IMPROVING SMARTPHONE PERMISSION ACCESS DISCLOSURES

by

HUIQING FU

A dissertation submitted to the

Graduate School-New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

written under the direction of

Prof. Janne Lindqvist

and approved by

New Brunswick, New Jersey

October 2017

ABSTRACT OF THE DISSERTATION

Improving Smartphone Permission Access Disclosures

By HUIQING FU

Dissertation Director: Prof. Janne Lindqvist

Modern day smartphones have access to unprecedented levels of user privacy data. Naturally, privacy concerns and protection from security breaches, create considerable challenges to designers as well as increase the responsibility of end-users. To address these challenges, this work focuses on 1) how to effectively supply feedback to users about their private data access on their phones and 2) how to help users make informative decisions based on this feedback. Supplying effective run-time disclosures can help users effectively be aware of their personal data's usage by apps on their phones without distracting them from their main task. By extracting the most useful information pertaining to data exposure would save users time and allow them to make informative decisions about their own apps' data access.

First, we explored the run-time disclosures of location access on Android phones and carried out a four-week field study. The study suggested that our run-time disclosures were effective in informing users of their apps' location access and had helped users to take actions to control their apps' location access on their phones. Second, we conducted an online survey to investigate Android users' understandings and privacy expectations of the location permissions on Android phones. The survey showed that users had a varied understanding of the approximate location permissions and their attitudes toward the privacy protection of the approximate location depended on their understanding of location accuracy. Third, we carried out a two-week field study to investigate the effectiveness of run-time disclosures with control options of apps' permissions request on Android phones. The permission field study showed that almost all of the participants would like to receive run-time disclosures about their apps' permission request. The participants liked the instant control options; however, too many and too frequent run-time disclosures were considered interruptive and decreased participants' willingness to read the disclosure contents and take effective action.

ACKNOWLEDGEMENTS

I would like to thank all the people who provided me support and help during my PhD study. First, I would like to express my deep gratitude to my advisor, Prof. Janne Lindqvist, for his continuous support, guidance and encouragement.

This material is based upon work supported by the National Science Foundation under Grant Numbers 1223977, 1228777 and 1211079. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

I also sincerely thank my other dissertation committee members: Prof. Wade Trappe, Prof. Yanyong Zhang, and Dr. Bernhard Firner. Thanks for their constructive suggestions on my research work and this dissertation.

I would like to thank group members: Can Liu, Xianyi Gao, Yulong Yang, Fengpeng Yuan, Gradeigh D. Clark. I would like to thank Prof. Marco Gruteser, Prof. Darcy Gioia, Dr. Feixiong Zhang, Dr. Chenren Xu, Dr. Xiruo Liu, Dr. Zhuo Chen, Bin Cheng, Ying Liu, Dr. Kai Su.

Finally, I would like to thank my family for their love, support and understanding.

TABLE OF CONTENTS

ABSTRACT ii

ACKNOWLEDGEMENTS iv

LIST OF TABLES viii

LIST OF FIGURES x

CHAPTER 1. INTRODUCTION 1
1.1 Overview 1
1.2 Organization 3
1.3 Contributions 4

CHAPTER 2. BACKGROUND AND RELATED WORK 7
2.1 Usable Security 7
2.2 Mobile Phone Security & Privacy 8
2.3 Default Android Location Access Disclosure 9
2.4 Disclosures of Data Access 10
2.5 The Conflict of Transparency and Disruption in Run-time Notifications . . . 14
2.6 Android Permissions Understanding and Improvements 15
2.7 Location Privacy 19

CHAPTER 3. A FIELD STUDY OF RUN-TIME LOCATION ACCESS DISCLOSURES ON ANDROID SMARTPHONES 22
3.1 Overview of Chapter 22
3.2 Method 25
3.2.1 Heuristic Discovery of All Apps' Location Access 25
3.2.2 User Interface Main Features and Interventions 27
3.2.3 Recruitment and Participants 31
3.2.4 Experiment Design 33
3.3 Results 35
3.3.1 Description of Collected Dataset 35

3.3.2 Overview of Participants' Apps on Their Phones 36
3.3.3 Apps Unexpected to Access Location 39
3.3.4 Comparison of Effectiveness of Run-time Disclosures and Other Disclosures 41
3.3.5 Comparison of Transparency Experience between two Groups 46
3.3.6 Common Findings: Tradeoffs with Privacy and Utility in the Two Groups 48
3.3.7 Attitudes and Suggestions to Our Run-Time Location Access Disclosures 49
3.4 Summary 52

CHAPTER 4. GENERAL AREA OR APPROXIMATE LOCATION? HOW PEOPLE UNDERSTAND LOCATION PERMISSIONS 53
4.1 Overview of Chapter 53
4.2 Method 55
4.2.1 Participants 56
4.2.2 Online Survey Design 57
4.3 Results 60
4.3.1 Understandings of Precise Location and Approximate Location 60
4.3.2 Location Privacy Model of the Approximate Location 62
4.3.3 Demographics Effects on Attitudes toward Location Privacy 66
4.4 Summary 68

CHAPTER 5. FIELD STUDY OF RUN-TIME PERMISSION REQUEST DISCLOSURES AND CONTROL 69
5.1 Overview of Chapter 69
5.2 Method 72
5.2.1 Recruitment and Participants 72
5.2.2 Run-time Disclosures Design and Implementation 73
5.2.3 Procedure 78
5.3 Results 82
5.4 Summary 97

CHAPTER 6. DISCUSSION 99
6.1 Field Study of Run-Time Disclosure Findings and Limitations 99
6.2 Online Survey of Location Permissions Findings and Further Work 103
6.3 Run-Time Permissions Request Disclosures and Control Findings 104

CHAPTER 7. CONCLUSION 105

BIBLIOGRAPHY 107

LIST OF TABLES

3.1 No Disclosure Group: Number of apps, which accessed location during the study, and number of apps participants did not expect to access their location. 39

3.2 Disclosure Group: Number of apps, which accessed location during the study, and number of apps participants did not expect to access their location. 40

3.3 Different Major Findings in Two Groups 46

4.1 Demographic of Participants 56

4.2 Breakdown of participants' understandings of the accuracy of network-based location and GPS location. The percentage of results is highlighted by *italic* which fell in the given answers of accuracy of GPS location and network-based location. 61

4.3 Breakdown of the responses in the location accuracy on screenshot of Maps. The correct answers are marked using the *italic*. 62

4.4 The above 7-point Likert scale was collapsed here into a 3-point scale: agree, disagree or neutral. Similarly, "first time percentage" indicate answers prior to the ground truth and "second time percentage" after seeing the ground truth. 64

4.5 Reasons respondents explained why approximate location could protect location privacy. 64

4.6 Reasons respondents explained why approximate location could *not* protect location privacy. 65

5.1 Summary of participants' reactions towards run-time disclosures. They were grouped into two stages. 92

5.2 Summary of each participant reactions towards the run-time disclosures. They were grouped into 11 participants. 93

5.3 Summary of reactions of each participant in the 1st stage. In the 1st stage, the options of OK and NotOK were not available. So, we did not show OK and NotOK options in this table. 94

5.4 Summary of reactions of each participant in the 2nd stage. In the 2nd stage, the option “setupList” was not available. So, we did not show this “setupList” option in this table. 95

LIST OF FIGURES

2.1 One version of the existing Android location access disclosure (Google Nexus with Android 4.2.2). On the top left corner, the symbol gets filled and unfilled when the foreground app uses *GPS* localization. Different versions and vendors of the Android platform have used different kind of symbols, for example, a blinking satellite on the right side of the notification bar. Our research (as anticipated) indicates that this is not an effective disclosure. 9

3.1 Main screen of the study app. Users can click "Show location access history per application" to see the list of apps (see Figure 3.2) that have accessed location during the study. Users also can give use feedback via "leave voice mail" or "send email". They can disable the vibration of notification in the notice bar and the pop-up notifications on the screen. 27

3.2 Users can see the history records of apps that have accessed location during the study. The list has app's name, app's icon and the latest time the app updated location. User can click a specific app to see the history of all locations this app has accessed on a map. Also, users can click the button "Show location access history for all apps" to see the history of all locations all apps in the list have accessed on a map (see Figure 3.4). 28

3.3 Example of "notifications on the screen" location disclosure we implemented with the "toast" functionality of the Android platform. The disclosure overlays briefly over the app the notification that "Your location is being accessed by [app name]." It also shows the icon of the app, and a map. Depending on the phone's settings, the app will also vibrate the phone and play a soft sound. 29

3.4 Example of “map of location accessed by a specific app.” It shows the location Google Maps accessed in the Boston area. During pre-trials one tester was visiting Boston and needed to navigate by walking in the Boston downtown and another location. The pins show the areas where Google Maps accessed his location. 29

3.5 Example of the location access disclosure implemented to the Android notice bar. Location access disclosure appeared in the Android Notifications List, which is expanded by pulling the Notification Bar downwards. 30

3.6 Number of installed location based apps and all apps on participants’ phones in the **Disclosure group**. 37

3.7 Number of installed location based apps and all apps on participants’ phones in the **No Disclosure group**. 38

3.8 Number of used location based apps and all used apps on participants’ phones in the **Disclosure group**. 38

3.9 Number of used location based apps and all used apps on participants’ phones in the **No Disclosure group**. 39

3.10 How many times each participant in the Disclosure group received a notification that their location is being accessed divided to second, third, and fourth week of participation. (Recall, we would start the notifications after first week of participation, and the Notification Bar based notification could not be disabled.) 44

3.11 How many times each participant in the Disclosure group used some of the major features of the study app: the listing of all apps that accessed the participant’s location, the map of any one app listed to be accessing locations, and the map of all location accesses by all apps. 50

4.1 Shows the “precise” location permission, which enables apps to localize the phone with both GPS and network-based (WiFi and cell-tower) methods. 54

4.2 Shows the “approximate” location permission. This permission enables only network-based localization, and the recent API updates also include limited random obfuscation for the location. 54

4.3 Screenshots of GPS localization on an Android smartphone using Google Maps. The yellow star depicts the Android phone’s exact location, and the blue circle is the location accuracy area. The map’s scale is 100ft / 20m. 58

4.4 Screenshots of WiFi localization on an Android smartphone using Google Maps. The yellow star depicts the Android phone's exact location, and the blue circle is the location accuracy area. The map's scale is 200ft / 50m. 59

4.5 Screenshot of cellular network-based localization on an Android smartphone using Google Maps. The map's scale is 2000ft / 500m. 59

4.6 Breakdown of "approximate location helps to protect location privacy" responses prior to showing the ground truth (1st) and after showing the ground truth (2nd). The participants' responses were limited to a 7-point Likert scale. 63

4.7 Breakdown of "approximate location helps to protect location privacy" responses in the 1st and 2rd time in female and male respondents respectively on 7-point Likert Scale. We obtain the percentage using 58 and 48 the total number of female and male respondents respectively as the base. 67

5.1 The main screen of the study app shows a general summary of the three permissions. It shows the number of apps requesting each of the three permissions: LOCATION, CONTACTS or INTERNET as well as the number of apps installed on the phone. 76

5.2 The setup list for LOCATION permission shows all the apps that request LOCATION permission. The button can be switched between OK or NotOK. 76

5.3 The run-time disclosure dialog in the first stage. The dialog has two options: PermissionDetail and setupList. 77

5.4 The run-time disclosure dialog in second stage. The dialog has three options: OK, NotOK and PermissionDetail. 77

5.5 The screenshot of permission details. It shows major permissions the app requests. It has two buttons: "Show Others," "Close and Back." When "Show Others" button is clicked all the left permissions will be shown. When "Close and Back" button is clicked the permission details window will be closed and the run-time disclosure dialog will be shown again. 79

5.6 The number of permissions each participant chose to be notified in the future. 86

5.7 The number of participants choose each permission to be notified in the future. 87

5.8 Summary of participants' reactions towards run-time disclosures. They were grouped into two stages. 92
5.9 Summary of each participant reactions towards the run-time disclosures. They were grouped into 11 participants. 93
5.10 Summary of reactions of each participant in the 1st stage. In the 1st stage, the options of OK and NotOK were not available. So, we did not show OK and NotOK options in this figure. There was no reaction in "Others", so this option was not shown in this figure. 95
5.11 Summary of reactions of each participant in the 2nd stage. In the 2nd stage, the option "setupList" was not available which was not shown in this figure. There was no reaction in "Others", so this option was not shown in this figure. 96

CHAPTER 1

INTRODUCTION

1.1 Overview

According to PewResearch (Research, 2014) as of January 2014, 58% of American adults have a smartphone. Smartphones have become ubiquitous devices with a diverse array of functions and applications, known as apps. For example, Google Play for Android and the Apple App Store for the iPhone report having over 1M apps and 50 billion downloads. The apps on the smartphones are used to perform common routine functions such as phone calls, MSG, web surfing, email, banking, games and social network. They have the potential ability to access large number of users' private data such as pervasive location data, contacts information and photos. How can users enjoy the convenience of these apps at the same time protect their personal data usage by these apps? The fundamental methods of protection might be awareness of data usage and control of data access.

The smartphone platforms have tried to inform users of apps' privacy-sensitive data usage by providing installation-time app capability disclosures ("permissions") on the Android platform, and by providing first-time usage requests on the iPhone platform. Previous work (Felt, Ha, et al., 2012; Kelley et al., 2012; Kelley, Cranor, & Sadeh, 2013) had explored the effectiveness of the permissions on Android phones.

Their results suggested that permissions at install time were not effective in informing users of the apps' data access. An online survey (Fisher, Dorner, & Wagner, 2012a) was also carried out to investigate the usage of privacy data access control on the iPhone. It analyzed collected data to show that users have diverse setups for apps' location requests. Our study was different from the previous studies in that we explored the effectiveness of self-designed run-time location access disclosures in a field study from users' daily life. We collected participants' reactions and afterwards interviewed them to learn why they took these actions.

Smartphone apps have unprecedented access to users' location. Since such location apps are very popular, disclosures of user location data access from such apps are of great interest. The smartphones as in-pocket devices enabled the apps to obtain locations for each site visited by users. Pew Research reported that about three quarters (74%) of smartphone users used their phones to receive location based services (Zickuhr, 2013). Location data access on smartphones was a concern to users (Balebako, Shay, & Cranor, 2013).

We aimed to investigate effective disclosure methods to inform users of their private data requests by apps on their own phones. At first, we explored the effectiveness of self-designed run-time location access disclosures on users' phones. We believed that users could not take the right actions until they had been aware of how their apps expose their location data. If they took actions due to our run-time disclosures, we could further to interview the reasons they took actions. The features of our run-time disclosures could be considered to improve the future design of private data access disclosures on smartphones.

Secondly, we carried out an online survey to explore end users' understandings of the two location permissions on Android phones and their location privacy models. It turned out an existing description of the two location permissions misled some participants. These participants were overly confident of the location privacy protection ability of the approximate location. To summarize, how end users understand the private data accessed by app and how they can obtain more effective and clear disclosure information to take informative actions are all topics we explored in this work.

We carried out a two-week field study on the run-time disclosures with control options of apps' permissions request. We found out that all the participants, except one, would like to have run-time disclosures about apps' permission request. They chose several permissions to be notified at run-time and preferred the instant control options available. However, too many notifications were interruptive. There should be a trade-off with transparency and interruption. Participants preferred one disclosure dialog with all concerned permissions for each app.

1.2 Organization

Chapter 2 will describe the related work and background for disclosures of data access on users' devices. In addition, it will present the current state of studies based on smartphone privacy and security. Chapter 3 details the heuristics of our run-time location access disclosures and a 4-week field study including study design, recruitment, participants, and results of the study. Chapter 4 will present the online survey of end users' understanding of location permissions on Android phones and their privacy models. Chapter 5 will describe the two-week field study of run-time permissions request disclosures and control. Chapter 6 are discussions.

1.3 Contributions

In summary, the contributions of our work to the disclosures of privacy data access on smartphones are as follows:

1. We design and implement a more effective run-time disclosure of apps' location access on users' phones. This method could detect all apps' location updates on users' Android phones. It included both run-time disclosures: notifications in the notice bar and toast on screen; and history disclosures: a list of history records and maps of all locations requested by the apps.

2. Transparency of location access by apps brought by our run-time disclosures were appreciated by participants. Participants would like to know the location request in detail. When a location was reported being requested, participants would like to know the details about which app requested the location at where, why and how often the app requested the location. They only expected and accepted the app to request location when it was performing the required functions.

3. Feedback based on the run-time disclosure features from participants could help to improve future designs of private data access on smartphones. Participants would like to have both run-time and history disclosures. The run-time disclosures should be obvious but not intrusive to disrupt users' regular tasks. A

corresponding convenient privacy setup tools would be necessary since our participants had the willingness to manage their apps' location access. They had already tried various actions to manage their apps' location access during the field study.

4. Understanding of the kind of data apps requested, namely permissions, were important for participants making privacy related decisions. Our survey suggested that Android users were misled by the approximate location permission descriptions and put too much trust in the approximate location's privacy protection ability. An improved permission presentation scheme can combine both a visual image such as maps example and accuracy descriptions. The accuracy of an approximate location was varied in the responses. The confidence in the location privacy protection of an approximate location was affected by the participants' expectation of the location's accuracy. Users shared the same understanding of the precise location as the "exact location" which suggested that literal descriptions were much easier to follow for common users. However, if there were diverse understandings of the same literal descriptions, there should be more methods included to clarify the meaning of the permissions.

5. Participants would like to receive run-time permission request disclosures with control options. Almost all of participants, except one, selected several permissions to be notified at run-time. They liked the instant control options. Too many too frequently run-time disclosures were considered interruptive and decreased participants' willingness to read the contents and take effective reac-

tions. Most of participants clicked NotOK or OK without purpose. They just wanted to dismiss the dialog as soon as possible. Participants preferred one disclosure dialog to show all the concerned permissions for each app.

CHAPTER 2

BACKGROUND AND RELATED WORK

In this chapter, we will discuss the relevant background pertaining to smartphone security and privacy, current Android location access disclosures, studies about disclosures of data access to users, Android permissions understanding and improvements proposed by previous work.

2.1 Usable Security

The field of usable security informs our research. For example, Zurko et al. (Zurko, Kaufman, Spanbauer, & Bassett, 2002) found that while users by default was not to allow running unsigned applications; but when they were faced with a choice during their work, they would allow unsigned content to run. Bravo-Lillo et al. (Bravo-Lillo, Cranor, Downs, & Komanduri, 2011) and Wash (Wash, 2010) worked on understanding people's mental models related to security. Stoll et al. (Stoll, Tashman, Edwards, & Spafford, 2008) and Raja et al. (Raja, Hawkey, Hsu, Wang, & Beznosov, 2011) implemented desktop and firewall visualizations. Hong et al. (Hong & Landay, 2004) implemented a framework to help application developers to build privacy-sensitive applications such as enhanced instant messaging clients. These works inform our design of a disclosure about privacy data access to inform users to make the right decisions.

2.2 Mobile Phone Security & Privacy

Becher et al. (Becher et al., 2011) presents an overview of mobile phone security history and developments, Anderson et al. studied different application markets and installation mechanisms (Anderson, Bonneau, & Stajano, 2010), and several authors have written position papers about application markets (McDaniel & Enck, 2010; Gilbert, Chun, Cox, & Jung, 2011; Barrera & Van Oorschot, 2011; Wetherall et al., 2011). Considerable effort has been made in understanding Android security and permissions (Chin, Felt, Greenwood, & Wagner, 2011; Enck, Octeau, McDaniel, & Chaudhuri, 2011; Felt, Greenwood, & Wagner, 2011; Felt, Chin, Hanna, Song, & Wagner, 2011; Felt, Wang, Moshchuk, Hanna, & Chin, 2011), and hardening the Android security model (Ongtang, McLaughlin, Enck, & McDaniel, 2009; Ongtang, Butler, & McDaniel, 2010; Shabtai, Fledel, & Elovici, 2010; Enck, Ongtang, & McDaniel, 2009). Recently, static taint analysis has been used to analyze leaks from iPhones (Egele, Kruegel, Kirda, & Vigna, 2011) and dynamic taint analysis from Android (Enck et al., 2010). AppFence (Hornyack, Han, Jung, Schechter, & Wetherall, 2011), MockDroid (Beresford, Rice, Skehin, & Sohan, 2011), and TISSA block data leaking to a network by faking the capabilities of the phone so that potential sensitive data cannot be retrieved. Chin et al. (Chin, Felt, Sekar, & Wagner, 2012) studied user confidence in smartphone security and privacy. Felt et. al. (Felt, Egelman, Finifter, Akhawe, & Wagner, 2012) proposed a set of guidelines for developers to determine the appropriate permission-granting mechanism. Fisher et al. (Fisher et al., 2012a) studied iPhone location request settings with Amazon Mechanical Turk (AMT). Fi-

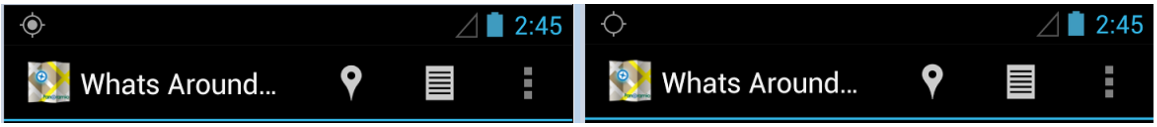


Figure 2.1: One version of the existing Android location access disclosure (Google Nexus with Android 4.2.2). On the top left corner, the symbol gets filled and unfilled when the foreground app uses *GPS* localization. Different versions and vendors of the Android platform have used different kind of symbols, for example, a blinking satellite on the right side of the notification bar. Our research (as anticipated) indicates that this is not an effective disclosure.

nally, Lin et al. (Lin et al., 2012) studied people's expectations of mobile applications with AMT surveys, and proposed a new installation time interface design.

Kang et al. study (Kang, Dabbish, Fruchter, & Kiesler, 2015) suggested that participants with different technical knowledge took similar protective actions towards their online data. Participants who had negative experiences, such as privacy breach or financial data breach, took more actions to protect their private data. Our study about permission request disclosures finding was consistent with their work. Participants in the permission study who found out a virus app scanning all downloaded documents were more concerned about storage access by apps. Their work focused on personal Internet privacy protection my work were about mobile phone data request disclosures.

2.3 Default Android Location Access Disclosure

The run-time location access disclosure examples on Android 4.0 as of November 2013 is depicted in Figure 2.1. We discovered that only GPS-based localization indicates that the user's location is being accessed. We tested this on the latest Google Nexus 4 running Android 4.2.2, and considerable older versions such as Samsung Galaxy S

–AT&T, running 2.1– update1, and Android GPSbuddy, running Android 3.2.6. We implemented separate simple apps that would localize the phone with 1) GPS and 2) network-based localization methods. Also, we disabled and enabled WiFi and cell tower based localization accordingly to try out both separately.

The default run time GPS (or Satelite) icon blinking in the notice bar on Android phones could not disclose most of the location request. The study by Baokar (Baokar, 2016) suggested that less than 1% of location requests were notified by a GPS icon in the notification bar. They mentioned that "66.1% of location request used TelephonyManager from cell tower information 33.3% used WiFi SSIDs." In our study on run-time location disclosures, the GPS icon were not effective to inform users about location request. Their study supported our findings from another viewpoint. Too few location request (less than 1%) were explicitly shown by the GPS icon. *In contrast, our approach discloses the location access with any active localization method (e.g. GPS, WiFi, network) available on Android platforms.*

We note that in recent versions of the iPhone iOS platform, users will receive a notification asking them if they would like to allow apps to access location (Fisher et al., 2012a). The notification is shown only once when the first time the apps request to access location.

2.4 Disclosures of Data Access

A lot of focus on revealing sensor data to users has been in the domain of social location-sharing studies. However, the studies (Ludford, Priedhorsky, Reily, & Terveen, 2007; Quentin Jones and Sukeshini A. Grandhi, 2005; Barkhuus et al., 2008;

Heyer, Brereton, & Viller, 2008; Patil & Lai, 2005; Tsai et al., 2009; Consolvo et al., 2005; Lederer, Mankoff, & Dey, 2003; K. P. Tang, Lin, Hong, Siewiorek, & Sadeh, 2010; Schlegel, Kapadia, & Lee, 2011; Jedrzejczyk, Price, Bandara, & Nuseibeh, 2010; K. P. Tang et al., 2010) have focused on the implications of exposure and utility to share location and other data with family, friends and colleagues. Schlegel et al. (Schlegel et al., 2011) used pairs of growing eyes to represent different groups who query users' location. The results of their lab study showed that giving visual feedback to people was at least as effective as giving feedback with a detailed disclosure interface. Jedrzejczyk et al. (Jedrzejczyk et al., 2010) explored the real-time feedback effects on users' behaviors by implementing a location-sharing social app Buddy Tracker. They qualitatively identified criteria for acceptance of the real-time feedback in social apps including trustworthiness, appropriate timing and minimal intrusiveness. Tsai et al. (Tsai et al., 2009) developed Locyoution, a location sharing system, and carried out a field study dividing participants into two groups: one group received location access history feedback while the other group did not receive feedback. Their results showed that disclosing the *history* of location accesses helped to reduce participants' privacy concerns and made them more comfortable about sharing location information with this particular app. We included a history feature in our study app which showed a map of locations accessed by the apps used by the participants. Hsieh et al. (Hsieh, Tang, Low, & Hong, 2007) explored the design of privacy controls and different feedback mechanisms using IMBuddy. Their study indicated that giving immediate notifications about which of the participants' friends had accessed their location worked well for contextual instant messaging. In our approach, we included run-time disclosure notifications in the Android's notice bar in addition to flashing them on the screen. We explored how run-time location access disclosures would affect participants' attitudes and responses to apps they already had or would install by their own choice. In contrast to our work, the above projects have focused on studying social location sharing with one selected app. Their participants were asked to use the specific app for social sharing.

Researchers have also studied disclosures with WiFi and desktop sensor accesses. Consolvo et al. (Consolvo et al., 2010) implementedn a WiFi Privacy Ticker, which displays information about sensitive data sent from the computer to the network, and the study indicated that this introduced changes to users' behavior when using WiFi. Howell et al. (Howell & Schechter, 2010) proposed a sensor-access widget model which could inform users of personal data being collected by corresponding sensors, but they did not implement their model. Tam et al. (Tam, Reeder, , & Schechter, 2010) studied different designs for disclosures of data authorized to a desktop application. In their lab study, the disclosure design had very little effect on participants' ability to understand the disclosure content, and most participants preferred disclosures using images or icons.

Recently, Jung et al. (Jung, Han, & Wetherall, 2012) and Balebako et al. (Balebako, Jung, Lu, Cranor, & Nguyen, 2013) ran laboratory studies related to run-time feedback. They found that participants were surprised by how often different data types were accessed by two game apps, which were the focus of the study. In contrast to the studies discussed above, to the best of our knowledge, we have conducted the first field study (Fu, Yang, Shingte, Lindqvist, & Gruteser, 2014) on run-time location access disclosures. Our field study was carried out on participants' own Android phones during their daily lives, and our method would disclose how any app accessed participants' location.

Schaub et al. (Schaub, Balebako, Durity, & Cranor, 2015) presented six timing schemes and three control methods in design space for private data access disclosure. The six timing schemes included "at setup, just-in-time, context-dependent, periodic, persistent and on demand." Our field studies mainly focus on just in time disclosure about data access on an Android phone. The three control methods were "blocking, non-blocking and decoupled." Ours were either non-blocking, namely no control, or blocking control methods. Different timing of permission request schemes was investigated by several works. The study by Balebako et al. (Balebako, Schaub, Adjerid, Acquisti, & Cranor, 2015) showed that information can hardly be recalled by users if it was shown only in the app store.

Some studies investigated the effects of grouping of information. Waddell et al. study (Waddell, Auriemma, & Sundar, 2016) found out that their paraphrased end user license agreement was considered more appealing and easier to understand than the traditional EULA. Their paraphrased EULA were short summary sentences appearing in different group windows. Gerber et al. study (Gerber, Volkamer, & Renaud, 2015) suggested that the Android grouping permission screen launched in 2014 did not enable users to make informative decisions. They gave an example: an app only requested the CAMERA permission was expressed unclearly as "Uses at least one of the following elements: camera, microphone."

Zhang et al. study (Zhang, Wu, Kang, Go, & Sundar, 2014) suggested that when the website did not have a security cue participants were less concerned about the privacy threats. By contrast, the website with security cue encouraged more social media information sharing. The security cue was a warning message about the lack of a trusted security certificate. They designed four versions of a fake mobile website called “City Food Map” with or without security or gratification cues.

2.5 The Conflict of Transparency and Disruption in Run-time Notifications

Users would like to have transparency about their data access. Some setting assistant apps might be helpful to manage the data access. Shklovski et al. study (Shklovski, Mainwaring, Skúladóttir, & Borgthorsson, 2014) showed that participants privacy concerns were high, but their actions were very few. Participants had various explainations to continue using the apps and allowing data access (Shklovski et al., 2014). Most of participants would like to have transparency about data usage on their smartphones. Our studies were consistent with their findings about transparency. Participants in our location access disclosure study (Fu et al., 2014) appreciated the transparency brought by the run time notifications. Almost all the participants in our permission study would like to receive run-time disclosures about two or more kinds of data access.

Users would like to have control over their data usage on their phones. The study by Wijesekera et al. (Wijesekera et al., 2015) suggested that at least 80% of participants (36) in the field study would have denied at least one permission request. Participants would have blocked 35% of 423 permission requests during the study. In our permissions run-time disclosure field study, all the participants selected two or more permissions to be notified at run time.

Some studies explored users' reactions and feelings about the run-time notifications. The study by Mehrotra et al. (Mehrotra, Pejovic, Vermeulen, Hendley, & Musolesi, 2016) suggested that notifications with useful information could cause disruption. Our study's findings were consistent with their results. Participants in our permission run-time disclosure study thought that the study apps' disclosure dialogs were interruptive. The work by Dan et al. (Tasse, Ankolekar, & Hailpern, 2016) suggested that pop ups with quick reactions were rated significantly more annoying than other visual user interface elements which were used to grab users' attention. Participants in our study on permission run-time disclosures had similar opinions as their counterparts and complained of the pop up disclosure dialogs annoyance.

The study by Sarma et al. (Sarma et al., 2012) showed that permissions in the dangerous groups defined in Android Developers sites were requested by less than 25% of benign apps (158,062 Android apps). This means that in 10 apps only two or three apps will be notified by a summary list of dangerous permission requests.

2.6 Android Permissions Understanding and Improvements

A lot of previous works have studied the Android permission scheme and tried to improve the permission design.

Some previous work has reported that users lack the ability to understand the permissions' meaning. Felt et al. (Felt, Ha, et al., 2012) study showed that only 3% of their online surveyed Android users could understand correctly the permission' exact meanings. Kelly et al. (Kelley et al., 2012) carried out an interview to explore end users understanding of permissions. According to the 20 participants' responses, they found that most participants did not have an accurate knowledge of the 10 permissions they chose from an existing Android permission list. However, participants knew that "file (GPS) location" was the exact location. But most participants were confused about the "coarse location." They reported qualitative ideas of the "coarse location" permission such as "...not know difference between the GPS, but basically where you are at." and "...I haven't the foggiest idea of what that means...." Our study reported both qualitative and quantitative results from an online survey with 106 responses. We also reported the attitudes according to respondents' knowledge of the location permission.

Users usually do not pay attention to or even understand the meaning of "permission" or "disclosure" at the installation time (Tam et al., 2010; Kelley et al., 2013; Felt, Ha, et al., 2012). We want to figure out other methods that can help users be aware of the private data being accessed and help users have a good sense of location access within the context of when, where and which application is accessing their location. Also, in our study, we include the application's icon combined with the app's name in the "pop-up notification" and "list of apps which accessed location" features, which can help users know which app is accessing location visually.

There are several proposals to improve the permissions to help users make better privacy decisions when installing a new app. Kelley et al. (Kelley et al., 2013) designed a "Privacy Facts" checklist for helping users to make privacy decisions when downloading apps from the app market. Their results suggested that users tended to choose apps with fewer permissions with the help of the checklist. Harbach et al. (Harbach, Hettig, Weber, & Smith, 2014) extended the previous work of Kelley et al. (Kelley et al., 2013) by visualizing the permissions' data with images of daily life scenarios. Their results showed that the personalized examples of daily life images help users to take more privacy into consideration while deciding which app to install. Rosen et al. (Rosen, Qian, & Mao, 2013) used static analysis to create high-level behavior profiles of application behavior, and to summarize how users' privacy might be impacted. Similarly, Lin et al. (Lin et al., 2012) studied people's expectations of mobile applications with Amazon Mechanical Turk, and proposed how crowdsourcing could be used to create better installation-time privacy summaries. We aimed to evaluate the effectiveness of run-time location disclosure to inform users of their apps' location data access. We were interested in whether disclosing apps' location data access at run-time would help users to make more informed decisions.

Some studies investigate the influence of permission request schemes on participants' sharing behaviors. Tan et al. ran an online survey and suggested that showing reasons for permission requests increase the approving possibility of the request significantly (Tan et al., 2014). Shih et al. (Shih, Liccardi, & Weitzner, 2015) carried out a four-week study. In their study, the effect of different factors on participants' willingness to share was evaluated. The factors included data collection purpose, apps usage frequency, apps type and context. They found out that the main factor influencing participants' willingness to divulge and share data was when no purpose to the data collection was presented. Zhang and Xu's (Zhang & Xu, 2016) carried out an online experiment using MTurk to investigate permissions interfaces nudge techniques on Android platform. They compared the effects of social nudges with approval percentage in users, frequency nudge with access rate of the app and no nudge as the traditional permission interfaces. They found out that the social nudges were the most effective to ease users' concern and increase their comfort level to share data.

Liu et al. (Liu et al., 2016) implemented an app Personalized Privacy Assistant to give participants different privacy settings for permission access on their rooted Android phones. The app classified Android users to different privacy profiles and generated personalized recommendations to deny permissions access. Their study showed that most of participants who completed the exit interview thought the recommendations were useful for configuration and decision support. Some participants would like to manually manage their apps' permission request.

Some studies tried to improve the traditional Google Play Store app installation interface. They added a score for the apps permissions to help users make installation decisions. Liccardi et al. (Liccardi, Pato, Weitzner, Abelson, & De Roure, 2014) launched an online survey with 125 Android Smartphone users. Their study embedded a sensitivity score (Liccardi, Pato, & Weitzner, 2014) in the Google Play Store app installation interface. The INTERNET permission sensitivity score was calculated using the number of personal data permissions. Otherwise, the sensitivity score was zero because the app did not have the ability to disclose the personal data (Liccardi, Pato, & Weitzner, 2014). Their survey suggested that the sensitivity score could help those participants, with a lower understanding level of permissions, to choose apps with a fewer number of personal data permissions. Participants tended to choose apps with a shorter list of permissions using the traditional Google Play Store interface. Some apps with a long list of permissions might have a low sensitivity score. The study by Gates et al. (Gates, Chen, Li, & Proctor, 2014) suggested that more participants chose the app with a lower risk score, when showing the Risk interface, than when showing the Standard interface. They calculated the risk score according to how many permissions the app requested. The Risk interface showed the risk score for each app. The standard interface was like the Google Play Store interface. In our field study on permission run-time disclosures, there was a summary of the number of permissions the app requested. In our study, participants did not pay attention to the number of permissions. The reason might be that with no second similar app to compare to, participants could not understand what the number meant.

2.7 Location Privacy

There have been several studies related to the privacy of smartphone users. Generally, a survey by Balebako et al. (Balebako, Shay, & Cranor, 2013) indicated that smartphone users were concerned about how their apps accessed their location. In a lab study by Felt et al. at least one participant decided not to install an app due to "exact location" permission (Felt, Ha, et al., 2012).

Knijnenburg et al. (Knijnenburg, Kobsa, & Jin, 2013) studied users' location sharing preference in coarse-grained and fine-grained location sharing options. Half of the participants(N=291) selected different granularity locations including name of place and general location such as city. We want to know if approximate location permission has some effect in the users' attitudes toward location privacy. The study by Tang et al. (K. Tang, Hong, & Siewiorek, 2012) showed that supplying more options encourages sharing history location using social network apps. We explore if Android phone's approximate location helps to release users' privacy concern when sharing location.

Some Android users had refused to install apps that ask for location permission and some users uninstalled apps after they knew some apps unexpectedly access their location (Fu et al., 2014).

Different location granularity can affect participants' willingness to share. For example, Leon et al. study showed that only 4% of participants (of 2912) were willing to share their exact current location with advertising companies; however, about one fourth were willing to share their zip code and town or city information (Leon et al., 2013). A previous lab study (N=25) showed that at least one participants decided not to install an app due to the "exact location" permission (Felt, Ha, et al., 2012) and another participant claimed, "most people are more hesitant about installing apps that reveal your location."

The work by Janice et al. suggested that location was a concern for a lot of smartphone users. (Janice, Burke, & Linda, 2014) and a large percentage of smartphone users had turned off the location tracking on their phones.

Kraus et al. carried out a survey (Kraus, Wechsung, & Möller, 2014) with 154 participants. They did not find a correlation between gender and privacy concern. Their findings were consistent with our online survey study (Fu & Lindqvist, 2014) which found that it was not significantly different between female and male participants related to the location protection expectations of approximate location.

CHAPTER 3

A FIELD STUDY OF RUN-TIME LOCATION ACCESS DISCLOSURES ON ANDROID SMARTPHONES

3.1 Overview of Chapter

Smartphone apps provide several useful ways for people to extend the capabilities of their phones. Both Google Play for Android and Apple App Store for iPhone report having over 1M apps and 50 billion downloads. These numbers indicate that people find these apps valuable. Unfortunately, as popular press and research (Barrera & Van Oorschot, 2011; Chin et al., 2011) has shown, there are considerable security and privacy risks with these apps.

Users are concerned of their location privacy. Caine (Caine, 2009) reported "location" as top private type of information. Location privacy risks are of particular interest since 74% smartphone users use location-based services (Zickuhr, 2012). According to Pew Research, almost one fifth of smartphone users (of 2254 respondents) had disabled location access features on their phones because they were concerned of location accesses by other individuals or companies (Boyles, Smith, & Madden, 2012). In another survey, more than 70% of participants desired to know about location data collection by apps on mobile devices (Balebako, Shay, & Cranor, 2013).

The smartphone platforms have tried to inform users of apps' privacy-sensitive data usage by providing installation-time app capability disclosures ("permissions") on the Android platform, and by providing first-time usage requests on the iPhone platform. There is already a body of research indicating that Android's approach is not effective, because people do not pay attention to the permission interfaces (Felt, Ha, et al., 2012; Kelley et al., 2012, 2013). The approach used by iPhone has so far been studied only with an Amazon Mechanical Turk survey (Fisher et al., 2012a). This survey reported that iPhone users' decisions were very diverse: 40 participants (out of 273) accepted all apps' location requests, most participants allowed at least two-thirds of such requests, and one participant denied all location requests. A recent laboratory study (Balebako, Jung, et al., 2013) evaluated run-time feedback of location and device ID leaks. The participants were surprised by the leaks from the two game apps chosen by the investigators. In summary, there have been no studies on how people react to run-time disclosures during their daily lives with their own smartphones and apps.

To the best of our knowledge, in this chapter we present the first field study of run-time location access disclosures on the Android platform. Towards the end of conducting the study, we designed and implemented a novel app, which enabled us to detect if any other app was accessing the participant's location. Our aim was to evaluate the effectiveness of run-time location access disclosures during participants' daily lives. In particular, we sought to understand how these disclosures affect users' attitudes and actions towards their apps.

We randomly divided our participants (N=22) into two groups. The Disclosure group (N=13) received run-time disclosures of apps' location access, and the No

Disclosure group (N=9) received no additional disclosures. We report the following major findings in this chapter.

> We confirm that the Android platform's location access disclosure is not effective to inform users of apps' location access. Participants who received no additional disclosures (No Disclosure group) did not take any actions to manage their apps to limit location accesses.
>
> Our run-time location access disclosure is effective compared to Android's location access disclosure. Prior to participating in our study, our participants were not aware of how many apps accessed their location and how often each app could access location. Our approach effectively informed the Disclosure group participants about apps' location accesses and their frequency.
>
> Participants in the Disclosure group took various actions to manage their privacy.
>
> Participants appreciated the transparency brought by our run-time disclosure method. They wanted to continue receiving the notifications after completing the study.
>
> Most participants reported having trade-offs between location privacy and the convenience of using their apps. We observed that some participants would rather give up the convenience to protect their location privacy.

3.2 Method

We sought to study how our location disclosures would work during people's daily lives with their own Android devices. We initially evaluated the possibility to use e.g. Taintdroid (Enck et al., 2010) as a basis to carry out the field study. Unfortunately, Taintdroid requires rooting of the phone. Rooting a phone would delete all data on the phone and could negate the phone's warranty. Therefore, we felt it would be inappropriate to ask participants to do so. Another alternative would be to give a second phone to participants with Taintdroid and our intervention and user interface design. However, participants might not use the second phone the same way as they use their own phones during their daily lives. This could limit the ecological validity of the study. Therefore, we aimed to implement a heuristic method to discover when apps were accessing the users' location.

The challenge in implementing a heuristic method is that the Android platform is designed to protect applications from accessing data and methods of other applications. All applications run in separate sandboxes, essentially Java virtual machines, and are protected with UNIX permissions. The Android platform provides a mechanism called *Intent* for inter-application communication (Chin et al., 2011).

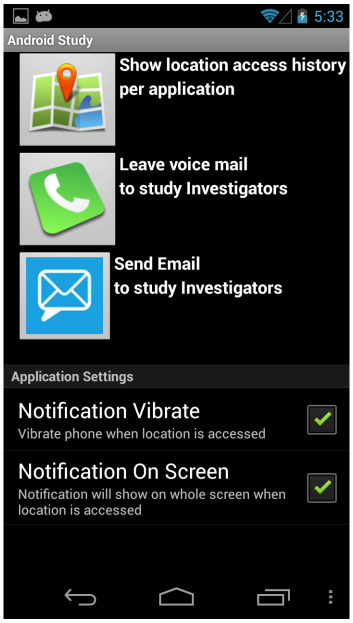
3.2.1 Heuristic Discovery of All Apps' Location Access

Because application is not allowed to access data and functions of other apps, a normal Android app cannot directly monitor whether other apps are accessing location. We find an effective side channel that the method *getLastKnownLocation* can be exploited to detect location update. This method is available in the Android Location API. The description of this method is *"Returns a Location indicating the data from the last known location fix obtained from the given provider."* After discovering this method, our heuristic for finding out if another app is accessing location is:

- If no apps are requesting updated locations, the location our app receives via *getLastKnownLocation* will not change;
- If any app is requesting location updates, *getLastKnownLocation* will change;
- If the location is updated, the most likely app requesting the location is the "foreground app" (the app the user is actively using).

Our study app has a main service to detect location changes and foreground apps which is running in the background. The main service checks and updates foreground application records every two seconds, and checks with *getLastKnownLocation* every three seconds to monitor if the location changes. We tested that these were reasonable numbers to keep the heuristic accurate. The service also uses the method *PackageManager.getPackageInfo* to check whether a given app has the following permissions *ACCESS_COARSE_LOCATION* or *ACCESS_FINE_LOCATION* enabled, to double-check that foreground app actually can access location. If location changes are detected, the service triggers notifications to users as described below. The main service will automatically start after installation or users' restarting their phones. This service will show instant notifications to users periodically about the apps' location update events as describe below.

We tested our approach for both GPS and network-based localization methods to verify that it works with all of them. In principle, it might be possible that other apps



5:33

Android Study

Show location access history per application

Leave voice mail to study Investigators

Send Email to study Investigators

Application Settings

Notification Vibrate ☑
Vibrate phone when location is accessed

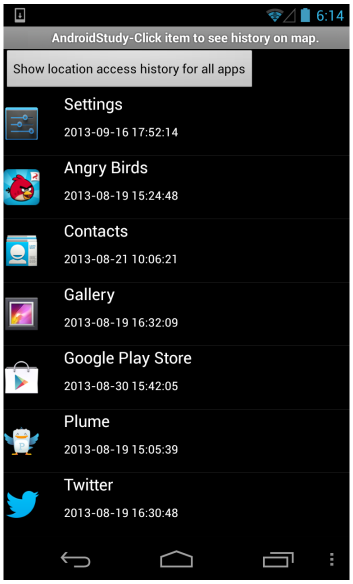
Notification On Screen ☑
Notification will show on whole screen when location is accessed

Figure 3.1: Main screen of the study app. Users can click "Show location access history per application" to see the list of apps (see Figure 3.2) that have accessed location during the study. Users also can give use feedback via "leave voice mail" or "send email". They can disable the vibration of notification in the notice bar and the pop-up notifications on the screen.

would be using *getLastKnownLocation* for getting their location fixes, but in practice this was not the case. We tested this with tens of popular apps from the Google Play Store. The tested apps included Glympse, Foursquare, Twitter, Facebook, Yelp, My Tracks, Whats Around Me, Maps, Footprints, Location Picker, Poynt and Coffee Finder downloaded from the Google Play Store. Apps could not make sure to obtain updated location on the spot by using *getLastKnownLocation*. If the location was not updated the app could not supply effective functions depending on the old location.

3.2.2 User Interface Main Features and Interventions

The main user-controllable screen (see Figure 3.1) of the app consists of only five different options. First, users have the option to have the app to *"Show location access history per application."* Pressing that option, the users will be presented with



AndroidStudy-Click item to see history on map.

Show location access history for all apps

Settings
2013-09-16 17:52:14

Angry Birds
2013-08-19 15:24:48

Contacts
2013-08-21 10:06:21

Gallery
2013-08-19 16:32:09

Google Play Store
2013-08-30 15:42:05

Plume
2013-08-19 15:05:39

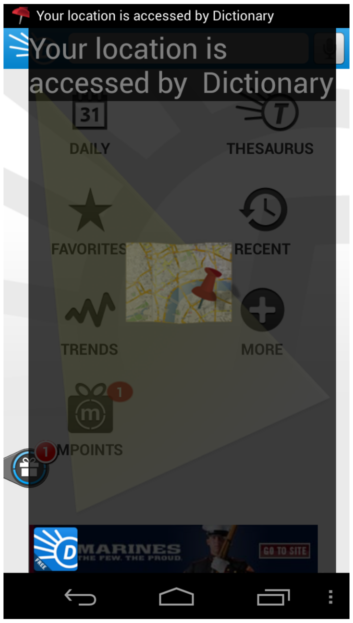
Twitter
2013-08-19 16:30:48

Figure 3.2: Users can see the history records of apps that have accessed location during the study. The list has app's name, app's icon and the latest time the app updated location. User can click a specific app to see the history of all locations this app has accessed on a map. Also, users can click the button "Show location access history for all apps" to see the history of all locations all apps in the list have accessed on a map (see Figure 3.4).

a *"List of apps that accessed location."* as shown in Figure 3.2. Two other options in the main screen include leaving voice mail or sending email to study investigators. We also provided options to disable vibration when a notification of location tracking is given, and to disable the feature showing the notifications on the screen.

The history records feature namely the *"List of apps that accessed location."* as shown in Figure 3.2 include the app's name, app's icon and the last time this app updated location. Users can click the button "Show location access history for all apps" on the top of the list to see all the locations the apps have accessed during the study on a map as shown in Figure 3.4. To see locations accessed by a specific app on the app users can click the specific app item in the list.

The interventions most often seen by participants are two location access disclo-



Your location is accessed by Dictionary

Your location is accessed by Dictionary

Figure 3.3: Example of "notifications on the screen" location disclosure we implemented with the "toast" functionality of the Android platform. The disclosure overlays briefly over the app the notification that "Your location is being accessed by [app name]." It also shows the icon of the app, and a map. Depending on the phone's settings, the app will also vibrate the phone and play a soft sound.

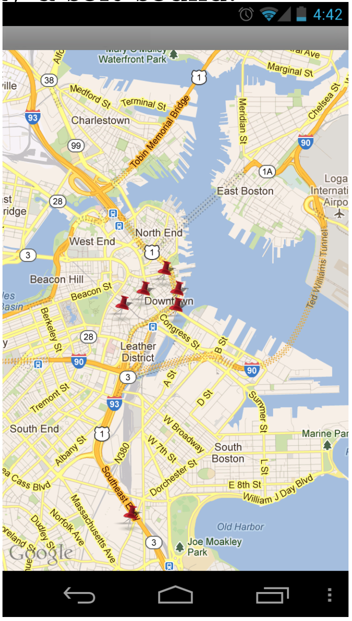
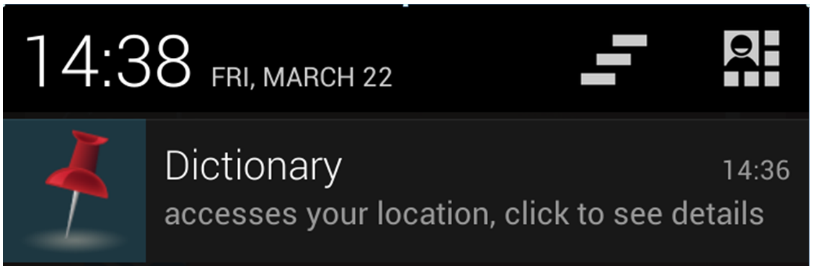


Figure 3.4: Example of "map of location accessed by a specific app." It shows the location Google Maps accessed in the Boston area. During pre-trials one tester was visiting Boston and needed to navigate by walking in the Boston downtown and another location. The pins show the areas where Google Maps accessed his location.



14:38 FRI, MARCH 22

Dictionary 14:36

accesses your location, click to see details

Figure 3.5: Example of the location access disclosure implemented to the Android notice bar. Location access disclosure appeared in the Android Notifications List, which is expanded by pulling the Notification Bar downwards.

sures: 1) a notification on the screen *"Your location is being accessed by [app name]."* as shown in Figure 3.3 and 2) a notification in the Android notice bar as shown in Figure 3.5. As triggered by the above discussed process, the two notifications were shown at the same time to participants. Figure 3.3 was implemented with Android's *toast* notification feature and it covers the whole screen of the phone using a semi-transparent picture. Depending on the phone's settings, the app also vibrated the phone and played a soft sound. There were also three other disclosure features: "map of location accessed by a specific app" as shown in Figure 3.4, "map of locations accessed by all apps" and "list of apps that accessed location."

There should be limits on how often the notification is shown to participants. Some apps were detected to update location very actively almost every several seconds the location was updated by the apps. It was obvious that notifications with such high frequency would interrupt users' regular activities when operating their phones. Based on initial lab tests, we decided to limit the notifications to every five minutes if the participant keeps using the same application. If the participant kept changing to different applications, we only used a one minute delay between the notifications.

3.2.3 Recruitment and Participants

Participants were recruited by several methods. Flyers were posted on campus and online advertisements were published in the local Craigslist and a student mailing list. Recruitment was also carried out in person at the university campus center. The recruitment was advertised that user studies were conducted to understand cell phone owners' attitudes towards mobile apps. Those who were interested in participating in the study were required to be age 18 or over, own an Android phone and answer a short online entry survey. The online entry survey collected general information including how many location based apps they used, how often they used location based apps, what the location based apps they used and demographic information. Participants were screened by the entry survey answers: they were qualified if they used location based apps in daily lives. We did not screen participants by the frequencies or number of location based apps they used. We believed that in daily life usage of location based apps were very diverse between individuals namely some users used a lot of location based apps while some used very few. We tried to make sure the participants we recruited represent the diverse usage patterns in individuals in daily life.

We made appointments with 25 persons who were qualified for our study. They were assigned randomly with a coin toss prior to the appointment to either the No Disclosure group or the Disclosure group:

- **No Disclosure group:** (n = 9) participants in this group did not receive run-time location access disclosures.
- **Disclosure group:** (n = 13) participants in this group received run-time

disclosures when apps were accessing location.

Three participants did not complete the study. During the first appointment, one person decided to quit after reading the consent form. Another person decided to quit the study after we finished the first questions, and when we asked to install our study app on this person's phone (we note that the participant had already consented to the study and signed the consent form). One participant was excluded because he formatted his phone soon after joining our study and in the exit interview told us he could not contact us afterwards due to sickness. Thus, 22 participants participated for around four weeks. The study resulted in 13 participants in the Disclosure group (denoted as P1-13) and 9 participants in the No Disclosure group (denoted as C1-C9).

In the Disclosure group, nine participants were male and four were female; ten participants were of age 18-25, three were of age 26-35. Five participants were originally from Asian countries, five participants were from a North American country, one participant was from an African country, one participant was from a European country, and one participant was from a South American country. Six participants were graduate students, five were undergraduate students, one self-identified as an administrative support person, and one was a teacher. In the No Disclosure group, eight participants were male and one was female; five were of age 18-25 and four were of age 26-35. Six participants were from Asian countries and three participants were from a North American country. Five participants were graduate students, three were undergraduate students, and one worked in the education sector.

All participants were compensated with $25 gift certificates for participating for four weeks, and were included in a raffle for two $50 gift certificates.

Our study was approved by the Institutional Review Board (IRB) of Rutgers University.

3.2.4 Experiment Design

Our study was a randomized experiment conducted during people's daily lives. The study consisted of four parts. All participants (1) went through an entry interview, (2) had the study app installed on their own phones, (3) ran the app in background for about four weeks, and (4) participated in an exit interview and debriefing.

The participants were asked to install the study app and were told that the app will record the name of the applications that request current location, and the locations where they request it. The app also records all installed applications, when the apps are installed or uninstalled, how long and when a given app is used, and when the phone is used. The application does not record any additional personally identifying information (such as usernames).

To compare the effects of run-time location access disclosures with the effects of existing disclosure methods on Android phones, we randomly divided our participants into two groups as Disclosure group and No Disclosure group.

> **Disclosure Group.** Participants in the Disclosure group would receive run-time notifications about their apps' location access on their phones. The notifications intervention features and their mechanism had been discussed above. To establish a baseline of participants' behavior before the designed interventions, the app's user interface activated only after the participant had been partici-

pating for seven days. To evaluate the usefulness of the features supplied by the study app, the app collected data on how people interacted with the user interface, e.g. what buttons on the main user-controllable screen they pressed, when they disabled any features and how long they viewed any particular screen such as *location access history for all apps on a map* (see Figure 3.4) or *"List of apps that accessed location."* as shown in Figure 3.2.

Importantly, we did not discuss with the Disclosure group participants any of the features of the app. We wanted them to discover all features by receiving the disclosure notifications, and, for example, potentially accessing the main user interface later. We believe this provided for ecological validity of our study, because apps downloaded from the Google Play Store do not usually come with instructions of all of their features.

No Disclosure Group. Participants in the No Disclosure group did not receive any notifications from the study app or have any user interface to interact with. Participants in this group only had the Android phones' default GPS location access disclosures. The Android phone will show a GPS icon flashing when apps are trying to use GPS localization. The study app collected the same data as in the Disclosure group except the data of user interface interaction operations in the background during the study. After participants in the study for one week, the participants were asked to read a recent article (Singer, 2013) from The New York Times about location-based apps tracking mobile phone users. We would like to see if the participants would pay more attention to their apps' location access and take some actions toward their apps related to location access. If they took actions due to the article what action they could take. We compared the differences in actions participants took in the two groups. We expected that the study app's run-time disclosure with explicit information about which app was accessing location would bring more transparency and enable participants to take more specific actions toward specific apps.

After one week of data collection, the participants in the two groups were contacted to see if they had any problems with the study app. Most of participants replied by email and told us that the app worked well. Two participants in the Disclosure group complained about the interruptions of the pop-up notifications on the screen.

3.3 Results

In this section, we will first describe the data collected from participants' phones by the study app. These collected data were used to understand some reasons for participants' reactions and attitudes in the study. Participants' reactions will be reported and compared below.

3.3.1 Description of Collected Dataset

The data we collected includes the apps participants installed and uninstalled during the study, apps which accessed location, disclosure notifications the Disclosure group participants received when apps were accessing their location and their usage of the features of the study app. There were 99 records of apps uninstalled and 135 records of apps installed. We analyzed more than 8000 rows of apps which accessed location records in the two groups. The Disclosure group participants received 3351 disclosure notifications during the study. They opened the study app 192 times totally. There were 26 Notification setup operations of the study app. The exit interviews we conducted took a total of 7.5 hours for the Disclosure group, and 4 hours for the No Disclosure group (due to the smaller number of participants and fewer topics to discuss).

3.3.2 Overview of Participants' Apps on Their Phones

We would like to explore the questions related to participants' apps on their phones: How many apps were installed on participants' phones? How many of these apps are location based apps? How many location based apps participants used in daily life? These questions can give an overview of the popularity of location based apps used in daily life.

The distributions of installed location based apps and all installed apps are shown in Figure 3.6 and Figure 3.7 respectively for the participants in the Disclosure group and in the No Disclosure group. It is very obvious that the percentage of location based apps is equal or less than 1/5 of the total installed apps. The maximum number of location based apps is about 75 for the participant P12 and the minimum number was about 20 for the participant P3. By contrast, the percentage of used location based apps in totally used apps was about 1/2 which is much larger than the percentage of installed location based apps in totally installed apps. The distributions of used location based apps were shown in Figure 3.8 and Figure 3.8 separately for the participants in the Disclosure group and in the No Disclosure group.

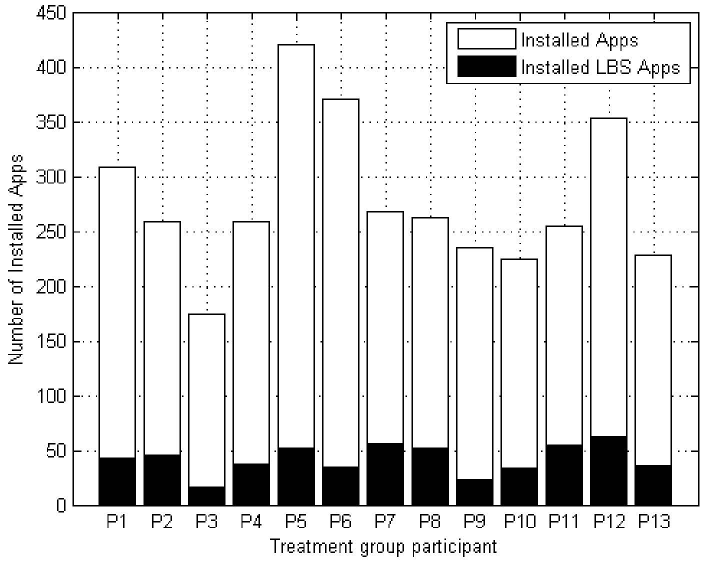


Figure 3.6: Number of installed location based apps and all apps on participants' phones in the Disclosure group.

We noted that the number of installed apps was more than 300 for some participants and the minimum was still 150. The reason might be that most of the basic functionalities of a smartphone have been implemented as an "app" on the Android platform. Further, Google, different vendors and telecommunications companies provide their own sets of default apps for the phones. Depending where the phone was purchased, the number of these apps can be several hundred.

A follow-up question about the high percentage of used location based apps in the totally used apps was that why location based apps were so popular in daily life used apps? Were participants aware of these apps could access their location? We would explore this question below.

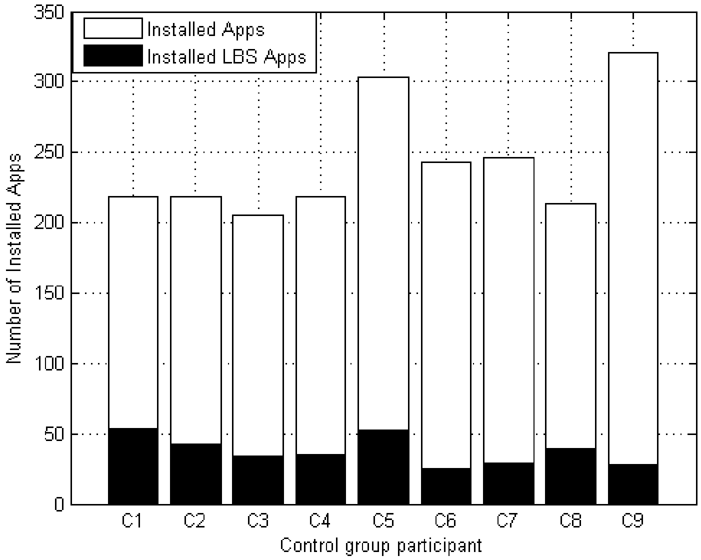


Figure 3.7: Number of installed location based apps and all apps on participants' phones in the No Disclosure group.

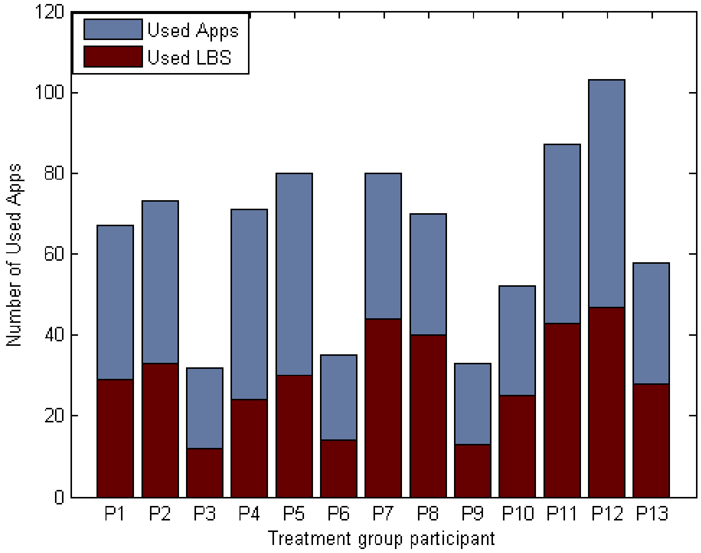


Figure 3.8: Number of used location based apps and all used apps on participants' phones in the Disclosure group.

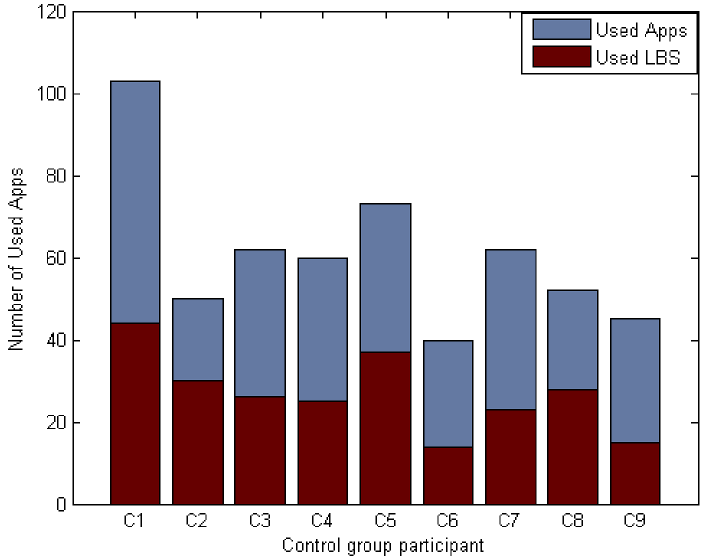


Figure 3.9: Number of used location based apps and all used apps on participants' phones in the No Disclosure group.

ID	C1	C2	C3	C4	C5	C6	C7	C8	C9
Total	40	13	23	22	32	10	0	16	11
Not Exp	9	5	5	9	8	3	0	9	3

Table 3.1: No Disclosure Group: Number of apps, which accessed location during the study, and number of apps participants did not expect to access their location.

3.3.3 Apps Unexpected to Access Location

At the end of the exit interview, the participants were shown the list of apps which had accessed their location during the study. The corresponding question was "Which of the following apps did you not realize could access location until the study app notified you that they were accessing your location?" They were asked to mark the apps, which they did not expect would access location.

In the No Disclosure group, all participants except one (C7) marked several apps as shown in Table 3.1. Participant C7 did not have records of any apps accessed location during the study.

ID	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
Total	28	19	2	21	20	8	39	29	5	19	41	37	21
Not Exp	7	4	0	17	8	5	3	1	4	3	3	14	14

Table 3.2: Disclosure Group: Number of apps, which accessed location during the study, and number of apps participants did not expect to access their location.

Participants were then asked to describe their feelings and attitudes about how the apps accessed their location. All participants (except C7) could not understand why several apps accessed their locations. They felt that these apps did not have any location related functions, therefore, these apps had no reasons to access location. For example, participant C8 shared, *"Apps like WhatsApp, ESPN, Cricinfo have no business knowing where I am. I am not using location based services through those apps."*

For the Disclosure group, during the exit interview, most participants themselves shared that they did not expect several apps they used to access their location. They found an unexpected large number of apps that accessed their location. Some felt that their location privacy was taken away somehow. Among these participants, seven (P1, P4, P5, P6, P7, P9, P13) expressed surprise and one (P12) told us about being confused about the apps' behavior. Most participants expressed the feeling that these apps' functions did not depend on location. Most participants shared the sentiment of P12 who commented *"Some unexpected apps are also using my location. They are totally unrelated. It is good thing that I know this."*

In the end of the interview, participants were shown a list of apps that accessed location. They were asked to mark apps they did not expect prior to our run-time disclosures to have accessed their location. We show the number of apps for each participant in Table 3.2. Only participant P3 did not mark any apps, because he only used Google Maps and Browser apps.

It was obvious that the default GPS location access disclosures on Android phones was not effective enough to inform users of their apps' location request. Most participants had some apps unexpectedly to access their locations. The following results would show that the study app's run-time location access disclosures were effective and participants in the Disclosure group had taken actions to manage their apps during the study, while no participants in the No Disclosure group had taken actions at all.

The contrast between the two groups was that the participants in the Disclosure group expressed stronger feelings about the unexpected apps' location access than in the No Disclosure group. We noted that we did not compare the number of apps unexpected to access location in the two groups statistically due to the small sample size. The consistence between the two groups was that most participants judged the acceptability of apps' location access depending on the apps' functions. It might imply that participants cared more about the feasibility of apps' location usage, but they cared less about apps' location access to perform some functions.

3.3.4 Comparison of Effectiveness of Run-time Disclosures and Other Disclosures

The nine participants in the No Disclosure group did not receive notifications of apps' tracking their location. Instead, after a week of participating, they were introduced to an article in The New York Times (Singer, 2013) about apps tracking people's locations.

We were interested in whether reading an article related to location privacy would increase participants' location privacy awareness. However, the self-reports of the participants in the exit interview showed that they did not have any behavior changes during the study due to the article. Only one participant (C8) said *"[being] more aware of location-based apps downloaded."* Three participants (C1, C7, C9) did not read the article.

The Android's default location access disclosure method depicted in Figure 2.1 was not effective to disclose apps' location request. In the No Disclosure group, five participants (C1, C3, C4, C5, C6) knew that the GPS icon would show up when some apps were using GPS to locate them. However, none of the participants had taken any actions due to the flashing GPS icon. Participants could not manage their apps' location usage because they were not sure which apps could access their location or how often these apps accessed their location. For example, participant C5 said *"If I sense that the data they are providing to me is location based, then I can guess they are using my location data. Mostly, it's the GPS icon."* Similarly, participant C6 shared, *"On general sense you don't [know when your location is accessed], unless I look at the screen and GPS icon show up, I know something is using it."*

The study app's run-time disclosures were effective to notify participants of their apps' location access and participants had taken several actions to manage their apps. In the following, we will describe the run-time disclosure notifications participants received during the study, actions taken by participants including uninstalling apps, stopping using apps, reducing frequencies of using apps, and searching through setup of the apps which were unexpected to access location.

As discussed before, the 13 participants in the Disclosure group received disclosure notifications when apps were accessing their location. They received run-time disclosures via several features including notifications on the screen (Figure 3.3) and notifications in notice bar (Figure 3.5). We limited the frequency of notifications to five minutes for a single app, one minute if the participants started using another app. Some of the features such as “vibration,” or “notifications on the screen” could be disabled (see Figure 3.3). The notifications on the notice bar and its sound could not be disabled. During the study, participants experienced relatively large amounts of run-time notifications. The participants received in total 3351 run-time notifications during the three weeks. The number of notifications each participant received in the study is shown in Figure 3.10. The maximum was 851 times, and the minimum was none (P3).

Uninstalled Location-Enabled Apps Unexpected to Access Location. The study app helped some participants realize that some apps access location unexpectedly. They took some actions to manage apps whose function was not based on location. Two participants (P4, P11) uninstalled apps specifically because of the disclosures provided by our app. Participant P11 uninstalled an app called “MiHome,” which is a third-party developed launcher app. Participant P11 learned via our implemented notifications that MiHome accessed location frequently. He thought a launcher app did not need location for its function. Participant P4 uninstalled three game apps after learning that these apps accessed her location. She felt that she really did not need these three apps and she did not like these apps accessing her location. Uninstalling an app was one of the extreme actions participants took due

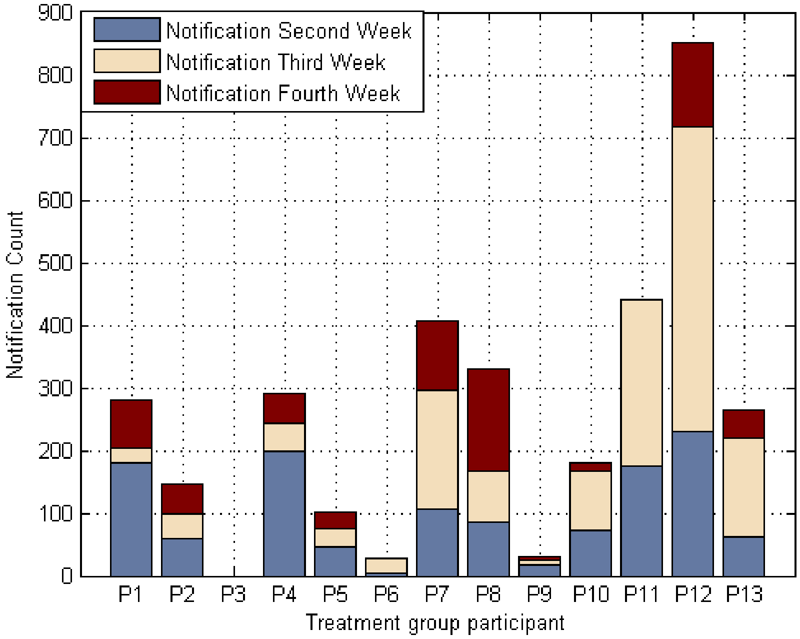


Figure 3.10: How many times each participant in the Disclosure group received a notification that their location is being accessed divided to second, third, and fourth week of participation. (Recall, we would start the notifications after first week of participation, and the Notification Bar based notification could not be disabled.)

to the notifications.

Other Actions Taken to Manage Apps Unexpected to Access Location. Participants tended to take actions to apps whose function were not supposed to depend on location. Our participants took several kinds of actions to control their apps' unnecessary location access because of our location access disclosures. Two participants (P4, P5) stopped using some game apps after seeing the notifications that these apps were accessing their location unexpectedly. Participant P4 told us that she played lots of games before our study. Participant P5 started to avoid games that accessed his location, *"If a game access my location I will not play the game anymore."* One participant (P6) started to reduce how often he would use apps he did not expect to access his location and found replacements for them. Participant P6 was not aware that TuneIn Radio, Firefox and Dictionary apps would access his location. Now he used the default music player instead of TuneIn Radio, DuckDuckGo instead of the Dictionary. He tried to use the desktop browser as much as possible instead of using the browser on his smartphone. P6 said after he realized that some apps accessed his location unnecessarily he would pay attention to these apps and use them more carefully. He thought these apps did not have reasons to access location. Participant P2 took actions most users might prefer; he searched through a game app's settings and disabled location access. He told us that the app still worked well after location was disabled. However, participants assumed most apps did not give the option to disable location.

We summarize the differences in reactions between the Disclosure group and the No Disclosure group in Table 3.3. The No Disclosure group participants did not

No Disclosure Group	Disclosure Group
(1) no actions due to GPS icon; (2) only one user might be more careful when downloading apps after reading The New York Times article (Singer, 2013);	(1) uninstall apps; (2) replace apps; (3) stop using some apps; (4) search through setup to disable the app's location

Table 3.3: Different Major Findings in Two Groups

take any actions due to GPS icon flashing or reading the location privacy related article. The Disclosure group participants had taken various actions to limit apps accessing their location. This suggests that the run-time location access disclosures were effective. By comparison, existing location access disclosures on Android were not adequate.

3.3.5 Comparison of Transparency Experience between two Groups

Participants in the Disclosure group appreciated the transparency brought by the study app's run-time disclosures. They expressed strong feelings such as using words "surprised" or "weird" to express their impression after receiving our run-time disclosures about their own apps' location access. They also took several actions to limit their apps' location access. We would like to explore what kind of transparency these participants had experienced. By comparison, we would analyze what information for transparency was missed for the participants in the No Disclosure group.

Awareness vs Unawareness of Frequency of Location Accesses. Run-time disclosure helped participants to become aware of how often an app accessed their location. Some participants even made decisions about apps depending on how often the apps were accessing their location. As discussed before, participant P11 uninstalled one app named MiHome. We noticed that P11 did not uninstall MiHome until he received at least 249 disclosure notifications of this app. Participants were interested in the frequency apps accessed location. Participant P12 said *"I would like to know the times each app accessed location. They tell me how many times I use the app and if I know some apps access my location too often, I would probably stop using them. One time would be fine."* Participant P5 said *"It [the study app] tells you really how many, and with what frequency the apps are accessing your location you understand that it's going to take something, but you don't realize how often and when."*

In the Disclosure group, we did not show the frequency of location accesses explicitly to the participants. They learned about the frequency via notifications they observed. We note that due to our limits towards not distracting the participants too much, they received these notifications less often than their locations were actually accessed. In contrast, the No Disclosure groups participants did not have a sense of how often their locations were accessed since they did not receive the notifications.

Explicit Message and Context Information Makes a Difference: Which App, Where, When, What Function. Our run-time disclosures enabled participants to understand how their apps used their location data with context. The disclosures showed participants clearly the name of the app which was accessing their location. The disclosures also included other contextual information: at what places, at what time and which function participants expected the app to perform. The context helped participants identify the unnecessary location accesses by some apps. Participants discovered that some apps accessed their location even when they did not use the location related functions. Participant P7 said *"Sometimes it was really surprising that all of the apps are using my location when my intention was not to use the location."*

The run-time disclosures educated participants to learn the patterns that an app would access their location. Participant P7 said that *"Your app used to notify me and each time it did so I knew like which of the app was accessing location at what time. Sometimes I was like surprised, oh this app used my location sort of that way."* By comparison, participants in the No Disclosure group had no way to know how their apps made use of their location data. They only saw a list of apps with ability to access location in the exit interview.

3.3.6 Common Findings: Tradeoffs with Privacy and Utility in the Two Groups

In both the No Disclosure and Disclosure groups, participants were clearly considering privacy vs. utility tradeoffs. They usually chose to take advantage of the apps which had at least one function they considered useful even though these apps did not need location for their main functions. Participant P2 in the Disclosure group shared, *"Yeah, because there are other features of the app I would want to use, right, unless there is no use for the app I would like to keep it even if it uses location sources."* Participant P4 said *"So when people become so dependent on technology doing things for them automatically they give up some of their freedom because now you have companies who can do that and use that technology."*

Participants in the No Disclosure group also had similar trade-off decisions. Participant C5 said *"Contacts and Phone. I was not aware that they were collecting* *my data, but I have no choice, I have to use them, and I accept that they use my data because they are part of the system."* He also shared *"I trust Google and trust Samsung that they will not do bad things. Yes. Actually, I agreed them to use as long as they use my location for my own use."* Participants would keep using apps they found beneficial even though these apps accessed location.

We observed that some participants would not give up their privacy for convenience. Participant C8 said, *"It is inconvenient but important to me that apps do not track where I am. I do it as far as possible. I have had other location based apps before but I deleted them now."*

3.3.7 Attitudes and Suggestions to Our Run-Time Location Access Disclosures

As discussed above, we implemented several kinds of location access disclosures. We were interested in participants attitudes and perceptions about these features.

We analyzed participants' usage of the study app's features from the data we collected from their phones. The breakdown per participant is shown in Figure 3.11. Not surprisingly, the feature "the list of apps that have accessed location" is the most used one with total 107 views. This is also because it can be directly linked from the notifications in notice bar (as shown in Figure 3.5). The other two features "map of location accessed by all apps" and "map of location accessed by a specific app" must be accessed from the list of apps. Most participants turned off "notifications on the screen" feature after several hours or the third day after the time to start receiving disclosure notifications.

The most popular feature was the notification in the notice bar. Eight participants

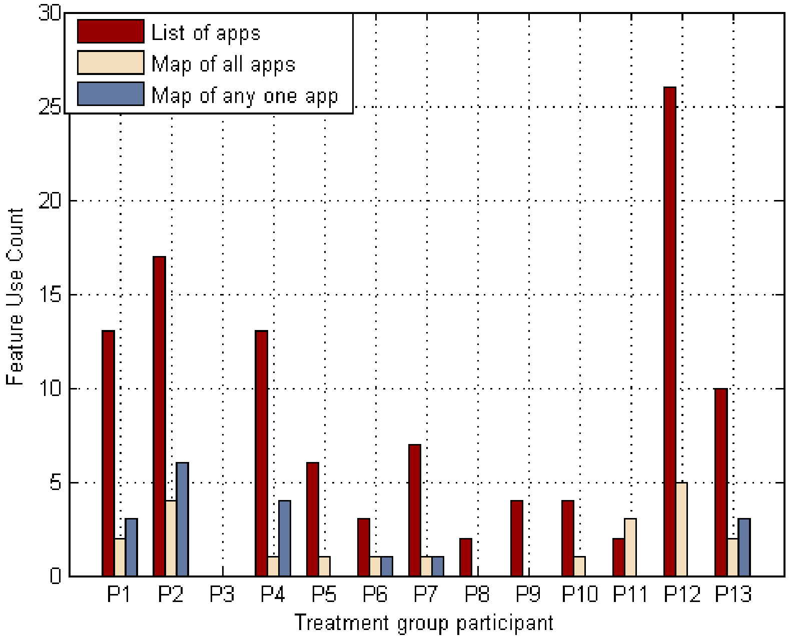


Figure 3.11: How many times each participant in the Disclosure group used some of the major features of the study app: the listing of all apps that accessed the participant's location, the map of any one app listed to be accessing locations, and the map of all location accesses by all apps.

(P4, P5, P6, P7, P9, P11, P12, P13) preferred this feature. Participant P7 said *"It just notified me whenever any of the apps used to access the location. It provided me instant notification of that."*

Two participants (P5, P11) also preferred the notifications on the screen. Participant P5 said *"I liked that it actually physically made a noise and vibrated every single time that it was my location was accessed...I liked how the popup was slightly translucent."*

Four participants (P1, P2, P4, P8) preferred the list of apps so they might just want to get the general idea of what apps accessed their location. Participant P2 said *"I think it [list of apps] was good because there are lot of apps that I didn't know used my location."* Three participants (P6, P10, P11) liked the map of apps that had accessed their location.

We asked participants if they would have liked to continue receiving run-time disclosure notifications. For the notifications in the notice bar, nine participants (P1, P2, P3, P5, P6, P7, P8, P11, P13) would have liked to continue receiving the run-time disclosures. Participants appreciated the awareness brought by the disclosures. They treated the disclosures as confirmations and reminders of their apps' using their location. Participant P11 said *"Actually for me it made me more aware of what was going on. I appreciated that."* Several participants emphasized that they would like to receive disclosure notifications occasionally. They would like to have the option to disable the notifications. One participant (P10) did not like to receive notifications at all. He shared *"Use the phone in rush, something else to worry about, so annoying. Plus, it is better you do not notify every time."* Three participants (P4, P9, P12) admitted that the disclosures were useful, but they did not think it was necessary. Participant P12 said *"It is good to be a feature, but should not be necessary. should have an option so that I can turn it on and off. Not notify every time, annoying."* We noticed that participant P12 received 851 notifications in three weeks (see Figure 3.10). Participant P4 seemed resigned, she shared *"At this point it doesn't really matter .... In this technologically advanced world, whether you like it or not you need a phone and they will somehow track you."* Most participants complained there were too many notifications. They thought the app should not show notifications every time apps accessed location. Most participants did not like to receive the toast notifications on the screen. They found it annoying because it interrupted their work. Some participants suggested that it would be better that the toast notification covered only small area of the screen instead of the whole screen.

3.4 Summary

Most participants would have liked to continue receiving run-time disclosure notifications in the Android's notice bar. They liked the transparency brought by the disclosures. This result is consistent with the previous work (Balebako, Shay, & Cranor, 2013) which showed that roughly 70% of users wanted to know location collection by apps. Participants clearly were concerned about location privacy. Our effective run-time location access disclosures actively alerted the Disclosure group participants when apps were using their location data. Some participants described the study app as an "eye opener." In contrast, participants in the No Disclosure group were generally not aware of what was happening on their own phones.

CHAPTER 4

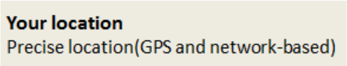
GENERAL AREA OR APPROXIMATE LOCATION? HOW PEOPLE UNDERSTAND LOCATION PERMISSIONS

4.1 Overview of Chapter

According to Pew Research, 56% American adults use smartphones (SMITH, 2013. Pew Internet, Tech. Rep.) and 74% of these users have used location-based services (Zickuhr, 2013). These location-based services, implemented as apps, can have unprecedented third-party access to the locations of their users. In our previous field study, some participants would like to differentiate between the fine location and coarse location access disclosures. They were not too concerned with the coarse location access by apps.

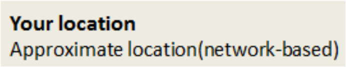
There have been several studies related to the privacy of smartphone users. A broad survey by Balebako et al. indicated that smartphone users were concerned about how their apps accessed their location (Balebako, Shay, & Cranor, 2013). In a lab study by Felt et al. at least one participant decided not to install an app due to “exact location” permission (Felt, Ha, et al., 2012). In a field study by Fu et al. some participants uninstalled apps after they became aware that some apps were accessing their location (Fu et al., 2014).

Android users do not clearly understand the apps’ installation-time permissions.



Your location
Precise location(GPS and network-based)

Figure 4.1: Shows the "precise" location permission, which enables apps to localize the phone with both GPS and network-based (WiFi and cell-tower) methods.



Your location
Approximate location(network-based)

Figure 4.2: Shows the "approximate" location permission. This permission enables only network-based localization, and the recent API updates also include limited random obfuscation for the location.

A study by Felt et al. (Felt, Ha, et al., 2012) showed that only 3% of their participants could correctly understand the permissions. Kelley et al. (Kelley et al., 2012) study also reported that most participants were confused about the "coarse (network-based) location" permission.

Different location granularities can affect users' willingness to share their location. For example, Leon et al. study showed that only 4% of participants (of 2912) were willing to share their exact current location with advertising companies. However, about one fourth were willing to share zip code and town or city information (Leon et al., 2013).

In this chapter, we investigate how Android users understand the location related permissions on the Android platform. The platform has two different location permission requests, as depicted in Figure 4.1 and Figure 4.2. These requests are shown at the same time for all other permissions requests the app might be enabled for. The "approximate" location is network-based using WiFi or cellular networks for localization. The "precise" location enables the use of GPS, in addition to network-based localization. Earlier versions of the Android platform referred to these permissions as "coarse-grained" and "fine-grained" location.

To investigate how people understand the location permissions on the Android platform, we carried out an online survey (N=106). Our results suggest that most participants could differentiate the two location permissions via the literal description as "precise" or "approximate." However, they interpreted the precise location as "exact location" and the approximate location as a "general area." Not surprisingly, a majority of participants could not distinguish the two permissions via technical descriptions, such as "GPS" or "network-based."

Our study contributes to the understanding of people's mental models related to smartphone app location privacy. Interestingly, about two thirds of participants thought that the approximate location accuracy was equal to or more than 1 miles – 2 miles (or 1.6 km – 3.2 km). The participants expected the approximate location to protect their location privacy because it was not close to the exact location and that third parties could not find them directly or obtain their personal details. After being shown ground truth of the localization accuracy, the number of participants who would not trust that approximate location could protect their location privacy almost doubled. They now considered "approximate" location to be almost the same as the exact location.

4.2 Method

In this section, we summarize our method, including our participants and online survey design.

	Number	Percentage
Total Participants	106	
Age		
18-25 years old	25	23.6
26-35 years old	44	41.5
36-45 years old	28	26.4
46-65 years old	9	8.5
Latest Degree		
Some college - no degree	35	33.0
Bachelors / 4 year degree	30	28.3
Associates / 2 year degree	14	13.2
High school graduate	13	12.3
Graduate degree	12	11.3
Some high school	2	1.9
Careers		
Service	16	15.1
Engineering or IT Professional	12	11.3
Business, Management, or Financial	11	10.4
Unemployed	11	10.4
College student	9	8.5
Administrative Support	8	7.5
Art, Writing, or Journalism	7	6.6
Skilled Labor	7	6.6
Education or Science	6	5.7
Graduate student	1	0.9
Legal	1	0.9
Retired	1	0.9
Other	16	15.1

Table 4.1: Demographic of Participants

4.2.1 Participants

We recruited 106 participants. According to their responses, 54.7% of them are female and 45.3% are male. The participants age ranged from 19 to 61 and the mean age was 33 with a standard deviation 8.8. Table 4.1 shows the additional demographic information of the participants.

All the participants were compensated $2 upon completion of the survey which took 15-20 minutes to complete.

Several methods were adopted to screen qualified participants. Participants were required to be at least 18 years old, have an Android phone, live in the United States, have been granted a Masters by MTurk, have a number of HITs approved greater than or equal to 100, and have a HIT Approval Rate greater than or equal to 95%. Unique Turk (Unkown, 2014) was also used in the MTurk HIT's html file to exclude duplicated worker IDs.

4.2.2 Online Survey Design

The study was approved by the Rutgers University IRB. It was conducted in November 2013. The survey was set "forward only" mode so that participants could only advance and not go back to previous screens. The survey had 26 questions, four of which were entry questions to screen participants.

After screening questions, the first four questions were open-ended items related to the location permissions on the Android smartphone platform. Participants were asked to describe how they understood the two location permissions, and the differences and reasons for them. The screenshot of the two location permissions (see Figure 4.1 and Figure 4.2) were shown to participants before the corresponding questions. These location permissions screenshots were taken using Android 4.0 version. Then, they were asked to answer a 7-point Likert scale question about their attitudes toward location privacy related to "approximate" location. The participants were also asked to give explanations for their choices.

We also probed the participants understanding regarding the meaning of "GPS

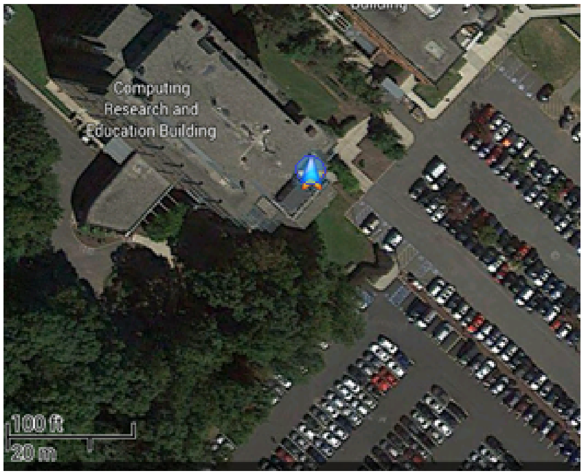


Figure 4.3: Screenshots of GPS localization on an Android smartphone using Google Maps. The yellow star depicts the Android phone's exact location, and the blue circle is the location accuracy area. The map's scale is 100ft / 20m.

location" and "network-based location." They were given multiple options and were asked to choose what they thought were the accuracy of the particular localization method. Next, participants were shown screenshots of maps for GPS, WiFi and cell-tower based localizations respectively as shown in Figure 4.3, Figure 4.4 and Figure 4.5). The participants were asked to select what method of localization the map would be the result of and they could only choose one from the three options including "GPS", "network-based" and "I do not know."

The participants were also given correct answers to the above questions on location accuracy as follows: Figure 4.3: The correct answer is "GPS location". Its accuracy is about 9.8 feet / 3 meters to 32.8 feet / 10 meters. Figure 4.4: The correct answer is "network-based location". Its accuracy is about 164 feet / 50 meters (Wi-Fi location) to about 3000 feet / 914 meters (cell tower location). Figure 4.5: The correct answer is "network-based location". Its accuracy is about 164 feet / 50 meters (Wi-Fi location)

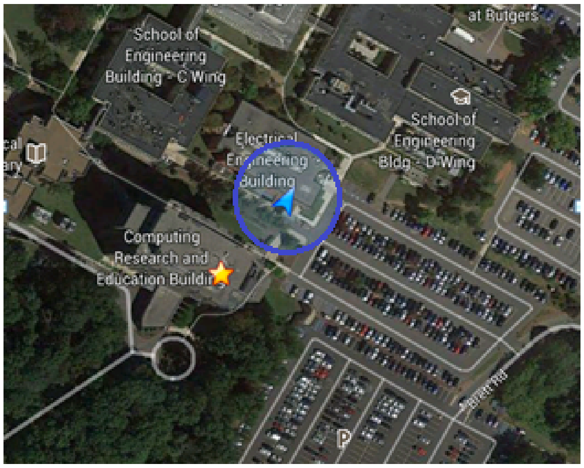

at Rutgers
School of Engineering Building - C Wing
School of Engineering Bldg - D Wing
Electrical Engineering Building
Computing Research and Education Buildi
P

Figure 4.4: Screenshots of WiFi localization on an Android smartphone using Google Maps. The yellow star depicts the Android phone's exact location, and the blue circle is the location accuracy area. The map's scale is 200ft / 50m.

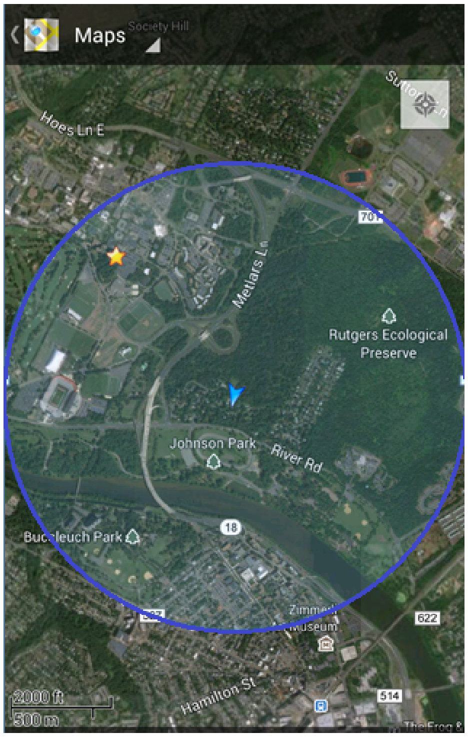


Figure 4.5: Screenshot of cellular network-based localization on an Android smartphone using Google Maps. The map's scale is 2000ft / 500m.

to about 3000 feet / 914 meters (cell tower location). After this, the identical 7-point Likert scale question mentioned above about their attitudes toward location privacy was shown again to participants.

Finally, at the end of the survey, there were six 7-point Likert scale questions relating generally to privacy and five questions relating to demographics.

4.3 Results

In this section, we will detail the results of the online survey including the common understanding of “precise” location, varied understanding of “approximate location,” participants’ privacy model of the “approximate location” and the relationship analysis between participants’ attitudes toward location privacy and their demographic information.

4.3.1 Understandings of Precise Location and Approximate Location

Most respondents shared common understanding of what “precise” location means. They supposed it was the exact location and very precise. For the approximate location, respondents’ answers varied. About one fourth participants supposed the approximate location was a general area (26.4%). More than one fourth of participants knew the approximate location was updated by a cellular tower or network connection (28.3%). Some participants supposed the approximate location was updated by both GPS and network (16.0%). We note that we did not have any kinds of limits or instructions for participants on how to formulate their responses. As a result, some respondents referred to specific technologies while some explained using a range and distance related concepts.

Accuracy	Network-based Percentage	GPS Percentage
9.8-32 ft/3-10 m	7.55	*66.04*
164-328 ft/50-100 m	*13.21*	26.42
1640-3000 ft/500-914 m	*15.09*	12.26
1 mi-2 mi/1.6 km-3.2 km	26.42	5.66
5 mi-10 mi/8.0 km-16.1 km	30.19	0.94
More than 10 mi/16.1 km	7.55	0
I do not know	9.43	0.94
Others	0	0

Table 4.2: Breakdown of participants' understandings of the accuracy of network-based location and GPS location. The percentage of results is highlighted by *italic* which fell in the given answers of accuracy of GPS location and network-based location.

The quantitative results were consistent with the qualitative findings above. Table 4.2 shows that most respondents supposed that GPS location was very accurate. More than 90% respondents thought the GPS location accuracy was equal to or less than 164 – 328 ft / 50 – 100 m. We note that two thirds of respondents (66.04%) expected the accuracy to be 9.8 – 32 ft / 3 – 10 m. For the network-based location accuracy, there was not a significant common understanding in responses of accuracy. The largest percentage was in the accuracy of 5 mi – 10 mi/ 8.0 km – 16.1 km at 30.19%. We note that a large amount of respondents supposed the accuracy of the network-based location was very low: 64.2% respondents supposed the accuracy was equal to or more than 1 mi – 2 mi / 1.6 km – 3.2 km. Interestingly, 20.76% of respondents expected the network-based location accuracy to be equal or less than 164 – 328 ft / 50 – 100 m.

Most respondents chose the correct answers about the accuracy of GPS location and network-based location when shown the figures based on Google Maps. Table 4.3 shows the results: 90.6% selected the correct answers for cellular location and 83.0%

Responses (Percentage)	GPS Screenshots	WiFi Screenshots	Cellular Screenshots
GPS	*83.0*	26.4	5.7
Network-based	14.2	*70.8*	*90.6*
I do not know	2.8	2.8	3.8

Table 4.3: Breakdown of the responses in the location accuracy on screenshot of Maps. The correct answers are marked using the *italic*.

for GPS location. The screenshot of WiFi location (see Figure 4.4) confused some participants: 26.4% of them made the wrong selection and chose GPS location.

We also asked the participants to compare the “Approximate location (network-based)” and “Precise location (GPS and network-based)” permissions. Most of the respondents assumed that the approximate location was a general area and the precise location was the exact location. For example, respondents self-reported the approximate location as “general idea of where you are,” “regional location (big area),” “ the area you are in” and precise location as “give my location within a few feet,” “exactly where you are,” “ the exact location down to your street address.”

4.3.2 Location Privacy Model of the Approximate Location

As mentioned above, participants were asked to express their attitudes towards location privacy of the “approximate” location on a 7-point Likert scale. A majority of respondents stated that the approximate location helped to protect their location privacy as shown in Figure 4.6 and Table 4.4. When asked about this prior to showing the ground truth, more than three fourths (75.74%) of respondents stated that the approximate location could protect location privacy. After showing the ground truth, there were still more than half (57.55%) of the respondents who believed that the approximate location could protect location privacy as Table 4.4 shows. A total

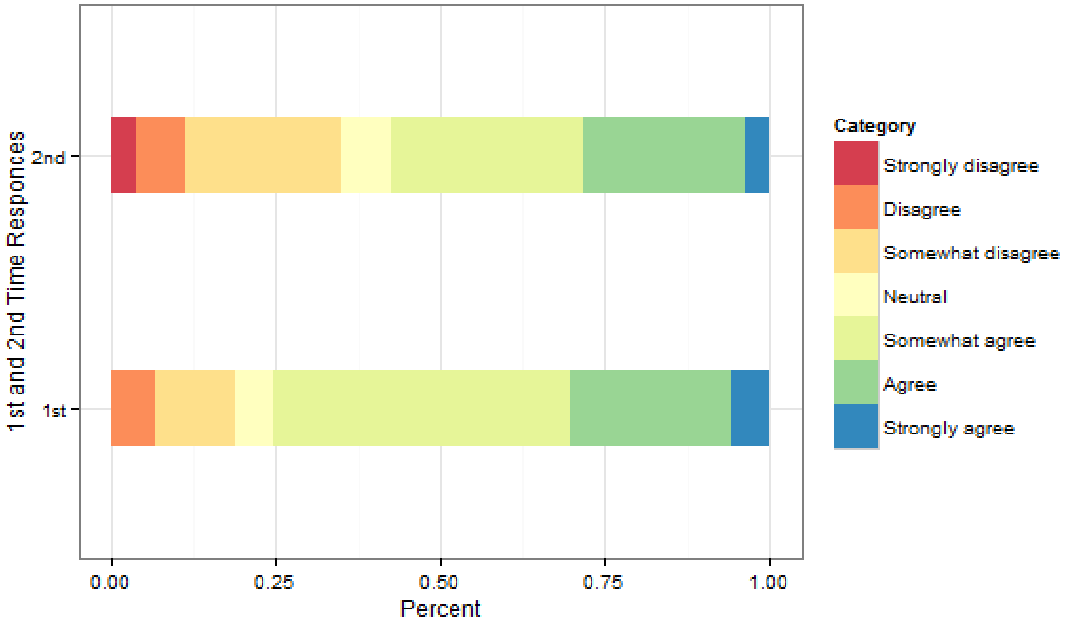


Figure 4.6: Breakdown of "approximate location helps to protect location privacy" responses prior to showing the ground truth (1st) and after showing the ground truth (2nd). The participants' responses were limited to a 7-point Likert scale.

72.64% of responses (see Table 4.5) shared the same popular reason that the general area was better for location privacy compared to exact location.

Some respondents gave further explanations for their responses, such as "in a broad area it is hard to find a person," "from the data people would not still know which stores you visited," and "still need further work to figure out personal details." For example, P130 shared *"Because it isn't exact. It would take more research and other allowances to figure out more personal details."* We note that very few respondents shared detailed explanations so we did not quantitatively show the percentage of the further explanations. Respondents expected that the approximate location existed to protect their location privacy. Some respondents (15%) explicitly mentioned privacy when asked why there were two kinds of location permissions.

Categories	First Time Percentage	Second Time Percentage
Disagree	18.87	34.91
Neutral	5.66	7.55
Agree	75.47	57.55

Table 4.4: The above 7-point Likert scale was collapsed here into a 3-point scale: agree, disagree or neutral. Similarly, "first time percentage" indicate answers prior to the ground truth and "second time percentage" after seeing the ground truth.

Categories	Percentage
Not actual address/not exact location	72.64
Better than GPS	2.83
Network provider will not reveal the location to others	0.94

Table 4.5: Reasons respondents explained why approximate location could protect location privacy.

Figure 4.6 shows that a large percentage of participants selected "somewhat agree" for the statement "approximate location helps to protect location privacy." These respondents supposed the approximate location did a better job than the precise location for protecting privacy but the approximate location still exposed the general area. P49 said *"I sort of agree with this because it only has a general idea of where you are located but not specifically where."*

How the participants understood the accuracy of the "approximate" location affected their location privacy concern. A total 16.98% of respondents (see Table 4.6) shared that if the approximate location's accuracy was too close to an exact location it was not good for location privacy. The common reasons resembled what participant P17 said *"The Approximate location was very accurate and close enough that there does not leave much room for guessing where the phone was located."*

After the respondents' saw the ground truth in the survey, the percentage of respondents who thought that the approximate location could not protect location

Categories	Percentage
Close to actual location is not good	16.98
Still know general area	13.21
Still find me	3.77
Trace movement	1.89
Repeated proximity could extrapolate exact building/hallway	0.94

Table 4.6: Reasons respondents explained why approximate location could *not* protect location privacy.

privacy doubled from 18.87% to 34.91% as shown in Table 4.4. The proportion increase is statistically significant (Upper Tail Test of Population Proportion, $p < .001$). The participants shared that they changed their minds because they saw that approximate location was too close to the exact location. Respondents did not expect the approximate location could be as accurate as the given answer in the beginning. Table 4.2 shows that only 28.30% of responses fell within the given answers relating to the network-based location's accuracy and 79.25% of responses were equal to or greater than 1 mi – 2 mi / 1.6km – 3.2 km which was more approximate than the given answers in a distance range.

The accuracy of the approximate location was an important factor respondents used to decide if the approximate location could help to protect location privacy. Kendall's rank correlation coefficient between approximate location accuracy definition and perception of the approximate location privacy protection ability was between small and medium ($\tau = .17$). There was a significant relationship between the two variables ($p = 0.03$). This suggested that participants were likely to think approximate location protects privacy if they assumed the localization accuracy was low. These quantitative results were consistent with the qualitative analysis above.

4.3.3 Demographics Effects on Attitudes toward Location Privacy

Previous studies (Patil, Le Gall, Lee, & Kapadia, 2012; Klasnja, Consolvo, Choudhury, Beckwith, & Hightower, 2009) suggested that women have more privacy concern related to location exposures. We have similar findings in our study that more female participants explicitly mentioned "[not] find me [is good]." For example, one participant (P128) said *"Someone would not be able to use the approximate location to find exactly where I am at."* However, our results are different from previous studies in that there were no significant differences between female and male participants in the location privacy protection ability related to approximate location. The responses of the location protection expectation of approximate location before and after seeing the ground truth are not significantly different between female and male participants (Wilcoxon Rank Sum Test, $p = 0.12$ prior seeing the ground truth, $p = 0.45$ after seeing ground truth). Although female participants were more concerned with physical security, both female and male participants cared more about the "exact location" and not the "general area." For example, a male respondent P121 shared *"Given just an approximate location helps to identify your phone's proximity to a certain area, which maintains privacy by not specifically identifying its exact location."* Respondents took the personal activities in to consideration respecting to location privacy.

As shown in Figure 4.7 the distributions of responses of female and male respondents in the first and second time were very similar. Not only were the distributions similar, the number of responses in both female and male respondents were increasing

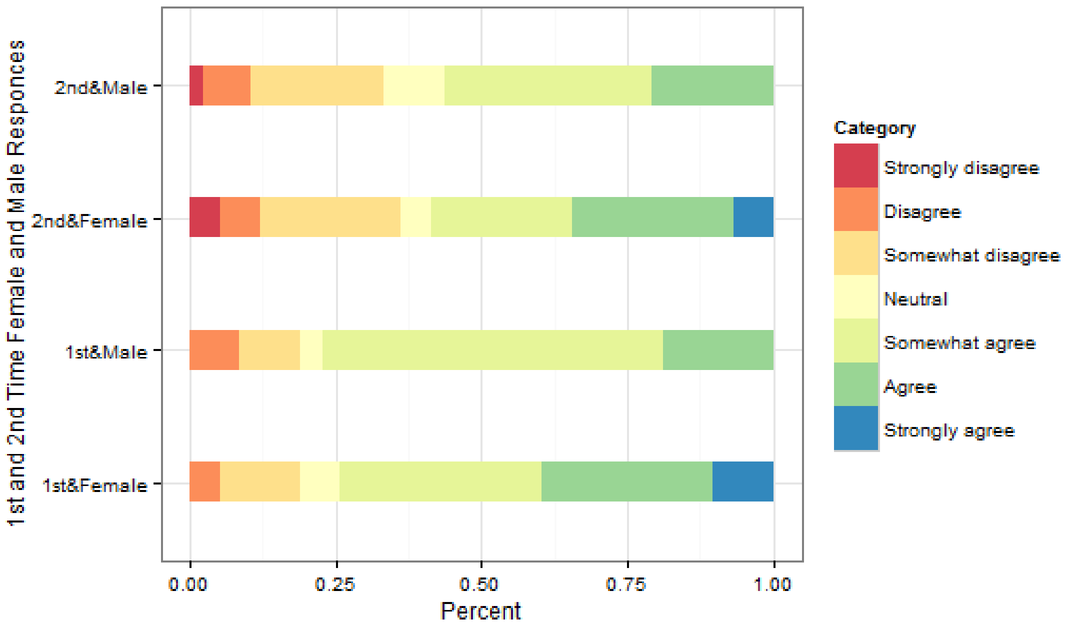


Figure 4.7: Breakdown of "approximate location helps to protect location privacy" responses in the 1st and 2rd time in female and male respondents respectively on 7-point Likert Scale. We obtain the percentage using 58 and 48 the total number of female and male respondents respectively as the base.

in the “Disagree” categories. After seeing the ground truth in the survey, both female and male respondents tended to doubt the approximate location’s privacy protection ability.

4.4 Summary

This chapter presents a concise novel contribution towards understanding people’s mental models of Android smartphone platform’s permissions. This chapter also contributes to our knowledge of how people generally understand localization technologies.

CHAPTER 5

FIELD STUDY OF RUN-TIME PERMISSION REQUEST DISCLOSURES AND CONTROL

5.1 Overview of Chapter

Privacy challenge becomes more and more pervasive as smartphones become more and more popular. Smartphones abilities and functionality are enhanced by a variety of apps. These apps have unprecedented access to users' private data including location and contacts. According to Pew Research more than 67% of adults in the U.S. own a smartphones and Android is one of the top two popular smartphone platforms. Users were concerned about their privacy regarding the personal data access on their phones. The report (Olmstead & Atkinson, 2015) by PewResearchCenter in 2015 suggested that 60% of app downloaders decided not to install a new app when they found out how much personal data were required by the app. The study by Chen et al. (Jorgensen et al., 2015) suggested that 74% of participants in their "study 1" ranked information privacy as the most important risk associated with installing applications. It should be noted that these participants had computer/smartphone security knowledge. Participants listed 14 types of personal information including address book, location, photos/videos, files, etc. Previous studies suggested that permissions at install-time were not effective to help users make informative decisions. Users either ignored the permissions or could not effectively understand the permissions' meanings. The problem was that how can we effectively notify users of their apps permissions request and help them make informative decisions about their apps permission request? We suppose that users can both enjoy the functions of the apps and conveniently control these apps' permissions request. A post-installation and run-time permissions disclosure method is proposed in this chapter. Users can decide if they allow the apps to access specific permissions when they use the app. In order to determine different timing to show all permissions details, we also provide an option to review all of the permissions information in our run-time disclosures. If participants reviewed the permissions details when they use the app, they might make more informative decisions by evaluating the functions of the apps and the payoff to exposing their private data to these apps. To the best of our knowledge, showing all permissions at run-time and evaluating the effectiveness of run-time feedback of the app being used has not yet been investigated. Hazim Almuhimedi's work (Almuhimedi et al., 2015) focused on how the run-time summary of some apps' permissions request enhanced the effectiveness of fine-grained controls. Our study was different from their work in that we focused on evaluating the effectiveness of run-time permissions of the single app being used and the effectiveness of run-time feedback. In our study, participants only need to make one simple click then they could review the entire permissions summary for the specific app. They could give feedback of their willingness about the app's permission request by only one click.

The iPhone with iOS 6 or later already has the run-time permissions request notification with Don't Allow or OK options. The notified permissions include Location, Contacts, Calendars, Reminders and Photos. Since Oct 2015 Android 6.0 Marshmallow (API level 23) has requesting permissions as a run-time feature. Android permissions were divided into two kinds of permissions: normal and dangerous permissions. There are nine groups in the dangerous permissions category. They are CALENDAR, CAMERA, CONTACTS, LOCATION, MICROPHONE, PHONE, SENSORS, SMS and STORAGE. A previous study by Fisher et al. (Fisher, Dorner, & Wagner, 2012b) analyzed the history data of apps location setup list. They carried out an online survey to collect the screenshots of iPhone users' location setup list. So far, as we know, there is no field study based on the effectiveness of run-time permission with instant reactions for each app. The study by Almuhimedi et al. (Almuhimedi et al., 2015) showed a summary on permissions request such as location permission. They did not show separate notification for a separate app.

Our previous study (Fu et al., 2014) focused on each app's location request run-time disclosures. It showed that run-time disclosures increased the transparency of apps location request on users' Android phones. Some participants in that study already took some actions to manage their apps' location usage. This permission disclosure study investigated several permissions run-time disclosures. The disclosures supplied participants with the instant reaction options. The study by Almuhimedi et al. (Almuhimedi et al., 2015) suggested that instant nudges of private data access increased the usage of the permission manager. There were no instant setup options on their nudges. Their study showed a history summary of permission request by several apps. Their participants need to link to the AppOps to induce a reaction. Our study was different in that we added the instant reactions options including

OK or NotOK in the run time notifications. Additionally, we evaluated the instant reactions effectiveness.

The instant reaction options were expected to help users quickly make decisions and take reactions conveniently. Patil et al. (Patil, Hoyle, Schlegel, Kapadia, & Lee, 2015) compared different feedback schemes: feedback of location request in delayed or immediate timing, with or without reaction options. Their study used their own developed app Locasa Study App and only disclosed location request by four recipient categories. Our study disclosed the permission request by apps participants used regularly. Our study investigated how to design a user friendly and useful run-time permission notifications.

Our study suggested that participants liked the instant reactions options. Participants preferred the instant reaction options in the run-time disclosures. They would like to have a single notification with all concerned permissions for each app. Too many and too frequent run time notifications interrupted users' usage of phones and decreased their attention to the run-time permission request disclosures.

5.2 Method

In this section, we described the recruitment and participants, design of the study app and study procedures. We investigated how Android users reacted toward the run-time notifications with instant reaction options per-app based in their daily lives.

5.2.1 Recruitment and Participants

Participants were recruited using several methods. Online advertisements were posted on Reddit Rutgers and local mailing lists and flyers were distributed on campus.

Participants were told that there was a study evaluating Android phone users' apps usage attitudes. Participants were screened by the following criteria: own an Android phone with Android version 4.4.4 or below; age 18 or over; speak English; can join interview session in person.

We recruited 11 participants. Four participants were female, seven were male. The average age was 24.9 with a standard deviation as 4.8. Six participants were graduate students, two were college students, one was an undergraduate student, one was a scientist, and one was a business accountant. Seven were from an Asian country and four were from the USA. We referred our 11 participants as P1 to P11.

All participants were compensated with $25 gift card and included in a raffle for two $50 gift cards. Our study was approved by the IRB Rutgers University.

5.2.2 Run-time Disclosures Design and Implementation

We designed and implemented the study app. The study app could show run-time disclosures about each app's LOCATION, CONTACTS or INTERNET permissions request separately.

User Interface and Interventions

Our study app was designed by referring to the previous studies based on the effectiveness of permission disclosures at install time or at run-time. The study by Felt et al. showed that permissions at install time were not effective in informing users of a new app's permissions request (Felt, Ha, et al., 2012). A previous study by Almuhimedi et al. (Almuhimedi et al., 2015) and our study (Fu et al., 2014) suggested that run-time notifications or instant nudges raised participants' awareness of apps' private information request. Some participants took active reactions towards some apps to manage private data usage on their phones. These previous works did not have the instant reaction options. Participants either had to link to AppOps permission manager (Almuhimedi et al., 2015) or had to uninstall or manually check a specific app's settings (Fu et al., 2014). We noted that the study app in the work by Almuhimedi et al. (Almuhimedi et al., 2015) gave an option to "keep sharing my location." The option was not for a single app, it was for several apps' permission request. We aimed to investigate the effectiveness of run-time permission disclosures with instant reaction options for a single app being used.

Three permissions were selected to be notified in the study app. They were LOCATION, CONTACTS and INTERNET. The first two permissions were in the dangerous permission category and the last one was in the normal permissions category. These three permissions were requested frequently by the apps.

The study by Chia et al. (Chia, Yamamoto, & Asokan, 2012) summarized a list of the top 12 most requested dangerous permissions. INTERNET, MEMORY (Write External Storage) LOCATION, CONTACTS, CAMERA, MICROPHONE (Record Audio) were all in the top 12 list. Interestingly, their study classified INTERNET to the dangerous permissions category. But on the Android Developers website INTERNET was not in the dangerous permissions category [1].

The main screen of the study app, including the number of installed apps on the phone, is shown in Figure 5.1. There were three buttons, each marked with permission name and number of apps requesting permission. For example, in Figure 5.1 there

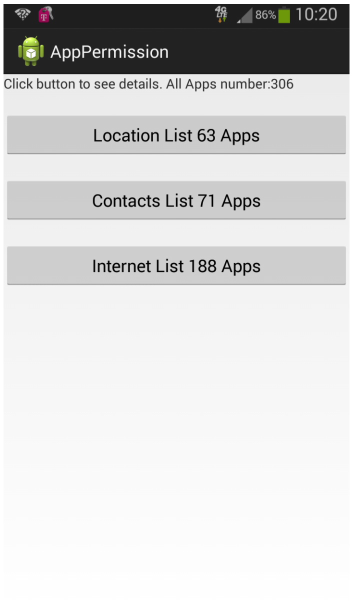
[1] Android Developers System Permissions https://developer.android.com/guide/topics/security/permissions.html

are a total of 306 apps on the Android phone and 63 apps requesting LOCATION permission. Each button can be clicked and linked to a setup list.

The setup list shows all the apps requesting the specific permission. There are three lists: LOCATION permission list, CONTACTS permission list and the INTERNET permission list. One example of the setup list is shown in Figure 5.2. It is a list of all the apps that request the LOCATION permissions. The number of apps in the list is shown on the top of the screen. Each item in the list includes the following information: app's name, app's icon and the time in which the app was installed on the phone. A button can be switched between OK and NotOK. This button allows participants to express their opinion about the permission request by the app. The design of the setup list for CONTACTS and INTERNET is the same as the setup list for LOCATION permission.

The run-time disclosure dialog is shown in Figure 5.3 and Figure 5.4. The run-time disclosure dialog has two versions, one for the first stage of the study (see Figure 5.3), the other for the second stage (see Figure 5.4). The dialog shows which app is requesting what permissions. In detail, it shows the app name and icon, the permission name and icon. It also includes the number of all permissions the app requests. The first time the app Contacts was opened in the study, a dialog was shown with the title "Contacts Internet perms 30." There was a detailed explanation: "Contacts requests your Internet and totally requests 30 permissions." The dialog is only shown once the first time the app is opened.

A button "PermissionDetail" is available for both stages. The "PermissionDetail" can be clicked and a new dialog will pop up with a list of all permissions the app re-



AppPermission

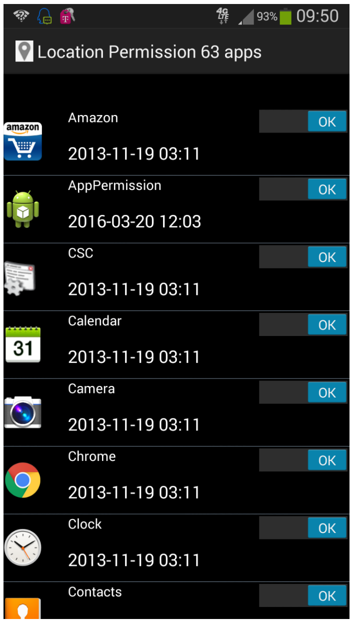
Click button to see details. All Apps number:306

Location List 63 Apps

Contacts List 71 Apps

Internet List 188 Apps

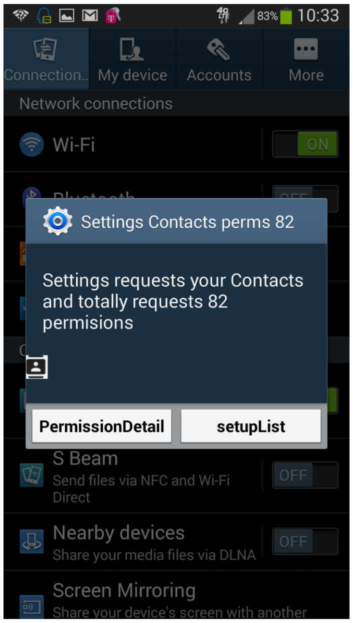
Figure 5.1: The main screen of the study app shows a general summary of the three permissions. It shows the number of apps requesting each of the three permissions: LOCATION, CONTACTS or INTERNET as well as the number of apps installed on the phone.



Location Permission 63 apps

Amazon 2013-11-19 03:11	OK
AppPermission 2016-03-20 12:03	OK
CSC 2013-11-19 03:11	OK
Calendar 2013-11-19 03:11	OK
Camera 2013-11-19 03:11	OK
Chrome 2013-11-19 03:11	OK
Clock 2013-11-19 03:11	OK
Contacts	OK

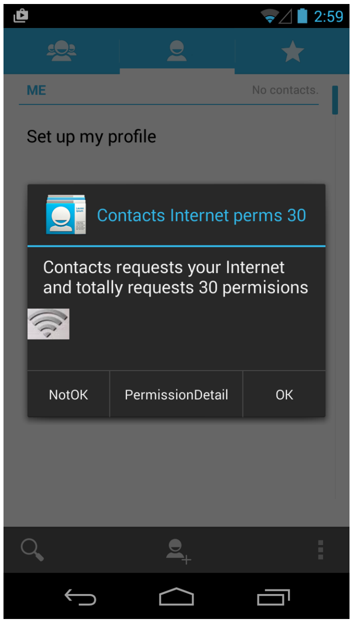
Figure 5.2: The setup list for LOCATION permission shows all the apps that request LOCATION permission. The button can be switched between OK or NotOK.



Settings Contacts perms 82

Settings requests your Contacts and totally requests 82 permisions

Figure 5.3: The run-time disclosure dialog in the first stage. The dialog has two options: PermissionDetail and setupList.



Contacts Internet perms 30

Contacts requests your Internet and totally requests 30 permisions

Figure 5.4: The run-time disclosure dialog in second stage. The dialog has three options: OK, NotOK and PermissionDetail.

quests as shown in Figure 5.5. The permissions in the dangerous permission category are directly shown in the list. Other permissions in the normal permissions category are hidden. The button “Show Others” can be clicked and another dialog will pop up with both dangerous and normal permissions. In the following, we use “Others” for short. A button “setupList” is available only for the first stage. The “setupList” can be clicked and linked to the main screen of the study app shown in Figure 5.1. Two buttons labeled as “OK” and “NotOK” are available only for the second stage. The “OK” or “NotOK” buttons can be clicked to make instant reactions towards the notified app’s permission request. We noted that the study app did not have the ability to enable or disable apps’ permission request.

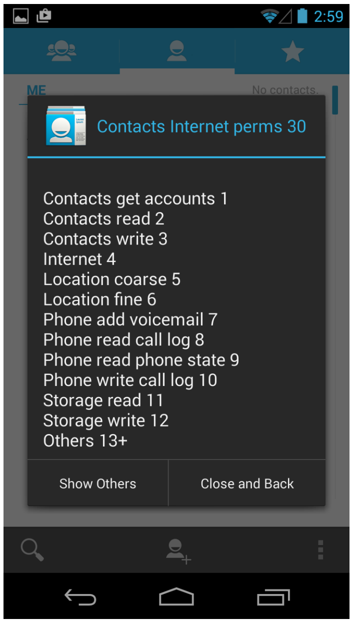
The notifications were shown instantly when participants opened their apps at the first time. If more than one kind of permission was requested by the app, there would be separate notifications shown one by one.

In each stage the combination of apps and permissions would only be notified once. There were records of notified apps and permissions combinations. The recorded ones would not be notified again in the same stage. At the end of the first stage the records were cleared and reset.

5.2.3 Procedure

Our field study was carried out using the participants’ own smartphones during their daily lives. The study consisted of an entry session interview, two stages of field experiments and an exit interview.

In the entry session, participants read and signed a consent form. They were



Contacts Internet perms 30

Contacts get accounts 1
Contacts read 2
Contacts write 3
Internet 4
Location coarse 5
Location fine 6
Phone add voicemail 7
Phone read call log 8
Phone read phone state 9
Phone write call log 10
Storage read 11
Storage write 12
Others 13+

Figure 5.5: The screenshot of permission details. It shows major permissions the app requests. It has two buttons: “Show Others,” “Close and Back.” When “Show Others” button is clicked all the left permissions will be shown. When “Close and Back” button is clicked the permission details window will be closed and the run-time disclosure dialog will be shown again.

told that the study was about users' attitudes toward their apps' permission request on their phones. A study app would be installed on their Android phones. The study app would collect some data from their smartphones including: apps used in the study period, permissions requested by apps, reactions made towards the study app. The study app did not collect any other personal identifying information. After signing the consent form, participants completed a short interview. The interview investigated participants' knowledge of their apps permission request, their attitudes toward the permission request, their awareness of the permissions at the install time and their general privacy attitudes. Participants were asked to keep their current Android versions until the end, the study app was uninstalled on their phones.

The field study was divided into two stages. In both stages, the run-time disclosures would show the app permission request in a run-time dialog. In each stage, participants received a run-time disclosure of the app's permission request the first time they opened an app. As mentioned before, LOCATION, CONTACTS and INTERNET were the three permissions notified by the study app. In the first stage, there were two buttons in the run-time disclosure dialog. One button named "PermissionDetail" could be clicked to show all permissions the app requested. The other button named "setupList" could be clicked and show the main screen of the study app. We noted that we did not link the "setupList" button to the specific permission setup list. We supposed participants could be aware of the main screen feature and explore the setup list. After reviewing the permission details, participants could close the permission detail and go back to the run-time disclosure dialog. The dialog would disappear when participants click other areas of the phone or click the back button on their devices. We noted that there was no button made available to close the dialog in the study app. In the second stage, there were three buttons in the run-time disclosure dialog. They were named “OK” “NotOK” and “PermissionDetail”. The “OK” or “NotOK” buttons were the instant reaction options. After participants clicked “OK” or “NotOK,” the dialog would disappear. Participants could click the back button on the phone to ignore the dialog.

We would like to compare the effectiveness of instant reaction options at run-time disclosures. We supposed that the instant reaction options would encourage more reactions than using the delayed reaction methods. The delayed reaction methods were not convenient for users to take reactions. Either they required more than one steps to take reactions or they had the users close a currently active app and open a new app such as Settings to take reactions.

In order to reduce our interference with the participants’ reactions we did not inform the participants of the meaning behind the “OK” and “NotOK” buttons, or other reactions options in the study.

The limitation of our study was that the app could not readily disable or enable apps permission requests. Our samples were limited to users with Android version 4.4.4 or below. The Android 6.0 users percentage was 1.2% and 4.4.4 or below users percentage was 65.7% on February 2016.

In the exit interview, participants visited our lab to complete an interview and had the study app uninstalled from their phones. We then questioned the participants to gather feedback on the study app, their knowledge of app permissions, and their usage of the study app.

5.3 Results

In this section, we present the results of the entry and exit interview and the reactions participants had towards the study app.

Permissions information at install time could help participants decide if they want to install a new app or not. Most of the participants read permissions at install time once in a while. Some of them decided not to install one or several apps due to permissions request. The reasons they declined to install the new app were either for privacy or devices performance concern. For example, P2 said “I decided to not install a new app which takes too much memory and the app is not very useful.” P4 read permissions before downloading an app from a third party. He showed no concern when downloading apps from the Google Play Store.

Our study app increased participants’ awareness of the large number of permissions requested by apps. P1 was surprised “apps asked a lot of staff” when she referred the detail of apps’ permissions. P5 said “many apps requested a lot of permissions.” As mentioned before, participants could click PermissionDetail and review a list permissions the app request. Participants were impressed by the long lists of permissions rather than the number we summarized in the notification dialog. The long list was more impressive and obvious than a single number in the dialog.

There were some suggestions for improving the run-time disclosures in the study app. Most participants would like to receive only one notification showing all permissions requested by the app. Participants would prefer to have control options in run-time disclosures. It was less interruptive. Since only a few of permissions were dangerous and concerned, it was easy to review them with one glance. It could be designed as a list of permissions with a separate control button to deny or allow each permission's request. Some participants would like to setup a reminder to review or take reactions in the future. In case they were busy when the run-time disclosure pop upped, they could click a button to have it repeated 2 hours later or the next day. This reminder method would give participants more than one opportunity to take reactions. Just like the previous study by Almuhimedi et al. (Almuhimedi et al., 2015) mentioned, some participants would have taken reactions if they were not busy at that moment. The reminder method could help participants choose a time when they were not busy to review and take reactions. Two participants suggested that there should be a quick button to cancel the notifications. They mentioned that when there was an incoming phone call and the study app's disclosure pop upped and there was no way to pick up the call before the notification disappear. For example, in the first stage, there was no button in the study app to cancel the notification.

Participants would like to have the run-time disclosure feature on their phones. There were various reasons why participants were interested in permissions requested by apps. The reasons could be divided into unknow permission requests, privacy concern, devices performance, financial concern and user experience. Participants were concerned about data access without their awareness and permit. Run-time disclosure of permissions request was useful if some apps access some data without the users' knowledge and permission. Operations made by apps without participants' awareness or consent were noticeable concerns. P10 mentioned that he refused to install some apps because the apps might make phone calls or send SMS. P10 also declined to install some apps because these apps requested unnecessary permissions. He thought the app did not need so many permissions for its function. P6 reported a virus app scanned all documents downloaded from the Internet including the attachments in email. This virus app was detected by an antivirus app on her phone.

Participants would like to know which apps disclosed their personal data including location and contacts. Location data requested by social apps were more concerning to especially female participants. P1 said "The detail of permissions is useful. I can see what kind of permissions the app requests especially social apps." P6 would like to know the location permission request. She was worried that some social apps might disclose her location without her awareness. She might not like some unfamiliar friends on social network to know about the places she was visiting. Participants would like to be sure their devices performance by limiting the resources usage by apps. For example, P2 would like to know how much memory each app used because he did not like to waste the limited memory resources. P7 also had space concern on his devices and wanted to know memory usage. P7 wanted to know when the apps were requesting the INTERNET permission so as to not overuse his data plan. One participant P6 wanted to recognize the apps which brought up too many interruptions. Participant P6 did not like some apps requesting Internet permission. He thought that these apps would show a lot of spam and ads after connecting to the Internet. Participants would like to know when their financial information (credit card information) and password was accessed by apps. They did not like any apps to access these kinds of information. P5 said that she had an app to manage all of her passwords. She would like to be notified if other apps accessed the data in the password manager app. Several participants mentioned they were more concerned with the apps requesting credit card or other financial information. Participants would like to know if the apps might bring financial problems. P2 did not like the apps to use SMS without her authorization. She had a prepaid SMS plan, she had to pay for SMS sent out from her phone. P5 would like to know the apps accessing the downloaded documents. She downloaded some financial paper online. She did not like other apps to access this financial information.

It is possible to design the run-time disclosures in accordance to feedback from participants. Of the 11 participants, all had the same concern with permission requests, albeit for varied reasons and perspectives. The permissions to be notified could be decided by both developers and users. The priority to show permissions and the timing to show permissions might be different according to different users' concern. Users cared more about devices performance might want to know about memory and battery usage. Users cared about private data disclosures might want to know about their location, contacts, pictures access.

We explored the run time permission notifications on Android 6.0. Usually when an app was opened and the app need a specific permission to fulfill a function there would be a permission request shown on top of the screen with Deny or Allow options.

We could not carry out the study on Android 6.0 devices. We could not collect their real time reactions with the run-time disclosures. There were very small percentage of Android 6.0 users at the time we carried out our study. It was 1.2% Android 6.0 users on February 2016. We designed the study app to collect participants' instant reactions towards run-time disclosures.

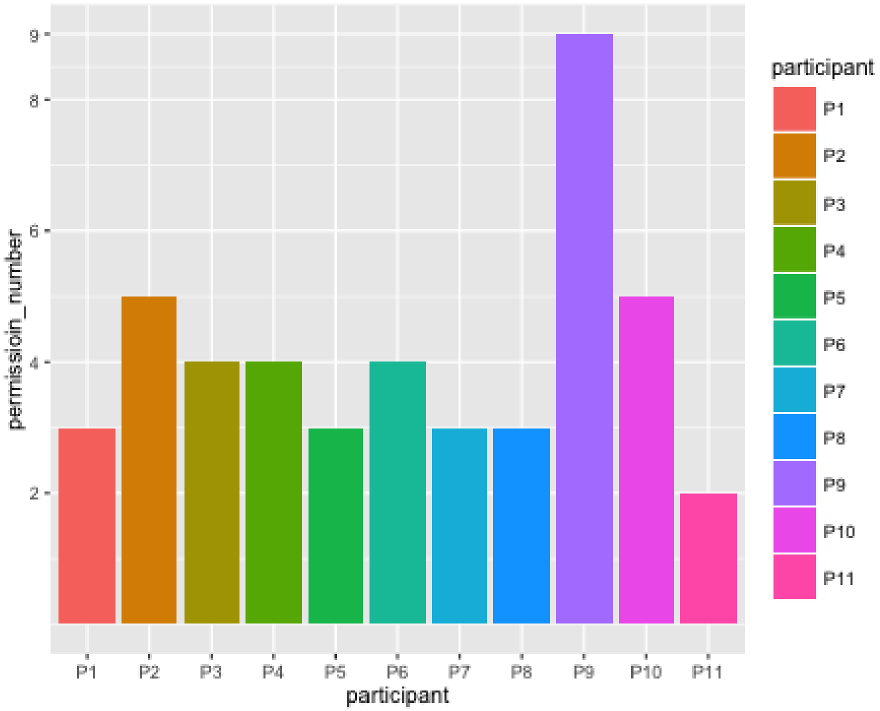


Figure 5.6: The number of permissions each participant chose to be notified in the future.

Participants would like to receive permission request at run-time. In the exit interview, participants were shown nine types of dangerous permissions defined by Android Developers. They were asked to select which permissions they wanted to be notified by. The summary of permissions selected by participants was shown in Figure 5.6. Most of the participants selected to be notified by three or four permissions. The minimum was two and the maximum was nine. One participant P10 chose all nine permissions to be notified at run-time. She thought all permission access should be by default denied. Permissions request should be authorized by users when setting up the phone.

How many participants selected each permission is summarized in Figure 5.7. Ten participants out of 11 chose location permission and wanted to be notified of

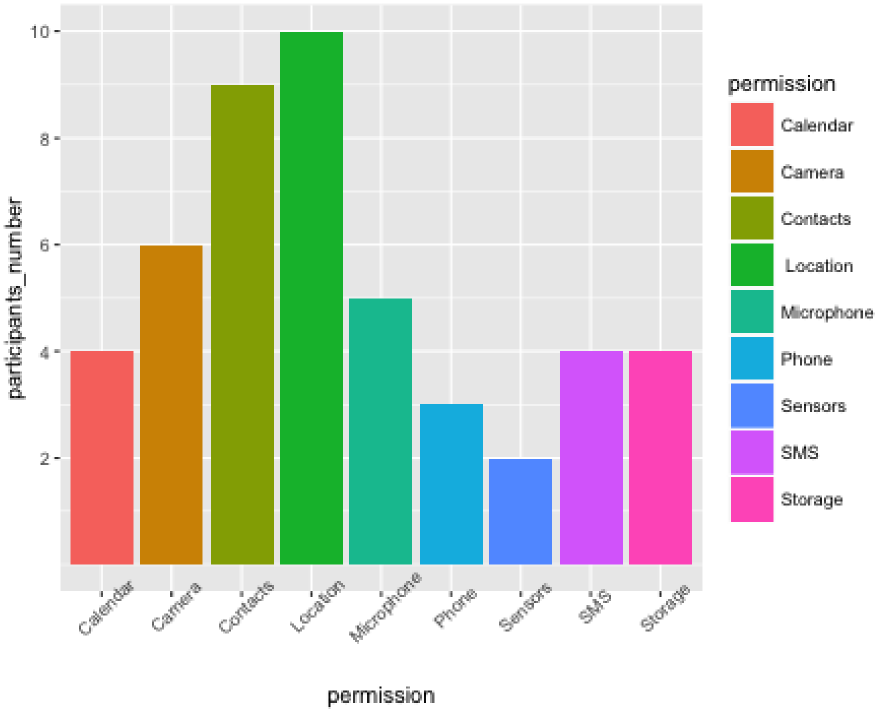


Figure 5.7: The number of participants choose each permission to be notified in the future.

a location request. This finding was different from previous study by Felt (Felt, Egelman, & Wagner, 2012). Their findings suggested that location was not of great concern to the participants.

One participant preferred to use the setup list to check the permission request rather than run-time disclosures. P2 was the only one who preferred the setup list over the run-time disclosure. He thought the setup list was easier to check about a specific app's specific permission request. He wanted to actively check via the setup list. After checking a newly installed app in the setup list, he decided to uninstall the app during the study.

One important finding in our study was that the setup list feature should be easy to access. We asked our participants whether they review the app's permission after installation. None of them reviewed. Some did not know how to check the permissions after installing the app. Others knew how to check but they did not use this feature. They thought our study app' setup list feature was more convenient to review the permissions. We explored the setup list features on Android 6.0, the setup list requires several steps to access. These steps were listed on the Google Play Help site with the title "Control your app permissions on Android 6.0 and up". There were four steps to review an app's all permissions: Settings, Apps Managers or Apps, Apps list, click on an app and review or setup permissions for this app. The permission type order list option was hidden in the gear icon in right up corner in the Apps list screen. The list showed dangerous permissions, after a specific permission was clicked, a list of apps requesting the specific permission was shown up. According to our study, we recommend moving the permission type order setup to a more obvious place instead of hidden in the gear icon. It can be put in the privacy control. It could be accessed with less steps.

Nine participants (P1,P3,P4,P5,P7,P8,P9,P10,P11) clicked the "setupList" button. Six out of the nine participants (P4,P5,P7,P8,P9,P11) did not know the setup list feature ((Demonstrated using location permission list 5.2). The reason was that the "setupList" button did not link to the setup list for a separate permission, instead it linked to the main screen of the study app (shown in Figure 5.1). If we would have changed the "setupList" button directly link to the list of apps, more users should have known about the "setupList" even checked about the list of apps. They might have reviewed the setup list feature more frequently. They thought the setup list feature was useful after we showed this feature in the exit interview.

We would discuss the data collected during the two to four weeks field study. For the 11 participants, we collected operations in setup list feature and reactions in run-time disclosure dialogs. We discussed participants' reactions towards the study app in the following. There were totally 451 rows data in setup list record. As we mentioned before, setup list records included all the OK or NotOk clicks participants made. Participants could click OK or NotOK in run-time disclosure dialogs which only available in the second stage (Figure 5.4) or in the setup list available in both stages (Demonstrated using location permission list 5.2).

Eleven rows of records were operations in setup list feature. Five participants P1, P5, P6, P8, P9 did the switch operations in setup list. Most of them setup one app's permission as NotOK and changed back to OK instantly. They did not use the setup list to control the app's permission request. They just explored the switch button in the setup list. The left 440 rows in setup list records were clicks of OK or NotOk in run time notifications dialog.

The summary of records of the reactions towards run-time disclosures is shown in Table 5.1 and Figure 5.8. We use short words to represent the options in tables and figures: "detail" for "PermissionDetail." Each participant's reactions are summarized in Table 5.2 and Figure 5.9. There were 1518 rows, out of which 766 rows are in the first stage and 752 rows are in the second stage. In the whole study, 1028 out of 1518 records were ignored reactions. The remaining 490 records were participants' interactions with our study app. We will explain the 490 records of interactions with our study app in the following.

Of the 490 records where participants button clicked the run-time disclosure dialog, sixteen records were “PermissionDetail” reactions. Eight participants reviewed the permission detail feature (shown in Figure 5.5) one or several times. In both stages, the “PermissionDetail” button was available. Fifteen out of the sixteen reviews were at the first stage. Participants might just be curious about this feature and clicked it to explore. According to the reactions number, the permissions detail feature was not necessary in run-time disclosures. Moving permission from install time to run-time was not effective. When “PermissionDetail” was clicked, there were two further options: one was “Others” to show other hidden non-dangerous permissions; one was “Close and Back” to go back to the main screen of run-time disclosure. None of participants took the two further reactions after opening the “PermissionDetail” screen. Our finding was consistent with previous studies which suggested that permissions at install time were not efficient to inform users about apps’ permission request. Participants seldom reviewed apps’ permission details while running the app. We found out that permission details were not a necessary feature in run-time disclosure dialog.

Sixty-five records out of 490 were records of the “setupList” button click reactions. Nine participants reviewed the setup list feature. P9 reviewed the setup list twenty-eight times. It was the maximum reviewed number. Others checked one or several times. Only in the first stage, was the “setupList” button available. Participants were more interested in the setup list feature than the permission detail feature. The link to the setup list should be more useful and interesting than the permission detail features shown in the run-time disclosure. There were two potential advantages of supplying a quick link to setup list: at first, participants were able to be aware of the hidden feature to review and setup apps' permission request; secondly, participants could quickly link to the setup list feature with a single click.

The limitations of our "setupList" option was that it linked to the main screen (shown in Figure 5.1) of the study app, not directly to the one of the three permissions setup list (LOCATION, CONTACTS or INTERNET permission). If we would have linked the option to the setup list for each permission (Demonstrated using location permission list 5.2), there might have been additional records of the setup list reviews. In the interview, we found that some participants were not aware of the setup list. They did not know about this feature until we showed it to them in the exist interview. After reviewing the setup list feature, most of them thought it was a good feature to have. Most of them showed an interest to explore the setup list and to review the list of apps requesting their data. They thought that it was good to know that so many apps were requesting their data. They would like to have real functionality to control the apps' permission request by clicking OK or NotOK. Linking directly to the setup list would be more informative and interesting for participants than showing the main screen with a general summary of all permission request.

There were 358 OK and 51 NotOK rows of data out of 490 interactions records. OK and NotOK options were only availabe in the second stage of the study. Nine participants clicked OK either four times or tens of times. For example, P4 clicked OK 80 times being the maximum out of all participants. Only five participants clicked NotOK. They clicked NotOK one or several times. P8 had the maximum NotOK click times at 45. During the interview, P8 told us he did not like the apps' permission requests and clicked NotOK most of the time. He clicked NotOK 45 times

reactions	ignore	ok	notok	detail	others	setuplist	sumup
1st stage	686	0	0	15	0	65	766
2nd stage	342	358	51	1	0	0	752
both stage	1028	358	51	16	0	65	1518

Table 5.1: Summary of participants' reactions towards run-time disclosures. They were grouped into two stages.

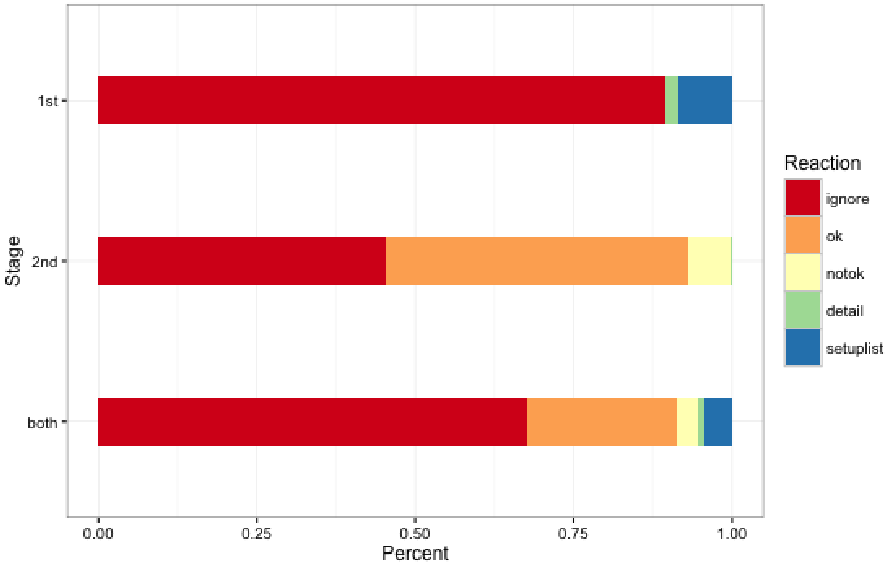


Figure 5.8: Summary of participants' reactions towards run-time disclosures. They were grouped into two stages.

and clicked OK 14 times. He did so purposefully to let us know his opinion of the apps' permissions requests.

Most of participants' reactions were ignore during the study. There were 1028 (67.7%) ignore reactions in the first and second stage totally. There were 686 (89.6%) ignore reactions and 342 (45.5%) in first and second stage respectively. It was shown in the Table 5.1 and Figure 5.8. Every participant had the maximum number of reactions in the ignore option as shown in Table 5.2 and Figure 5.9. P2 had only one kind of reaction, he ignored all the disclosures, during the whole study. In the second stage, the largest percentage (54.4%)of reactions were OK or NotOK.

The reactions of each participant in the first and second stages were separately

reactions	ignore	ok	notok	detail	others	setuplist
P1	87	67	0	1	0	8
P2	122	0	0	0	0	0
P3	91	70	1	1	0	1
P4	90	80	0	8	0	1
P5	75	58	1	1	0	3
P6	108	25	3	1	0	0
P7	82	35	0	1	0	3
P8	73	14	45	0	0	6
P9	95	4	1	0	0	8
P10	78	5	0	1	0	28
P11	127	0	0	2	0	7

Table 5.2: Summary of each participant reactions towards the run-time disclosures. They were grouped into 11 participants.

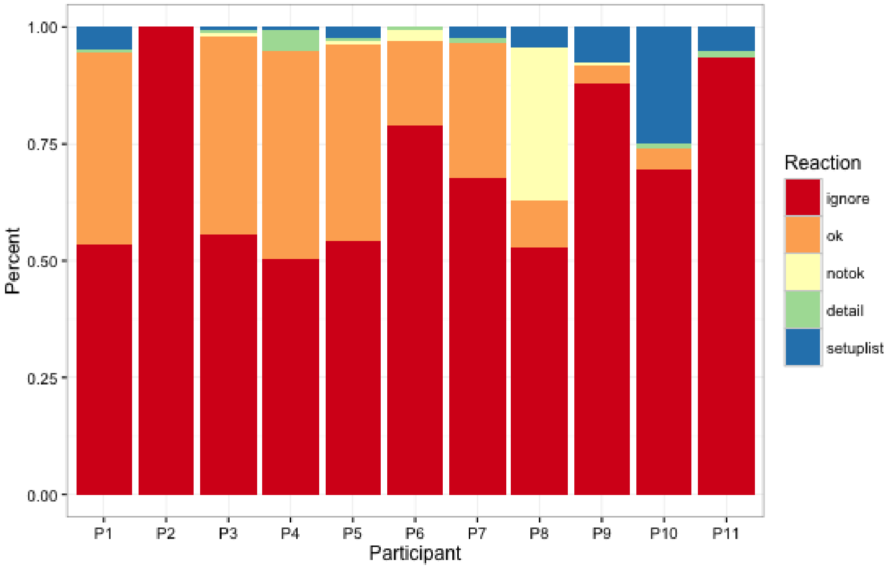


Figure 5.9: Summary of each participant reactions towards the run-time disclosures. They were grouped into 11 participants.

reactions	ignore	detail	others	setuplist
P1	70	0	0	8
P2	77	0	0	0
P3	77	1	0	1
P4	76	8	0	1
P5	64	1	0	3
P6	70	1	0	0
P7	58	1	0	3
P8	54	0	0	6
P9	53	0	0	8
P10	18	1	0	28
P11	69	2	0	7

Table 5.3: Summary of reactions of each participant in the 1st stage. In the 1st stage, the options of OK and NotOK were not available. So, we did not show OK and NotOK options in this table.

shown in Table 5.3 Figure 5.10 and Table 5.4 Figure 5.11. In the first stage, participants' reactions were very similar. More than 80% percentage of reactions was ignore for all participants except one participant (P10). "Setuplist" button was more interested to participants than "PermissionDetail" button. Seven participants had more reactions in Setuplist than PermissionDetail. In the second stage, participants' reactions in the second stage were varied. Five participants had OK reactions as the largest percentage, the other five participants had ignore reactions as the largest percentage. One participant had NotOK as the largest percentage. "PermissionDetail" button was available in both stages. The number of participants who click "PermissionDetail" decreases from first stage to second stage. In the first stage, seven participants clicked "PermissioinDetail" button. Only one participant clicked the "PermissionDetail" button in the second stage.

There were three reasons for why there were so many ignore reactions. First, in the first stage, we did not supply an option to close the dialog in our study app. Ignore was the way to cancel the run-time disclosure dialog. Participants had to click

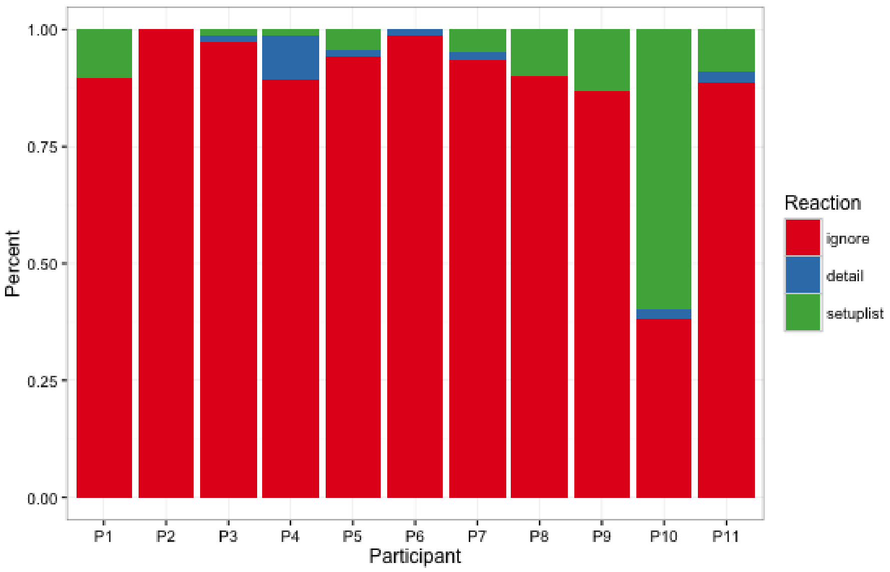


Figure 5.10: Summary of reactions of each participant in the 1st stage. In the 1st stage, the options of OK and NotOK were not available. So, we did not show OK and NotOK options in this figure. There was no reaction in “Others”, so this option was not shown in this figure.

reactions	ignore	ok	notok	detail	others
P1	17	67	0	1	0
P2	45	0	0	0	0
P3	14	70	1	0	0
P4	14	80	0	0	0
P5	11	58	1	0	0
P6	38	25	3	0	0
P7	24	35	0	0	0
P8	19	14	45	0	0
P9	42	4	1	0	0
P10	60	5	0	0	0
P11	58	0	0	0	0

Table 5.4: Summary of reactions of each participant in the 2nd stage. In the 2nd stage, the option “setupList” was not available. So, we did not show this “setupList” option in this table.

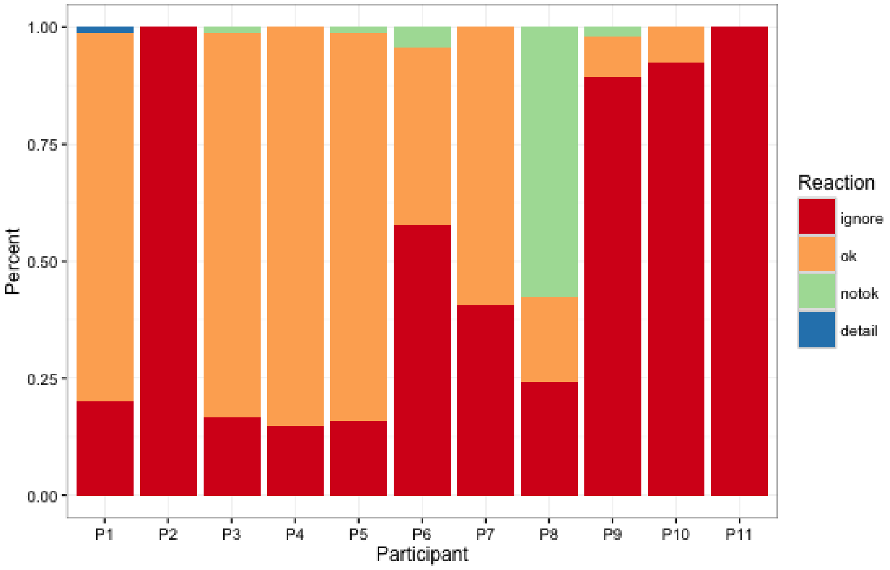


Figure 5.11: Summary of reactions of each participant in the 2nd stage. In the 2nd stage, the option "setupList" was not available which was not shown in this figure. There was no reaction in "Others", so this option was not shown in this figure.

space out of the dialog to ignore it or click the return key on their devices. Second, most of participants thought it was interruptive because there were too many run-time disclosure dialogs. They just wanted it gone as soon as possible. They might have clicked the return button to make the disclosure dialog disappear. In the exit interview two participants (P9, P10) explicitly suggested that the study app could allow an option to close the run-time disclosure dialog. It would be convenient for users to close the dialog. Third, some participants thought they already knew about the permissions requested by the apps because they have reviewed the permissions at install time. It was not necessary to review them again.

There was a reason why some participants had more OK and NotOK reactions than ignore reactions in the second stage. In the second stage, if the participants clicked the OK or NotOK, the dialog would disappear instantly. For some participants, clicking OK button might be more convenient so they clicked OK or sometimes NotOK simply to get rid of the dialog.

Too frequent and too many run-time disclosure dialogs did not increase participants' attention to permission requests. On the contrary, most of the participants found it interruptive and just wanted it disappear fast. Most participants ignored the run-time disclosures. This finding was different from the previous study by Patil et al. (Patil et al., 2015) where they found out that too much information made participants more worried about their privacy.

Some data was missing in the run-time disclosure reactions records OK and NotOK. Because there were 409 (358 OK and 51 NotOK) rows in run-time disclosure reaction records but 440 rows in setup list records with OK NotOK reactions via run-time disclosure (setup list recorded and showed the run-time disclosures reactions with OK or NotOK). We claimed that these missing data did not affect our findings in this study.

In the interview our participants were not sure about what the OK, NotOK really meant. As mentioned before, we did not tell participants about OK and NotOK in the entry interview. We wanted to let participants experience and explore the study app's features themselves. We would like to reduce our personal interference of the study.

5.4 Summary

Participants would like to have the run-time disclosures of app's permission request with instant control options. All participants chose two or more permissions to be notified in the future. They would like to have control over their apps' permission access on their phones. Participants would like to receive one run-time disclosure of all concerned permissions for each newly installed app.

Too many too frequent run-time disclosures were considered interruptive. It decreased participants' attention to the disclosures.

Our results suggested that the control options in run-time disclosures was convenient for participants to take reactions. During the first stage, most of the disclosures were ignored. During the second stage, most of the disclosures were reacted to by clicking OK button.

After the study, we proposed some improvements to the design of the run-time disclosures. All concerned permissions of each newly installed app could be notified in one run-time disclosure dialog. Each permission had its own control button. It could be denied or allowed separately.

CHAPTER 6

DISCUSSION

6.1 Field Study of Run-Time Disclosure Findings and Limitations

Through a four-week randomized field experiment, we examined the efficiency of run-time location access disclosure during participants' daily lives. Our results showed that our run-time disclosures were effective in informing participants of their apps' location access. It helped participants to discover apps they did not expect to access their location. Participants could recognize unnecessary location accesses by some apps because of the context information supplied by the run-time disclosures. Several participants were also alarmed by how often some apps accessed their location. In contrast, participants in the No Disclosure group were not aware of the apps' location accesses and did not take any actions to manage the location accesses.

Our work confirms the existing research literature that Android permissions are not an effective method for disclosing and consenting for location data access. The previous work (Felt, Ha, et al., 2012; Kelley et al., 2012, 2013) has shown that Android's installation-time permissions are usually ignored by users and the permissions are hard to understand. Our results showed that the existing location access disclosure mechanism on the Android platform, the flashing GPS icon, was not effective to inform users of apps' location accesses. Nearly all participants in the two groups had some apps they did not expect to access their location. The reasons a flashing GPS icon was not efficient might be that it did not tell users explicit information such as the name of apps which were accessing location. Participants could only guess that their location was being accessed with GPS but they did not know by which app.

We found that in the Disclosure group, participants took various actions to protect their privacy, in the form of 1) uninstalling apps, 2) stopping the use of some apps, 3) reducing the time using some apps and 4) searching through apps' setups to disable location accesses. This suggests that participants were willing to manage apps they used to limit location access. By contrast, participants in the No Disclosure group had not taken any actions to manage specific apps' location access due to the existing location access disclosure mechanism on Android phones.

Most participants were making explicit privacy vs. utility tradeoffs. They kept using some apps whose functions were necessary or beneficial for them even though location was not necessary for these apps' function. In contrast, some participants gave up convenience to use an app in order to keep their location privacy.

According to participants' reactions apps can be divided to three categories. The first category of apps is not critical to users and these apps access location against users' expectations. Participants would usually take actions towards apps in this category. For example, game apps usually fall in this category. The second category of apps are helpful to users, but location accesses feel unnecessary. It is acceptable to most participants so long as the category of apps benefit users in some way. For instance, Video player, Dictionary and some chatting apps usually belong to the second category. The third category is useful to users and the apps required access to location in order to provide functionality. An obvious example app in this category is Google Maps. Our results confirmed a previous survey's (Fisher et al., 2012a) finding that users "grant access more often to apps where location is central to the purpose of the app than to apps where location is a more optional feature or where it is less clear what benefit the user gets from sharing their location."

Design Implications. Based upon the reactions of our participants we discovered the following design implications. Explicit disclosure information (what app is accessing location and when) should be included on smartphones. The frequency of the disclosures should be reasonable and non-intrusive. Participants suggested reducing how often they received disclosures in our study. Hundreds of notifications in three weeks seemed excessive for participants. As participants were concerned of the frequency of location accesses, statistics could be included in list of apps. Some participants suggested including a setup option to disable notifications. After three weeks experience, our participants might have already learned most of the apps' location access behaviors. We noticed that some participants mentioned they preferred silent notifications in the notice bar. They considered that sometimes the sounds of the notifications were intrusive in public settings. The toast notification on the screen might be more acceptable if it could be designed to cover only a small area of one side of the screen.

Enabling users to choose can an app access location would be helpful. So far, there is only a generic localization configuration available on the Android platform. Users can either allow all apps to access location or deny all apps' location access. In contrast, iPhone has the "Location Services Settings" to manage a specific app's location access. A previous study (Fisher et al., 2012a) has shown that several users have used this feature on the iOS platform to disable location access for some of their apps.

Limitations We consider that the ecological validity of our study was good, because 1) we studied our participants in their daily lives with the smartphones they already owned, and 2) we did not give any instructions or training on how to use or react to our app.

The purpose of randomly assigning participants to the No Disclosure group and the Disclosure group was to provide assurance that effects occurred during the study period are due to our interventions with the Disclosure group, and not to other factors. Our results, including exit interviews, clearly indicate that this is the case.

We acknowledge certain limitations in our study. Our volunteer participants came only from our institution or nearby areas. Our participants were from different countries and they had different cultural backgrounds. Our study had more male participants than female participants. We did not screen participants of their technical skills.

Our heuristic method did not consider the condition that apps were accessing location in the background. However, this condition is very rare. We note that almost all apps do not access location in the background. Before the study, we verified this by testing the most popular apps from the app market. We had used location access permissions to filter apps so that only apps with the ability to access location were reported to access location by the study app. During the study, we had collected data of all the apps participants used. We verified that the findings and conclusions of our paper was not affected by any apps accessing location in the background.

6.2 Online Survey of Location Permissions Findings and Further Work

We collected 106 responses from MTurk and analyzed their understanding of the precise location and approximate location permissions on Android phones and their privacy model related to the approximate location.

Not surprisingly, most participants had a good understanding about what "precise" location means. However, participants varied considerably in how they understood what "approximate" location means. Over half (64.2%) of the participants thought that network-based localization was very inaccurate considering its accuracy to be equal to or more than 1 mi – 2 mi / 1.6 km – 3.2 km. Unsurprisingly, respondents understood the two location permissions better via the descriptions "precise" and "approximate" compared to the technology-based explanation using GPS and network-based location.

Our participants expected "approximate" location to cover a larger geographical area than it actually does. Their understanding might mislead them to trust the approximate location to protect their location privacy. Current versions of the Android location API obfuscate the network-based location to some degree. Our results indicate that there might be need for more obfuscation or a better way to inform the users about how accurate the localization actually is.

Finally, we note that participants' attitudes changed towards "approximate" location after they had been shown the ground truth in our survey. Prior seeing the ground truth, about 19% of participants thought that approximate location did not help to protect location privacy. After seeing the ground truth, almost 35% thought the same. This further indicates that the location permissions could be improved. For example, location permissions might use a combination of methods, including visualizations with maps and examples of accuracy of the localization.

6.3 Run-Time Permissions Request Disclosures and Control Findings

There were some limitations to our permission request disclosures and control study. First, our study app's instant reaction OK or NotOK did not have the real capability to control the app's permission request. Second, the study app could only run on Android 4.4.4 or below so the participants were limited to those who own an older Android version. The percentage of Android users with Android 4.4.4 was 70% when we carried out the study. Third, the small sample size, with 11 participants, was not large enough to have statistical conclusions. We could only have some summary and qualitative results.

Our study suggested that participants liked the instant reactions options. Participants showed more interest in instant control options than the permission detail list. They would like to have a single notification with all concerned permissions for each app. Too many and too frequent run time notifications interrupted users' usage of phones and decreased their attention to the run-time permission request disclosures.

CHAPTER 7

CONCLUSION

In conclusion, we investigate how to effectively disclose and manage private data request on smartphones. We make the following contributions:

First, we proposed a method to show run-time disclosure of location request on smartphones and carried out a four-week field study. Our study suggested that our designed run-time disclosure were effective to notify users of their apps' location request. Participants appreciate the transparency brought by the run-time disclosures. Most of them took actions to manage their app's location request after receiving the run-time disclosures. Our study contributes to designing mechanisms to increase the transparency of location access on smartphones and effectively inform users of their location request.

Second, we conduct an online survey about users' understanding of location related permissions on the Android platform. It showed that users had varied understandings of the location permission. Users expected too much privacy from "approximate location" in the end of survey, they realized that "approximate location" breached their privacy almost the same as "precise location". Our study contributes to the understanding of people's mental models related to smartphone app location privacy.

Third, we designed a run-time permission request disclosure with instant control options and conducted a two-week field study. Our study found out that participants would like to have the run-time permission disclosures and they like the instant control options. Too many and too frequent run time notifications interrupted users' usage of phones and decreased their attention to the run-time permission request disclosures. Our study contributes to understanding users' reactions and attitudes towards the run-time disclosure with instant control.

BIBLIOGRAPHY

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... Agarwal, Y. (2015). Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual acm conference on human factors in computing systems* (pp. 787–796). New York, NY, USA: ACM. Retrieved from `http://doi.acm.org/10.1145/2702123.2702210` doi: 10.1145/2702123.2702210

Anderson, J., Bonneau, J., & Stajano, F. (2010). Inglourious installers: Security in the application marketplace. In *Proc. of weis 2010.*

Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013). "Little brothers watching you": raising awareness of data leaks on smartphones. In *Proc. of soups'13.*

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., & Cranor, L. (2015). The impact of timing on the salience of smartphone app privacy notices. In *Proceedings of the 5th annual acm ccs workshop on security and privacy in smartphones and mobile devices* (pp. 63–74). New York, NY, USA: ACM. Retrieved from `http://doi.acm.org/10.1145/2808117.2808119` doi: 10.1145/2808117.2808119

Balebako, R., Shay, R., & Cranor, L. F. (2013). *Is your inseam a biometric? evaluating the understandability of mobile privacy notice categories* (Tech. Rep. No. CMU-CyLab-13-011). CMU.

Baokar, A. (2016). *A contextually-aware, privacy-preserving android permission model.* EECS Department, University of California, Berkeley. Retrieved from `http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-69.html`

Barkhuus, L., Brown, B., Bell, M., Sherwood, S., Hall, M., & Chalmers, M. (2008). From awareness to repartee: sharing location within social groups. In *Proc. of chi '08.*

Barrera, D., & Van Oorschot, P. (2011, May). Secure software installation on smartphones. *IEEE Security and Privacy*, *9*, 42–48. Retrieved from `http://dx.doi.org/10.1109/MSP.2010.202` doi: http://dx.doi.org/10.1109/MSP.2010.202

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Proc of sp '11.*

Beresford, A. R., Rice, A., Skehin, N., & Sohan, R. (2011). Mockdroid: trading privacy for application functionality on smartphones. In *Proc. of hotmobile.*

Boyles, J. L., Smith, A., & Madden, M. (2012). *Privacy and data management on mobile devices* (Tech. Rep.). Pew Internet. Retrieved from `http://pewinternet.org/Reports/2012/Mobile-Privacy/Key-Findings.aspx`

Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011, March). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, *9*, 18–26. Retrieved from `http://dx.doi.org/10.1109/MSP.2010.198` doi: http://dx.doi.org/10.1109/MSP.2010.198

Caine, K. (2009). *Exploring everyday privacy behaviors and misclosures.* Unpublished doctoral dissertation, Georgia Institute of Technology.

Chia, P. H., Yamamoto, Y., & Asokan, N. (2012). Is this app safe?: A large scale study on application permissions and risk signals. In *Proc of www '12.*

Chin, E., Felt, A. P., Greenwood, K., & Wagner, D. (2011). Analyzing inter-application communication in android. In *Proc. of mobisys'11.*

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In *Proc. of soups'12.*

Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. (2010). The wi-fi privacy ticker: improving awareness & control of personal information exposure on wi-fi. In *Proc. of ubicomp '10.*

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location disclosure to social relations: why, when, & what people want to share. In *Proc. of chi '05.*

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). Pios: Detecting privacy leaks in ios applications. In *Proc. of ndss.*

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2010). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of osdi.*

Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S. (2011). A study of android application security. In *Proc. of usenix security.*

Enck, W., Ongtang, M., & McDaniel, P. (2009). On lightweight mobile phone application certification. In *Proc. of ccs '09.*

Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. (2011). Android permissions demystified. In *Proc. of acm ccs.*

Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., & Wagner, D. (2012). How to ask for permission. In *Proc. of hotsec'12.*

Felt, A. P., Egelman, S., & Wagner, D. (2012, May). *Ive got 99 problems, but vibration aint one: A survey of smartphone users concerns* (Tech. Rep. No. UCB/EECS-2012-70). EECS Department, University of California, Berkeley. Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-70.html

Felt, A. P., Greenwood, K., & Wagner, D. (2011). The effectiveness of application permissions. In *Proc. of webapps.*

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: user attention, comprehension, and behavior. In *Proc. soups'12* (pp. 3:1–3:14).

Felt, A. P., Wang, H. J., Moshchuk, A., Hanna, S., & Chin, E. (2011). Permission re-delegation: Attacks and defenses. In *Proc. of usenix security.*

Fisher, D., Dorner, L., & Wagner, D. (2012a). Short paper: Location privacy: User behavior in the field. In *Proc. spsm'12* (pp. 51–56).

Fisher, D., Dorner, L., & Wagner, D. (2012b). Short paper: location privacy: user behavior in the field. In *Proc. of spsm'12.*

Fu, H., & Lindqvist, J. (2014). General area or approximate location? how people understand location permissions. In *Proc. wpes'14.*

Fu, H., Yang, Y., Shingte, N., Lindqvist, J., & Gruteser, M. (2014). A field study of run-time location access disclosures on android smartphones. In *Proc. usec'14.*

Gates, C. S., Chen, J., Li, N., & Proctor, R. W. (2014, May). Effective risk communication for android apps. *IEEE Trans. Dependable Secur. Comput.*, *11*(3), 252–265. Retrieved from http://dx.doi.org/10.1109/TDSC.2013.58 doi: 10.1109/TDSC.2013.58

Gerber, P., Volkamer, M., & Renaud, K. (2015, February). Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *SIGCAS Comput. Soc.*, *45*(1), 16–21.

Gilbert, P., Chun, B.-G., Cox, L. P., & Jung, J. (2011). Vision: automated security validation of mobile apps at app markets. In *Proc. of mcs.*

Harbach, M., Hettig, M., Weber, S., & Smith, M. (2014). Using personal examples to improve risk communication for security &#38; privacy decisions. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 2647–2656). New York, NY, USA: ACM. Retrieved from http://doi.acm.org/10.1145/2556288.2556978 doi: 10.1145/2556288.2556978

Heyer, C., Brereton, M., & Viller, S. (2008). Cross-channel mobile social software: an empirical study. In *Proc. of chi '08.*

Hong, J. I., & Landay, J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. In *Proc. of mobisys '04.*

Hornyack, P., Han, S., Jung, J., Schechter, S., & Wetherall, D. (2011). These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In *Proc. of the 18th acm conference on computer and communications security.*

Howell, J., & Schechter, S. (2010). What you see is what they get: Protecting users from unwanted use of microphones, cameras, and other sensors. In *Proc. of w2sp.*

Hsieh, G., Tang, K. P., Low, W. Y., & Hong, J. I. (2007). Field deployment of imbuddy: a study of privacy control and feedback mechanisms for contextual im. In *Proc. of ubicomp'07.*

Janice, S., Burke, W., & Linda, V. (2014). Privacy concerns associated with smartphone use. In *Journal of internet commerce.*

Jedrzejczyk, L., Price, B. A., Bandara, A. K., & Nuseibeh, B. (2010). On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. In *Proc. soups '10.*

Jorgensen, Z., Chen, J., Gates, C. S., Li, N., Proctor, R. W., & Yu, T. (2015). Dimensions of risk in mobile applications: A user study. In *Proc of codaspy '15.*

Jung, J., Han, S., & Wetherall, D. (2012). Short paper: enhancing mobile application permissions with runtime feedback and constraints. In *Proc. spsm'12* (pp. 45–50).

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). my data just goes everywhere: user mental models of the internet and implications for privacy and security. In *Proc of soups '15.*

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. In *Proc. fc'12.*

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proc. of chi'13.*

Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., & Hightower, J. (2009). Exploring privacy concerns about personal sensing. In *Proc. pervasive'09* (pp. 176–183).

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Preference-based location sharing: Are more privacy options really better? In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 2667–2676). New York, NY, USA: ACM. Retrieved from `http://doi.acm.org/10.1145/2470654.2481369` doi: 10.1145/2470654.2481369

Kraus, L., Wechsung, I., & Möller, S. (2014, jul). A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. In *Symposium on usable privacy and security (soups 2014) - workshop on privacy personas and segmentation (pps).* Retrieved from `http://cups.cs.cmu.edu/soups/2014/workshops/privacy/s2p4.pdf` (Online)

Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who wants to know what when? privacy preference determinants in ubiquitous computing. In *Chi '03.*

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., ... Cranor, L. F. (2013). What matters to users?: Factors that affect users' willingness to share information with online advertisers. In *Proc soups'13.*

Liccardi, I., Pato, J., & Weitzner, D. J. (2014). Improving mobile app selection through transparency and better permission analysis. *Journal of Privacy and Confidentiality*, *5*(2), 1–55.

Liccardi, I., Pato, J., Weitzner, D. J., Abelson, H., & De Roure, D. (2014). No technical understanding required: Helping users make informed choices about access to their personal data. In *Proceedings of the 11th international conference on mobile and ubiquitous systems: Computing, networking and services.*

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proc. of ubicomp'12.*

Liu, B., Andersen, M., Schaub, F., Almuhimedi, H., Zhang, S., Sadeh, N., ... Agarwal, Y. (2016). follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Proc of soups '16.*

Ludford, P. J., Priedhorsky, R., Reily, K., & Terveen, L. (2007). Capturing, sharing, and using local place information. In *Proc. of chi '07.*

McDaniel, P., & Enck, W. (2010, September). Not so great expectations: Why application markets haven't failed security. *IEEE Security and Privacy*, *8*, 76–78. Retrieved from `http://dx.doi.org/10.1109/MSP.2010.159` doi: http://dx.doi.org/10.1109/MSP.2010.159

Mehrotra, A., Pejovic, V., Vermeulen, J., Hendley, R., & Musolesi, M. (2016). My phone and me: Understanding people's receptivity to mobile notifications. In *Proc of chi '16.*

Olmstead, K., & Atkinson, M. (2015). *Apps permissions in the google play store* (Tech. Rep.). Pew Internet. Retrieved from `http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/`

Ongtang, M., Butler, K., & McDaniel, P. (2010). Porscha: policy oriented secure content handling in android. In *Proc. of acsac.*

Ongtang, M., McLaughlin, S., Enck, W., & McDaniel, P. (2009). Semantically rich application-centric security in android. In *Proc. of acsac.*

Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., & Lee, A. J. (2015). Interrupt now or inform later?: Comparing immediate and delayed privacy feedback. In *Proceedings of the 33rd annual acm conference on human factors in computing systems* (pp. 1415–1418). New York, NY, USA: ACM. Retrieved from `http://doi.acm.org/10.1145/2702123.2702165` doi: 10.1145/2702123.2702165

Patil, S., & Lai, J. (2005). Who gets to know what when: configuring privacy permissions in an awareness application. In *Proc. of CHI '05.*

Patil, S., Le Gall, Y., Lee, A. J., & Kapadia, A. (2012). My privacy policy: Exploring end-user specification of free-form location access rules. In *Proc. fc'12* (pp. 86–97). Retrieved from `http://dx.doi.org/10.1007/978-3-642-34638-5_8`

Quentin Jones and Sukeshini A. Grandhi. (2005). P3 Systems: Putting the Place Back into Social Networks. *IEEE Internet Computing*, *9*(5). (38-46)

Raja, F., Hawkey, K., Hsu, S., Wang, K.-L. C., & Beznosov, K. (2011). A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Proc. of soups '11.*

Research, P. (2014). *Cell phone and smartphone ownership demographics* (Tech. Rep.). Pew Internet. (`http://www.pewinternet.org/data-trend/mobile/cell-phone-and-smartphone-ownership-demographics/`)

Rosen, S., Qian, Z., & Mao, Z. M. (2013). AppProfiler: a flexible method of exposing privacy-related behavior in android applications to end users. In *Proc. of codaspy'13.*

Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2012). Android permissions: A perspective combining risks and benefits. In *Proceedings of the 17th acm symposium on access control models and technologies.*

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In *Proc of soups '15).*

Schlegel, R., Kapadia, A., & Lee, A. J. (2011). Eyeing your exposure: quantifying and controlling information sharing for improved privacy. In *Proc. of soups '11.*

Shabtai, A., Fledel, Y., & Elovici, Y. (2010). Securing android-powered mobile devices using selinux. *IEEE Security Privacy Magazine*, *8*(3), 36–44.

Shih, F., Liccardi, I., & Weitzner, D. (2015). Privacy tipping points in smartphones privacy preferences. In *Proc of chi '15.*

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proc of chi '14.*

Singer, N. (2013). Their apps track you. will congress track them? *The New York Times.* (http://www.nytimes.com/2013/01/06/technology/legislation-would-regulate-tracking-of-cellphone-users.html)

SMITH, A. (2013. Pew Internet, Tech. Rep., June). *Smartphone ownership 2013.* (http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx)

Stoll, J., Tashman, C. S., Edwards, W. K., & Spafford, K. (2008). Sesame: informing user security decisions with system visualization. In *Proc. of chi '08.*

Tam, J., Reeder, R. W., , & Schechter, S. (2010, May). *I'm allowing what? disclosing the authority applications demand of users as a condition of installation* (MSR-TR-2010-54). Microsoft Research.

Tan, J., Nguyen, K., Theodorides, M., Negrón-Arroyo, H., Thompson, C., Egelman, S., & Wagner, D. (2014). The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proc. of chi '14.*

Tang, K., Hong, J., & Siewiorek, D. (2012). The implications of offering more disclosure choices for social location sharing. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 391–394). New York, NY, USA: ACM. Retrieved from http://doi.acm.org/10.1145/2207676.2207730 doi: 10.1145/2207676.2207730

Tang, K. P., Lin, J., Hong, J. I., Siewiorek, D. P., & Sadeh, N. (2010). Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. In *Proc. of ubicomp '10.*

Tasse, D., Ankolekar, A., & Hailpern, J. (2016). Getting users' attention in web apps in likable, minimally annoying ways. In *Proc of chi '16.*

Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J., & Sadeh, N. (2009). Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proc. of chi '09.*

Unkown. (2014). Unique turker [Computer software manual]. (`http://uniqueturker.myleott.com/`)

Waddell, T. F., Auriemma, J. R., & Sundar, S. S. (2016). Make it simple, or force users to read?: Paraphrased design improves comprehension of end user license agreements. In *Proc of chi '16.*

Wash, R. (2010). Folk models of home computer security. In *Proc. of soups '10.*

Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., ... Wang, X. (2011). Privacy revelations for web and mobile apps. In *Proc. of hotos.*

Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., & Beznosov, K. (2015). Android permissions remystified: A field study on contextual integrity. In *24th usenix security symposium (usenix security 15).*

Zhang, B., Wu, M., Kang, H., Go, E., & Sundar, S. S. (2014). Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In *Proc of chi '14.*

Zhang, B., & Xu, H. (2016). Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. In *Proc of cscw '16.*

Zickuhr, K. (2012, May). *Three-quarters of smartphone owners use location-based services.* Retrieved from `http://www.pewinternet.org/Reports/2012/Location-based-services.aspx?src=prc-headline`

Zickuhr, K. (2013). *Location-based services* (Tech. Rep.). Pew Internet. (`http://pewinternet.org/Reports/2013/Location.aspx`)

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). Did you ever have to make up your mind? what notes users do when faced with a security decision. In *Proc. of acsac '02.*