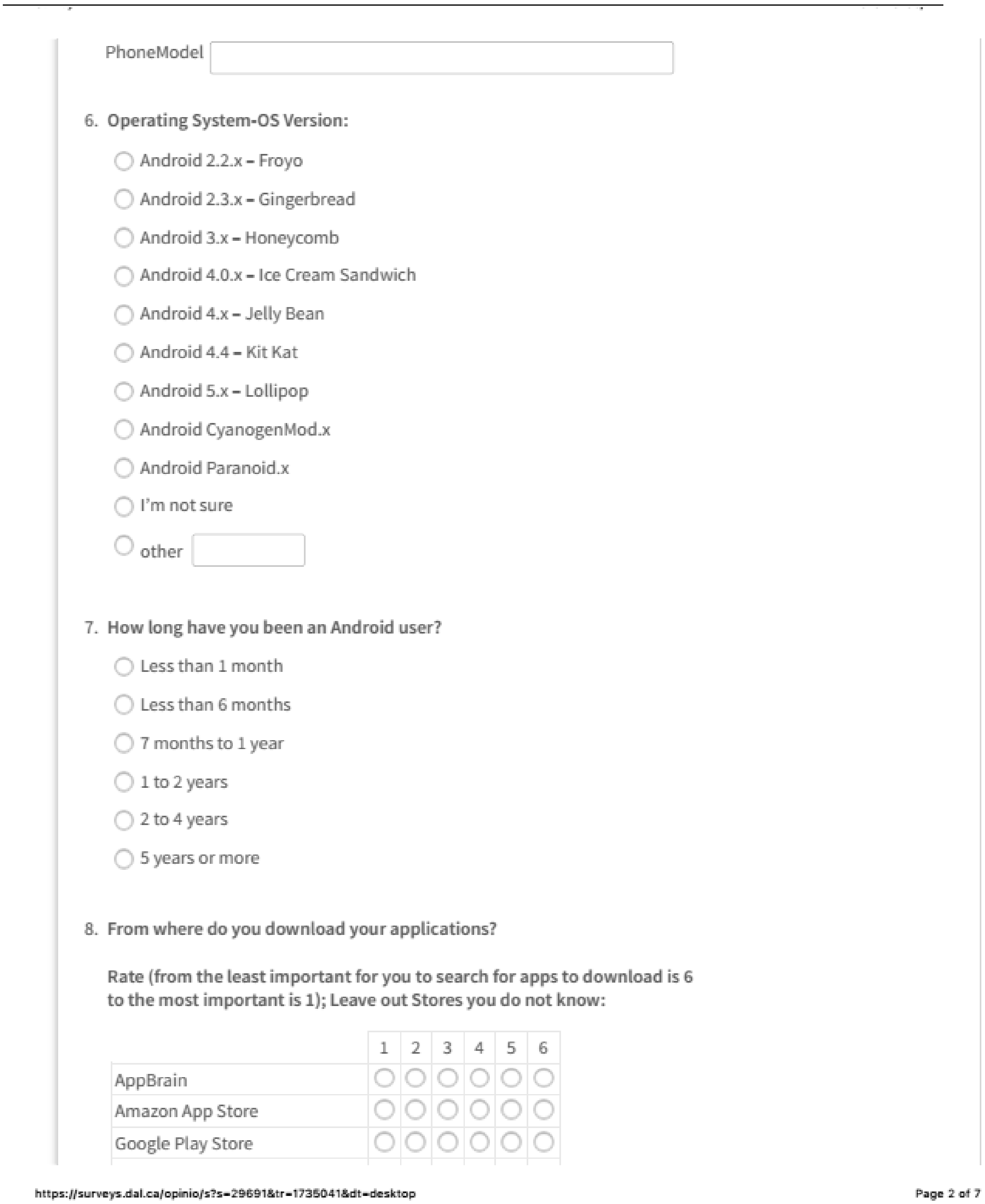
   ○ Master's degree (Graduate)

   ○ PhD degree (Post-Graduate)

5. **Phone Model:**
   Name it (Brand or Manufacture):

https://surveys.dal.ca/opinio/s?s=29691&tr=1735041&dt=desktop

Page 1 of 7



PhoneModel

6. **Operating System-OS Version:**

○ Android 2.2.x – Froyo

○ Android 2.3.x – Gingerbread

○ Android 3.x – Honeycomb

○ Android 4.0.x – Ice Cream Sandwich

○ Android 4.x – Jelly Bean

○ Android 4.4 – Kit Kat

○ Android 5.x – Lollipop

○ Android CyanogenMod.x

○ Android Paranoid.x

○ I'm not sure

○ other

7. **How long have you been an Android user?**

○ Less than 1 month

○ Less than 6 months

○ 7 months to 1 year

○ 1 to 2 years

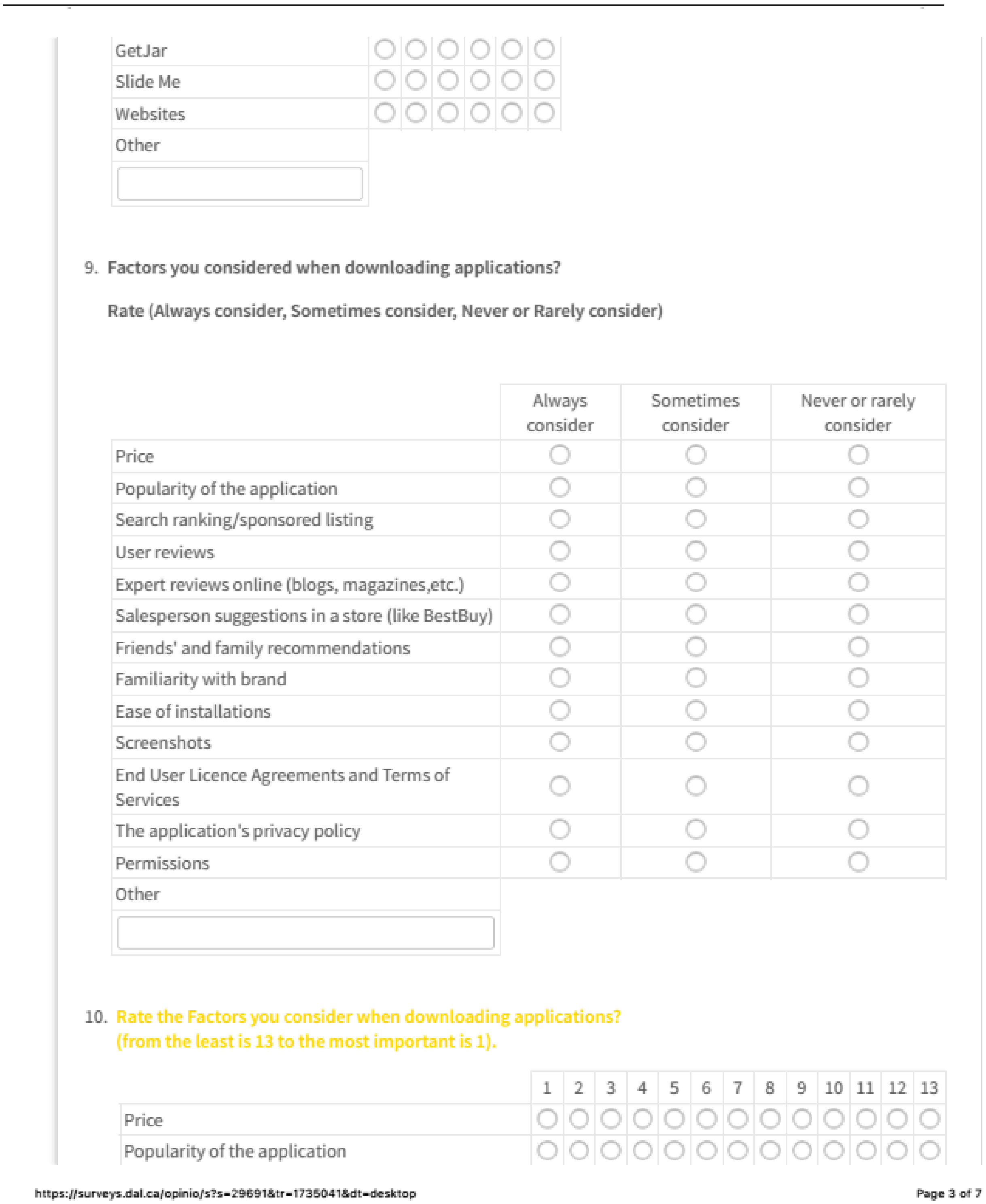
○ 2 to 4 years

○ 5 years or more

8. **From where do you download your applications?**

Rate (from the least important for you to search for apps to download is 6 to the most important is 1); Leave out Stores you do not know:

	1	2	3	4	5	6
AppBrain	○	○	○	○	○	○
Amazon App Store	○	○	○	○	○	○
Google Play Store	○	○	○	○	○	○



GetJar	○	○	○	○	○	○
Slide Me	○	○	○	○	○	○
Websites	○	○	○	○	○	○
Other						

9. **Factors you considered when downloading applications?**

Rate (Always consider, Sometimes consider, Never or Rarely consider)

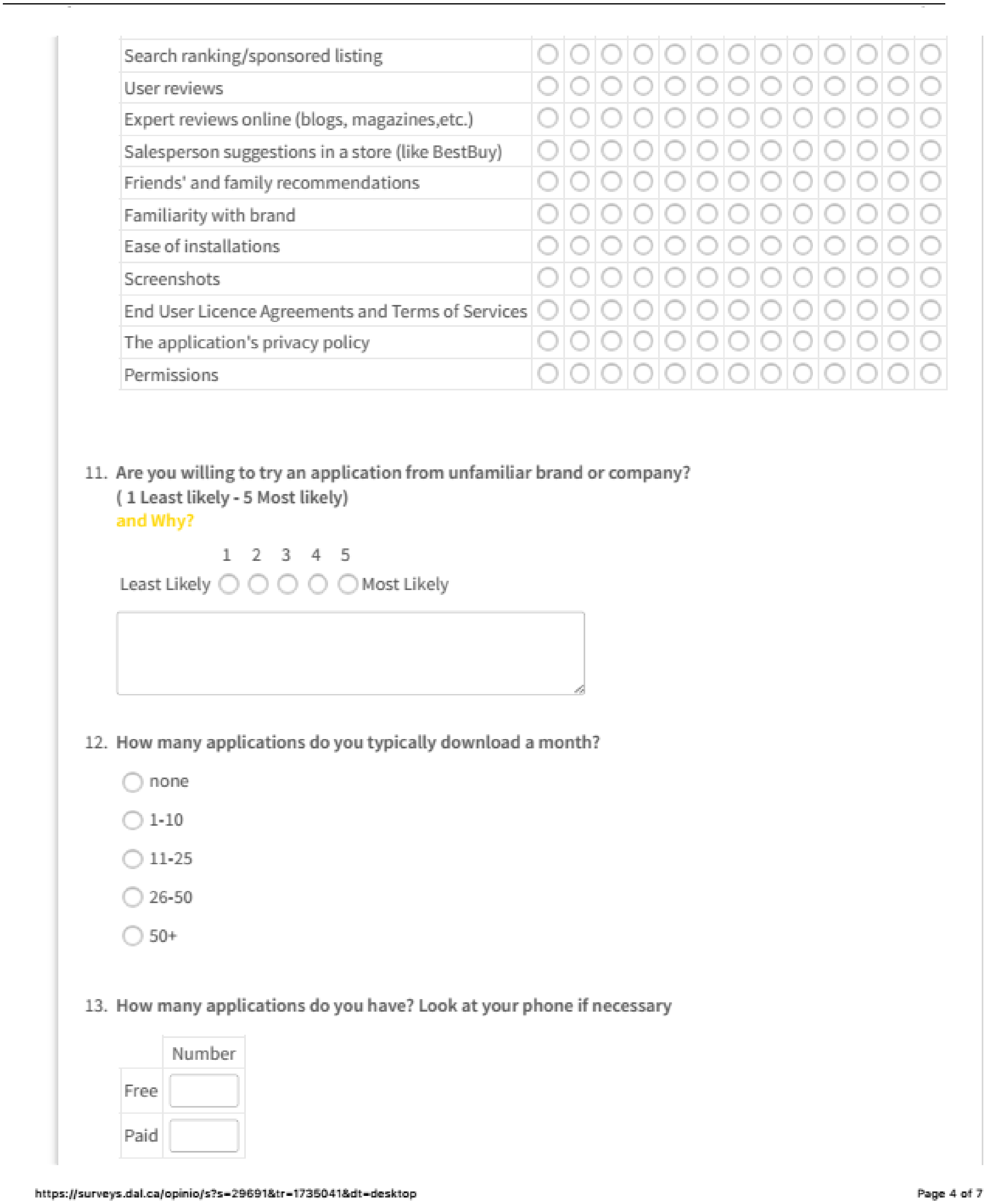
	Always consider	Sometimes consider	Never or rarely consider
Price	○	○	○
Popularity of the application	○	○	○
Search ranking/sponsored listing	○	○	○
User reviews	○	○	○
Expert reviews online (blogs, magazines,etc.)	○	○	○
Salesperson suggestions in a store (like BestBuy)	○	○	○
Friends' and family recommendations	○	○	○
Familiarity with brand	○	○	○
Ease of installations	○	○	○
Screenshots	○	○	○
End User Licence Agreements and Terms of Services	○	○	○
The application's privacy policy	○	○	○
Permissions	○	○	○
Other			

10. **Rate the Factors you consider when downloading applications? (from the least is 13 to the most important is 1).**

	1	2	3	4	5	6	7	8	9	10	11	12	13
Price	○	○	○	○	○	○	○	○	○	○	○	○	○
Popularity of the application	○	○	○	○	○	○	○	○	○	○	○	○	○

https://surveys.dal.ca/opinio/s?s=29691&tr=1735041&dt=desktop

Page 3 of 7



Search ranking/sponsored listing	○	○	○	○	○	○	○	○	○	○	○	○	○
User reviews	○	○	○	○	○	○	○	○	○	○	○	○	○
Expert reviews online (blogs, magazines,etc.)	○	○	○	○	○	○	○	○	○	○	○	○	○
Salesperson suggestions in a store (like BestBuy)	○	○	○	○	○	○	○	○	○	○	○	○	○
Friends' and family recommendations	○	○	○	○	○	○	○	○	○	○	○	○	○
Familiarity with brand	○	○	○	○	○	○	○	○	○	○	○	○	○
Ease of installations	○	○	○	○	○	○	○	○	○	○	○	○	○
Screenshots	○	○	○	○	○	○	○	○	○	○	○	○	○
End User Licence Agreements and Terms of Services	○	○	○	○	○	○	○	○	○	○	○	○	○
The application's privacy policy	○	○	○	○	○	○	○	○	○	○	○	○	○
Permissions	○	○	○	○	○	○	○	○	○	○	○	○	○

11. **Are you willing to try an application from unfamiliar brand or company?**
(1 Least likely - 5 Most likely)
and Why?

	1	2	3	4	5	
Least Likely	○	○	○	○	○	Most Likely

12. **How many applications do you typically download a month?**

○ none

○ 1-10

○ 11-25

○ 26-50

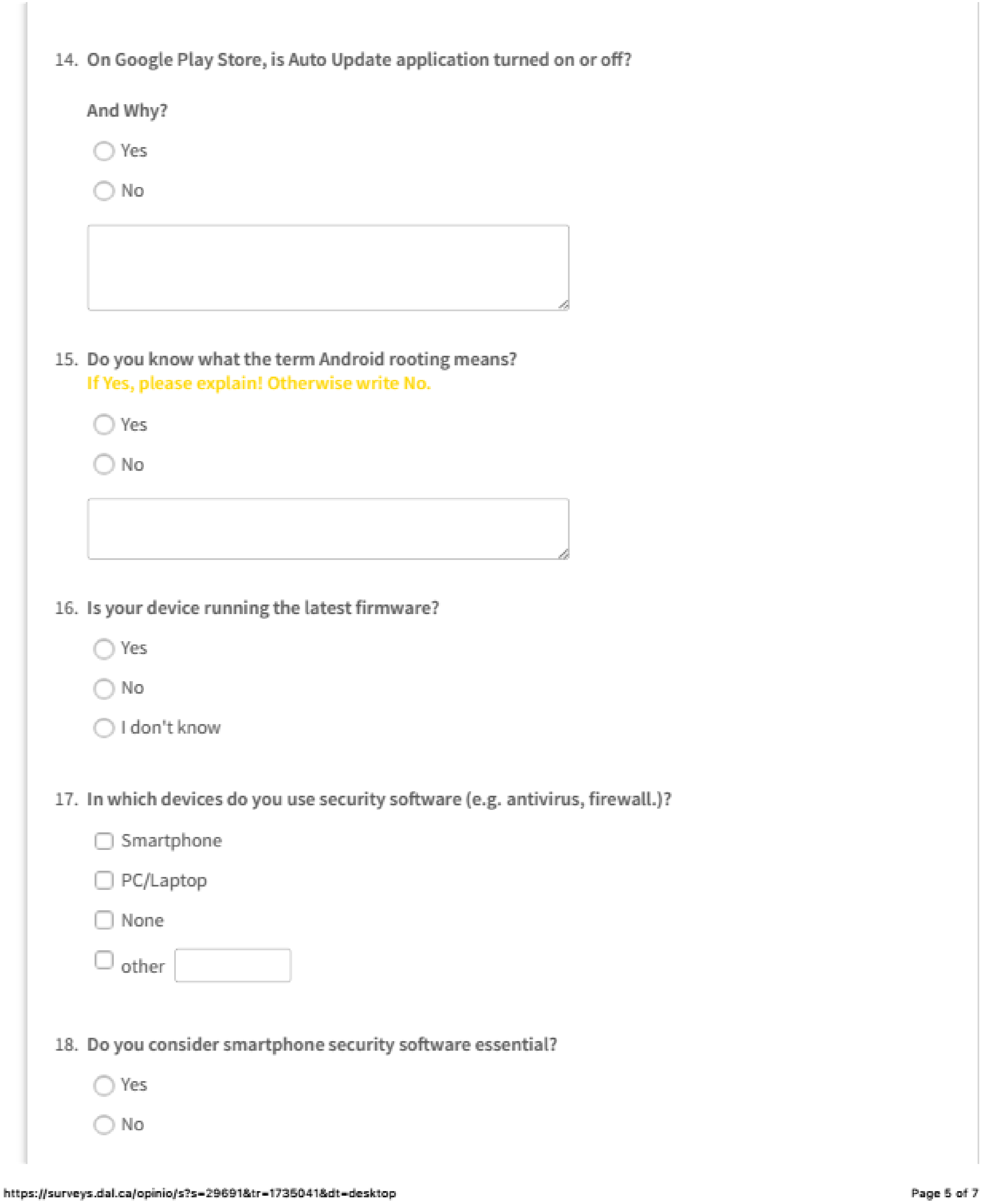
○ 50+

13. **How many applications do you have? Look at your phone if necessary**

	Number
Free	
Paid	

https://surveys.dal.ca/opinio/s?s=29691&tr=1735041&dt=desktop

Page 4 of 7



14. On Google Play Store, is Auto Update application turned on or off?

And Why?

○ Yes

○ No

15. Do you know what the term Android rooting means?
If Yes, please explain! Otherwise write No.

○ Yes

○ No

16. Is your device running the latest firmware?

○ Yes

○ No

○ I don't know

17. In which devices do you use security software (e.g. antivirus, firewall.)?

□ Smartphone

□ PC/Laptop

□ None

□ other

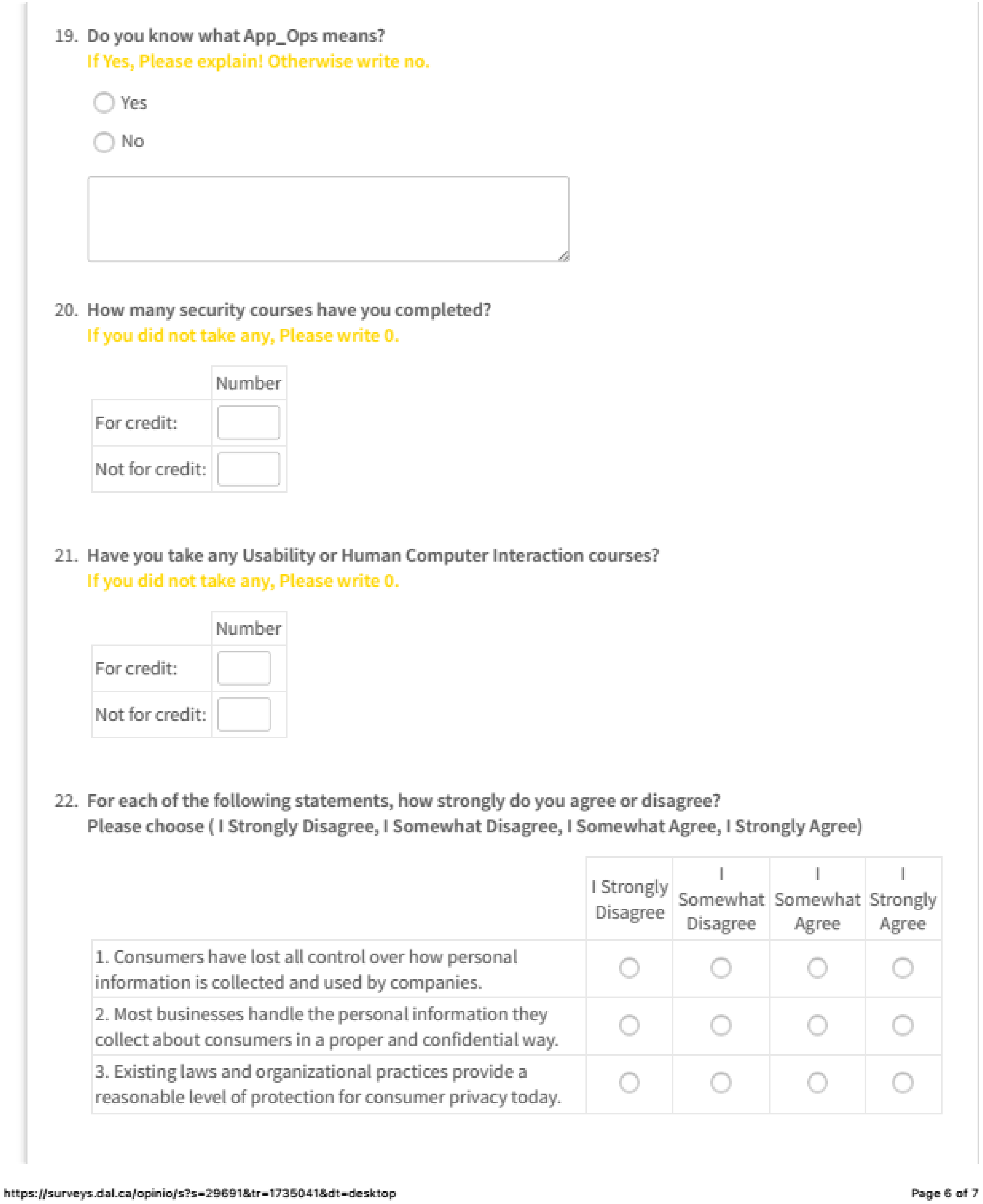
18. Do you consider smartphone security software essential?

○ Yes

○ No

https://surveys.dal.ca/opinio/s?s=29691&tr=1735041&dt=desktop

Page 5 of 7



19. Do you know what App_Ops means?
If Yes, Please explain! Otherwise write no.

○ Yes

○ No

20. How many security courses have you completed?
If you did not take any, Please write 0.

	Number
For credit:	
Not for credit:	

21. Have you take any Usability or Human Computer Interaction courses?
If you did not take any, Please write 0.

	Number
For credit:	
Not for credit:	

22. For each of the following statements, how strongly do you agree or disagree?
Please choose (I Strongly Disagree, I Somewhat Disagree, I Somewhat Agree, I Strongly Agree)

	I Strongly Disagree	I Somewhat Disagree	I Somewhat Agree	I Strongly Agree
1. Consumers have lost all control over how personal information is collected and used by companies.	○	○	○	○
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	○	○	○	○
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○

https://surveys.dal.ca/opinio/s?s=29691&tr=1735041&dt=desktop

Page 6 of 7

APPENDIX B1: Letter of Approval

Social Sciences & Humanities Research Ethics Board

Letter of Approval October 07, 2015
Mr Adel Al-Hejaili
Computer Science\Computer Science

Dear Adel,

REB #: 2015-3643

Project Title: Exploring the Implications of the Changes of Presenting Android Permissions on Google Play Store to End Users

Effective Date: October 07, 2015 **Expiry Date:** October 07, 2016

The Social Sciences & Humanities Research Ethics Board has reviewed your application for research involving humans and found the proposed research to be in accordance with the Tri-Council Policy Statement on *Ethical Conduct for Research Involving Humans.* This approval will be in effect for 12 months as indicated above. This approval is subject to the conditions listed below which constitute your on-going responsibilities with respect to the ethical conduct of this research.

Sincerely,

Dr. Karen Beazley, Chair

APPENDIX B2: Amendment Approval Letter

DALHOUSIE
UNIVERSITY
Inspiring Minds

Social Sciences & Humanities Research Ethics Board
Amendment Approval October 19, 2015
Mr Adel Al-Hejaili
Computer Science\Computer Science

Dear Adel,

REB #: 2015-3643
Project Title: Exploring the Implications of the Changes of Presenting Android Permissions on Google Play Store to End Users

The Social Sciences & Humanities Research Ethics Board has reviewed your amendment request received October 15,2015 and has approved this amendment request effective today, October 19, 2015.

Sincerely,

Dr. Karen Beazley, Chair