General Area or Approximate Location? How People Understand Location Permissions

Huiqing Fu and Janne Lindqvist
Rutgers University

ABSTRACT

More than half of American adults use smartphones and about two thirds of them use location-based services. On Android smartphones, these location-based services are implemented by apps. Android phones provide two location-related permissions: "precise" location and "approximate" location. In this paper, we present an online survey of 106 Android users to investigate how people understand location descriptions related to their apps. Our results suggest that most participants considered the "precise" location to mean their exact location and the "approximate" location as a general area. This mental model of the "approximate" location seems to allay people's privacy concerns related to their apps. However, after participants were shown the ground truth of how accurate "approximate" location actually is, twice as many participants no longer thought "approximate" location offered enough protection, compared to before showing the ground truth. Our results indicate that the location permissions might mislead smartphone users about the privacy protections the apps are providing.

Categories and Subject Descriptors

H.5.m [**Information Interfaces and Presentation**]: Miscellaneous; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; K.4.1 [**Computers and Society**]: Public Policy Issues—Privacy

Keywords

Android; Location Permissions; Mental Models; Privacy

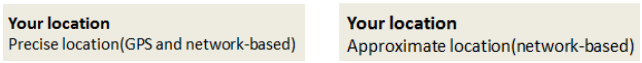
1. INTRODUCTION AND RELATED WORK

According to Pew Research, 56% American adults use smartphones [7] and 74% of these users have used location-based services [8]. These location-based services, implemented as apps, can have unprecedented third-party access to the locations of their users.

There has been several studies related to privacy of smartphone users. Generally, a survey by Balebako et al. indicated that smartphone users were concerned about how their apps' accessed their location [1]. In a lab study by Felt et al. at least one participant decided not to install an app due to "exact location" permission [2]. In a field study by Fu et al. some participants uninstalled apps after they became aware that some apps were accessing their location [3].

WPES'14, November 3, 2014, Scottsdale, AZ, USA.

ACM 978-1-4503-3148-7/14/11 ...$15.00.
http://dx.doi.org/10.1145/2665943.2665957.



(a) (b)

Figure 1: Screenshots of Android smartphone platform's two different location permissions requests. These requests are shown at the same time than all other permissions requests the app might be enabled for. (a) Shows the "precise" location permission, which enables apps to localize the phone with both GPS and network-based (WiFi and cell-tower) methods. (b) 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.

Android users do not clearly understand the apps' installation-time permissions. A study by Felt et al. [2] showed that only 3% of their participants could correctly understand the permissions. Kelley et al. [4] 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 zipcode and town or city information [5].

In this paper, 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 1. 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 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.

2. METHOD

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

2.1 Participants

The online survey was conducted on Amazon Mechanical Turk. We recruited 106 participants. According to their responses, 54.7% were female and 45.3% were male. The participants' age ranged from 19 to 61 and the mean age was 33 with standard deviation 8.8. All 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 HIT Approval Rate greater than or equal to 95%. Unique Turk [6] was also used in the MTurk HIT's html file to exclude duplicated worker IDs.

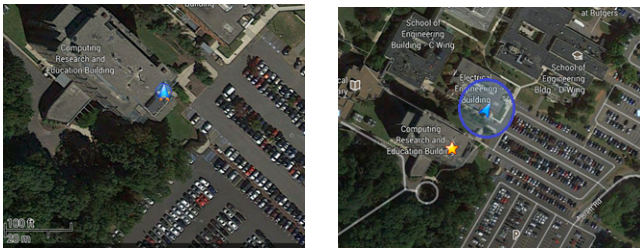
2.2 Online Survey Design

The study was approved by the Rutgers University IRB. The survey was set 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 1a and Figure 1b) were shown to participants before the corresponding questions. 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 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 2a, Figure 2b and Figure 3). 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 2a: The correct answer is "GPS location". Its accuracy is about 9.8 feet / 3 meters to 32.8 feet / 10 meters. Figure 2b: 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 3: 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). After this, the identical 7-point Likert scale question mentioned above about their attitudes toward location privacy was shown again to participants.



(a) (b)

Figure 2: Screenshots of (a) GPS and (b) 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. In (a) The map's scale is 100ft / 20m, and in (b) the map's scale is 200ft / 50m.

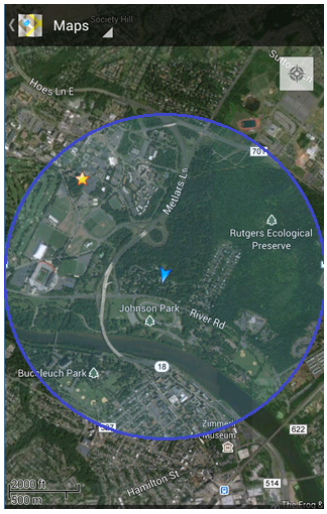


Figure 3: Screenshot of cellular network-based localization on an Android smartphone using Google Maps. The map's scale is 2000ft / 500m.

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.

3. RESULTS

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 participants knew the approximate location were updated by 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 how to formulate their responses. As a result, some respondents referred to specific technologies while some explained using 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 1: Breakdown of participants' understandings of the accuracy of network-based location and GPS location. The percentage of results is highlighted by *italic* and red color which fell in the given answers of accuracy of GPS location and network-based location.

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 2: Breakdown of the responses in the location accuracy on screenshot of Maps. The correct answers are marked using the *italic* and red color.

The quantitative results were consistent with the qualitative findings above. Table 1 shows that most respondents supposed the GPS location was very accurate. More than 90% respondents thought 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 were no 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 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 2 shows the results: 90.6% selected the correct answers for cellular location and 83.0% for GPS location. The screenshot of WiFi location (see Figure 2b) 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".

A majority of respondents stated that the approximate location helped to protect their location privacy as shown in Figure 4 and Table 3. 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 was still more than half (57.55%) respondents who believed that the approximate location could protect location privacy as Table 3 shows. A total 72.64% of responses (see Table 4) shared the same popular reason that general area was better for location privacy compared to exact location.

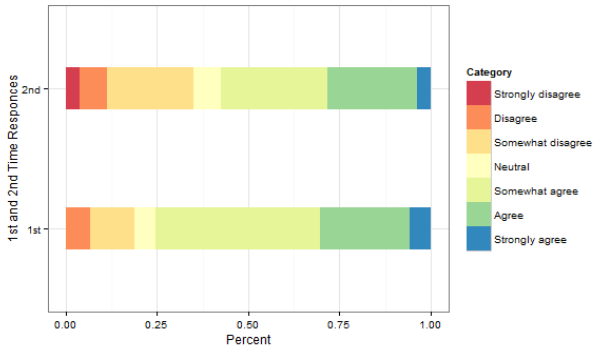


Figure 4: Breakdown of "approximate location helps to protect location privacy" responses prior to showing the ground truth (1st) and after showing the ground truth (2nd). The participants responses were limited to a 7-point Likert scale.

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

Table 3: The above 7-point Likert scale was collapsed here into 3-point scale: agree, disagree or neutral. Similarly, "first time percentage" indicate answers prior to 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: Reasons respondents explained why approximate location could protect location privacy.

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.

Figure 4 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 5) shared that if the approximate location's accuracy was too close to exact location it was not good for location privacy. The common reasons resembled what participant P17 said *"The Approximate location was very accurate and*

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

close enough that there does not leave much room for guessing where the phone was located."

After respondents' saw the ground truth in the survey, the percentage of respondents who thought that the approximate location could not protect location privacy doubled from 18.87% to 34.91% as shown in Table 3. 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 1 shows that only 28.30% of responses fell in the given answers about the network-based location's accuracy and 79.25% of responses were equal or more than 1 mi – 2 mi / 1.6km – 3.2 km which was more approximate than the given answers in distance range.

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 suggest that participants were likely to think approximate location protects their privacy if they assumed that the localization accuracy was low. These quantitative results were consistent with the qualitative analysis above.

4. DISCUSSION AND CONCLUSIONS

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

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 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 obfuscates 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.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant Number 1223977. 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.

5. REFERENCES

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

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

[3] H. Fu, Y. Yang, N. Shingte, J. Lindqvist, and M. Gruteser. A field study of run-time location access disclosures on Android smartphones. In *Proc. USEC'14*, 2014.

[4] 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. USEC'12*, 2012.

[5] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor. What matters to users? factors that affect users' willingness to share information with online advertisers. In *Proc. SOUPS'13*, 2013.

[6] M. Ott. Unique turker. `http://uniqueturker.myleott.com`.

[7] A. SMITH. Smartphone ownership 2013, June 2013. Pew Internet, Tech. Rep. `http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx`.

[8] K. Zickuhr. Location-based services. Technical report, Pew Internet, 2013. `http://pewinternet.org/Reports/2013/Location.aspx`.