# A Field Study of Run-Time Location Access Disclosures on Android Smartphones

Huiqing Fu, Yulong Yang, Nileema Shingte, Janne Lindqvist†, Marco Gruteser
Rutgers University
Email: {huiqing,yulong,janne,gruteser}@winlab.rutgers.edu nileema.shingte@gmail.com
†Corresponding author: contact at janne@winlab.rutgers.edu

***Abstract*—Smartphone users are increasingly using apps that can access their location. Often these accesses can be without users knowledge and consent. For example, recent research has shown that installation-time capability disclosures are ineffective in informing people about their apps' location access. In this paper, we present a four-week field study (N=22) on run-time location access disclosures. Towards this end, we implemented a novel method to disclose location accesses by location-enabled apps on participants' smartphones. In particular, the method did not need any changes to participants' phones beyond installing our study app. We randomly divided our participants to two groups: a Disclosure group (N=13), who received our disclosures and a No Disclosure group (N=9) who received no disclosures from us. Our results confirm that the Android platform's location access disclosure method does not inform participants effectively. Almost all participants pointed out that their location was accessed by several apps they would have not expected to access their location. Further, several apps accessed their location more frequently than they expected. We conclude that our participants appreciated the transparency brought by our run-time disclosures and that because of the disclosures most of them had taken actions to manage their apps' location access.**

## I. Introduction

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 [1], [2] has shown, there are considerable security and privacy risks with these apps.

Location privacy risks are of particular interest since 74% smartphone users use location-based services [3]. 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 [4]. In another survey, more than 70% of participants desired to know about location data collection by apps on mobile devices [5].


USEC '14, 23 February 2014, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2014.23044

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 [6], [7], [8]. The approach used by iPhone has so far been studied only with an Amazon Mechanical Turk survey [9]. 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 [10] 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 paper 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 five major findings in this paper.

> 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.


Fig. 1: One version of the existing Android location access disclosure (Google Nexus 4 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.

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.

## II. Background and Related Work

In this section, we discuss the relevant background pertaining to current Android location access disclosures and related work.

**Default Android Location Access Disclosure.** The current run-time location access disclosure is depicted in Figure 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. *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 [9]. The notification is shown only once when the first time the apps request to access location.

**Related Work.** There has been considerable interest in mobile security and privacy recently. Becher et al. [11] give an overview of mobile phone security history and developments. Chin et al. [12] studied users' confidence in smartphone security and privacy. Researchers have shown that users generally do not pay attention to or even understand the meaning of "permission" or "disclosure" at installation time [6], [7], [8], [13]. Our present study confirms this since participants were not expecting location accesses by several apps.

A lot of focus on revealing sensor data to users has been in the domain of social location-sharing studies. However, the studies have focused on the implications of exposure and utility to share location and other data with family, friends and colleagues. Schlegel et al. [14] used pairs of growing eyes to represent different groups who query users' location. 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. [15] 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. [16] 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 location accessed by the apps participants used. Hsieh et al. [17] 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. In contrast to our work, the above projects have focused on studying social location sharing with one selected app. In particular, the participants were asked to use the apps for social sharing. 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.

Researchers have also studied disclosures with WiFi and desktop sensor accesses. Consolvo et al. [18] implemented 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. [19] 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. [13] 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 a majority of participants preferred disclosures using images or icons.

There are several proposals to enhance Android users' understanding of privacy issues. Kelley et al. [8] 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 the help of checklist. Rosen et al. [20] 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. [21] 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. Recently, Jung et al. [22] and Balebako et al. [10] 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 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.

## III. Run-Time Location Access Disclosures

In this section, we present our approach for run-time location access disclosures. We first discuss a heuristic method for discovering location accesses that allowed us to implement our approach as a normal app. We proceed to present the intervention and user interface design.

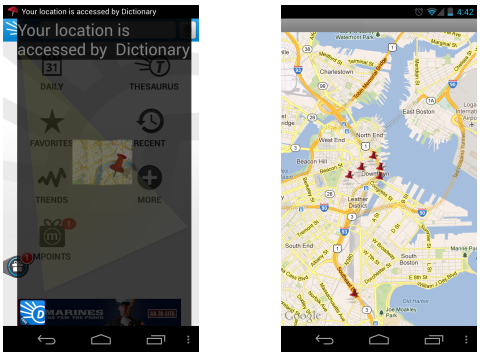
We sought to study how our location disclosures would work during people's daily lives with their own Android devices. We initially evaluated the possibility to use e.g. Taintdroid [23] as a basis to carry out the field study. Unfortunately, Taintdroid requires rooting of the phone. Rooting a phone would 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 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 [2].

### A. Heuristic Discovery of Location Access

As it turns out, there is no obvious way for a normal Android app to monitor whether other apps are accessing location. However, we discovered we could exploit the method *getLastKnownLocation* available in the Android Location API for this purpose as an effective side channel. 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;




(a) (b)

Fig. 2: (a) 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 [appname]." 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. (b) 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.

- The most likely app requesting the location is the "foreground app" (the app the user is actively using).

Our study app has two services running in the background: a main service and an uploading data service. The main service is for collecting data of participants' phone usage. This service gets the foreground applications' information, detects location change events and creates notifications to users as described below. The uploading data service is used to upload collected data to our servers using encrypted channel with Transport Layer Security (TLS).

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.

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 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.

### B. Intervention and User Interface Design

The main features most often seen by participants are two location access disclosures: 1) a notification on the screen

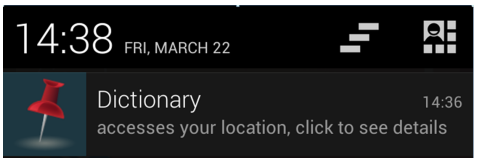



Fig. 3: Example of the location access disclosure implemented to the Android notice bar. Location access disclosure appeared in the Android Notifications List, which is expanded by pulling the Notification Bar downwards.

*"Your location is being accessed by [appname]."* as shown in Figure 2a and 2) a notification in the Android notice bar as shown in Figure 3. As triggered by the above discussed process, the two notifications were shown at the same time to participants. Figure 2a 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 2b, "map of locations accessed by all apps" and "list of apps that accessed location."

It is obvious that there should be limits to how often the notification is shown to participants. 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 keeps changing to different applications, we only used a one minute delay between the notifications.

The main user-controllable screen of the app consists of only five different options. First, the user has the option to have the app to *"Show location access history per application."* Pressing that option, the users will be presented a *"List of apps that accessed location."* 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.

## IV. Method

In this section, we describe our method: participants, experiment design and procedure.

### A. Participants

We recruited participants by several methods. We posted flyers on campus and published online advertisements in the local Craigslist and a student mailing list. We carried out recruitment in person at our university campus center. We advertised that we were conducting user studies 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. Participants were screened by the entry survey answers: they were qualified if they used location based apps in daily lives.

We made appointments with 25 persons who were qualified for our study. We assigned randomly with a coin toss all participants 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 (we denote them with P1-13) and 9 participants in the No Disclosure group (we denote them with 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 participants were undergraduate students, one participant self-identified as an administrative support person, and one participant was a teacher. In the No Disclosure group, eight participants were male and one participant was female; five participants were of age 18-25 and four participants 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.

### B. 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 phones, (3) ran the app for about four weeks, and (4) participated in an exit interview and debriefing. 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 described above.

### C. Procedure

We recruited participants from Android users. The participants were asked to install an application we had implemented and discussed in Section III. They were told that the application 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).

**No Disclosure Group.** For the No Disclosure group, the installed app did not have any user interface or user interaction available. It just collected the data over the time the participants participated in the study. As discussed in Section II, Android phones show a GPS icon flashing when apps are trying to use GPS localization.

After one week of data collection, the No Disclosure group participants were contacted to see if they had any problems with the study app. At the same time, the participants were asked to read a recent article [24] from The New York Times about location-based apps tracking mobile phone users. We wanted to see if 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.

**Disclosure Group.** For the Disclosure group, the app behaved as discussed above in Section III. However, to establish a baseline of participants' behavior before the designed interventions, the app's user interface activated only after the participant had been participating for seven days. The app also collected data on how people interacted with the user interface, e.g. what buttons they pressed, when they disabled any features and how long they viewed any particular screen.

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 also do not usually come with instructions of all of their features.

## V. Results

In this section, we will first describe the data we collected from our participants' phones. We used these records to understand some reasons for participants' reactions and attitudes in the study. We will report the participants' reactions in the No Disclosure group and the Disclosure group separately below.

### A. 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 feature of the study app they used. 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. Additionally, 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).

### B. No Disclosure Group

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 [24] 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.

**Android's Location Access Disclosure Method is not Effective.** The next question we were interested in was whether the Android's default location access disclosure method depicted in Figure 1 was effective. In the remainder of the paper we will refer to this disclosure method as the GPS icon. In our study, 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 despite the flashing GPS icon. Participants could not manage their apps' location usage because they were not sure which apps could access their location 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."*

**Unexpected Location Accesses.** At the end of the exit interview, the No Disclosure group 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. All participants except one (C7) marked several apps as shown in Table I. Participant C7 did not have records of any apps accessed location during the study.

Participants were then asked to describe their feelings and attitudes about 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."*

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

**Reactions to Unexpected Location Accesses.** We asked participants what actions if any they would take after seeing apps unexpectedly access location. According to their answers, we divided participants into three groups. The first group (C2,C3) expressed the willingness to take actions to protect their location data. Participant C2 might uninstall an app called S Voice (an app for recording audio). He did not understand why the app accessed location and he could find a replacement for the app. Participant C3 would keep Internet turned off longer than otherwise. The second group (C4,C6,C8) thought they had tried their best to protect their location privacy and it was hard to think of more steps to take. Participant C4 thought that he had already protected his location data as much as possible. He usually kept GPS turned off and data plan closed most of the time. Participant C8 uninstalled many location based apps before the study. He chose to manually enter location instead of letting apps automatically access location. The participants in the second group strongly expressed the idea that they did not like being tracked. They did not like others to know where they were. The third group (C1,C5,C9) did not express willingness to take actions. Participant C5 said, *"I do not see any actual harm it(app he did not expect to access location) can do. I actually for most of the apps I checked the setup page. I liked to see the settings for most of the apps."* Participant C9 just said *"[I] cannot do anything."* Participants in the third group showed the willingness to take advantage of the apps on phones. They tended to put more value on the functions apps performed than protecting location privacy.

### C. Disclosure Group

As discussed before, the 13 participants in the Disclosure group received disclosure notifications when apps were accessing their location. They would receive run-time disclosures via several features including notifications on the screen (Figure 2a) and notifications in notice bar (Figure 3). 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 2a). 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 4. The maximum was 851 times, and the minimum was none (P3).

We will next describe several experiences by the Disclosure group participants. These include unexpected location accesses by apps, taking action by uninstalling apps, other actions taken to manage apps which were unexpected to access location, and participants attitudes towards the study app's run-time disclosures.

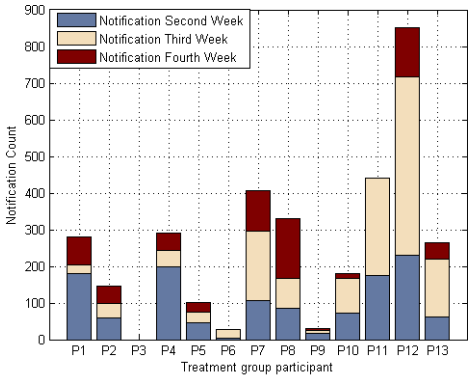



Fig. 4: How many times each participant in the Disclosure group received a notification that their location is being accessed divided to second, third, and fourth week of participation. (Recall, we would start the notifications after first week of participation, and the Notification Bar based notification could not be disabled.)

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

**Unexpected Location Accesses.** In the exit interview, most participants 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 II. Only participant P3 did not mark any apps, because he only used Google Maps and Browser apps.

**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 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.

**Attitudes and Suggestions To Run-Time Location Access Disclosures.** As discussed above, we implemented several kinds of location access disclosures. We report 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 5. 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). 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 on the third day after started receiving the notifications.

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

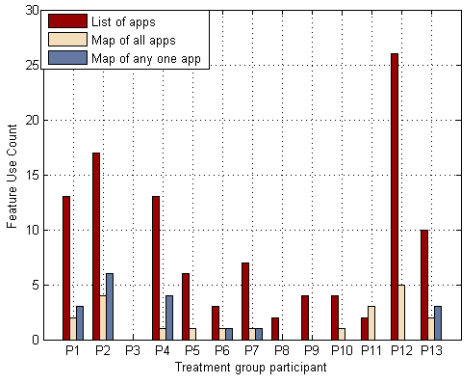



Fig. 5: How many times each participant in the Disclosure group used some of the major features of the study app: the listing of all apps that accessed the participant's location, the map of any one app listed to be accessing locations, and the map of all location accesses by all apps.

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 once in a while. 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 4). 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.

### *D. Comparison between Participant Groups*

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

| 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 [24]; | (1) uninstall apps; (2) replace apps; (3) stop using some apps; (4) search through setup to disable the app's location |

TABLE III: Different Major Findings in Two Groups

comparison, existing location access disclosures on Android were not adequate.

**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 its gonna take something, but you don't realize how often 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.

**Common Findings: Tradeoffs with Privacy and Utility in the Two Groups.** In both 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."*

## VI. Discussion and Conclusions

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. 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 [6], [7], [8] 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 flashing GPS icon was not efficient might be that it did not tell users explicit information such as 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 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 [9] 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 to 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 learnt most 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 [9] has shown that several users have used this feature on the iOS platform to disable location access for some of their apps.

**Limitations and Further Work.** 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 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. Thus, further work is required for generalizing the results for different populations. We plan to launch the app in the Google Play app market for further studies. We focused on the Android platform due to practical implementation reasons, thus, similar studies for other platforms would be useful for further work.

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 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 apps participants used. We verified that the findings and conclusions of our paper were not affected by any apps accessing location in the background.

**Conclusions.** 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 [5] 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.

## ACKNOWLEDGMENTS

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.

## REFERENCES


[1] D. Barrera and P. Van Oorschot, "Secure software installation on smartphones," *IEEE Security and Privacy*, vol. 9, pp. 42–48, May 2011. [Online]. Available: http://dx.doi.org/10.1109/MSP.2010.202

[2] E. Chin, A. P. Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in android," in *Proc. of MobiSys'11*, 2011.

[3] K. Zickuhr, "Three-quarters of smartphone owners use location-based services," May 2012. [Online]. Available: http://www.pewinternet.org/Reports/2012/Location-based-services.aspx?src=prc-headline

[4] J. L. Boyles, A. Smith, and M. Madden, "Privacy and data management on mobile devices," Pew Internet, Tech. Rep., 2012. [Online]. Available: http://pewinternet.org/Reports/2012/Mobile-Privacy/Key-Findings.aspx

[5] R. Balebako, R. Shay, and L. F. Cranor, "Is your inseam a biometric? evaluating the understandability of mobile privacy notice categories," CMU, Tech. Rep. CMU-CyLab-13-011, 2013.

[6] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proc. of SOUPS'12*, 2012.

[7] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: installing applications on an android smartphone," in *Proc. of USEC'12*, 2012.

[8] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proc. of CHI'13*, 2013.

[9] D. Fisher, L. Dorner, and D. Wagner, "Short paper: location privacy: user behavior in the field," in *Proc. of SPSM'12*, 2012.

[10] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, ""Little brothers watching you": raising awareness of data leaks on smartphones," in *Proc. of SOUPS'13*, 2013.

[11] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices," in *Proc of SP '11*, 2011.

[12] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proc. of SOUPS'12*, 2012.

[13] J. Tam, R. W. Reeder, and S. Schechter, "I'm allowing what? disclosing the authority applications demand of users as a condition of installation," Microsoft Research, MSR-TR-2010-54, May 2010.

[14] R. Schlegel, A. Kapadia, and A. J. Lee, "Eyeing your exposure: quantifying and controlling information sharing for improved privacy," in *Proc. of SOUPS '11*, 2011.

[15] L. Jedrzejczyk, B. A. Price, A. K. Bandara, and B. Nuseibeh, "On the impact of real-time feedback on users' behaviour in mobile location-sharing applications," in *Proc. SOUPS '10*, 2010.

[16] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh, "Who's viewed you?: the impact of feedback in a mobile location-sharing application," in *Proc. of CHI '09*, 2009.

[17] G. Hsieh, K. P. Tang, W. Y. Low, and J. I. Hong, "Field deployment of imbuddy: a study of privacy control and feedback mechanisms for contextual im," in *Proc. of UbiComp'07*, 2007.

[18] S. Consolvo, J. Jung, B. Greenstein, P. Powledge, G. Maganis, and D. Avrahami, "The wi-fi privacy ticker: improving awareness & control of personal information exposure on wi-fi," in *Proc. of Ubicomp '10*, 2010.

[19] J. Howell and S. Schechter, "What you see is what they get: Protecting users from unwanted use of microphones, cameras, and other sensors," in *Proc. of W2SP*, 2010.

[20] S. Rosen, Z. Qian, and Z. M. Mao, "AppProfiler: a flexible method of exposing privacy-related behavior in android applications to end users," in *Proc. of CODASPY'13*, 2013.

[21] J. Lin, N. Sadeh, S. Amini, J. Lindqvist, J. I. Hong, and J. Zhang, "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," in *Proc. of UbiComp'12*, 2012.

[22] J. Jung, S. Han, and D. Wetherall, "Short paper: enhancing mobile application permissions with runtime feedback and constraints," in *Proc. SPSM'12*, 2012.

[23] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," in *Proceedings of OSDI*, 2010.

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