University of Groningen

Bachelor thesis

Studying the decoy effect in the Android location permission prompt

Supervisor:
F.F.M.Mohsen, PhD
Second supervisor:
F.Turkmen, PhD

Authors:
Xiaoyu Guan *(s3542807)*

March 17, 2022

Abstract

The Decoy effect is widely used by companies to nudge their customers to choose the product that companies want customers to choose most. Nowadays, with the development of technology people's private data becomes easier and easier to expose to others. Thus, we are interested if it's possible to prevent this issue by implementing the decoy effect when people need to make decisions for their data. According to our research, we found a study that focuses on setting passwords aspect and they mentioned a direction in-app permission that has not been investigated, which gives us the inspiration of this research.

The modern operating system companies are also paying more attention to protecting their users' privacy, such as Android, they have worked on adding or modifying the third option in permission prompts to secure users' data. Therefore, we propose to study if the current permission prompts have already implemented the decoy effect to nudge users to choose the better permission. In addition, we want to understand users' mental activity when they are giving permission(s) to an app by sending a survey to participants.

Contents

1 Introduction & motivation

The start point of this research is to investigate the decoy effect in the information privacy field because there is only one direction that has been investigated in detail. However there are more aspects are mentioned in the paper such as privacy settings, application permissions, etc [11].

Information privacy becomes more and more important because there are a huge amount of users who are using social media to share their life and this action puts them in a dangerous position. This paper points out five possible security issues(Security risks, Identity Theft, Phishing, Profiling Risk, and Fake Product Sale) caused by users do not treat their personal information properly[8].

We propose to conduct a study to expand the current research to the area of application permissions that they mentioned in their study. According to our research, the current mobile operating system such as Android has already worked on adding more options(Android 10) or modifying the current options(Android 11) in permission prompts, but we're not clear if they employ the decoy effect. Therefore, in this research, we are going to build two apps to test our uncertainty, one for Android 10 and the other for Android 11.

For doing this research, we start by reviewing the literature and then is the description of our methodologies such as the hypothesis we made in this research, how we find our participants, the architecture of our apps, and more details of construct this study. Finally, we will show the results of this research and our conclusion.

After this research, we are expecting to figure out if the android system especially in Android 10 and Android 11 has already used the decoy effect when they are crafting the permission prompt. In addition, we hope to understand users' thoughts when they are giving their permission to the app as well.

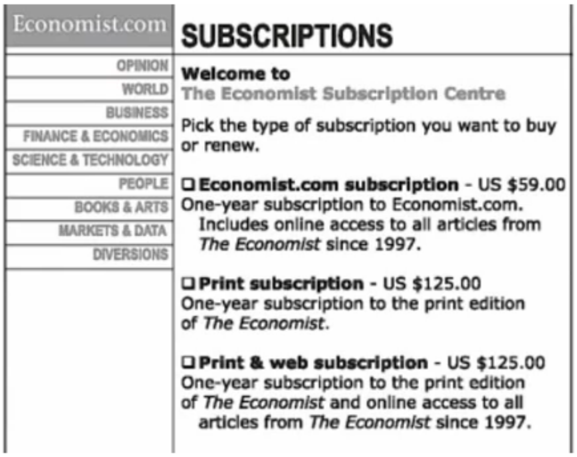
2 State of the Art

2.1 Decoy Effect

The decoy effect is a widely used strategy in the marketing world that is defined as when people are faced with a third alternative(”decoy option”) that is asymmetrically dominant, they will tend to have a particular shift in preference between two options(”target option” and ”competitor option”), where ”decoy option” means it’s significantly worse than one choice(”target option”), but only slightly worse than the others(”competitor option”).

2.1.1 Experiment of decoy effect in marketing

As the explanation of professor Ariely’s experiment, added ”decoy option” print subscription in the advertisement, and the result is the number of people who chose print & web subscription increased 52 percent than without the ”decoy” option [12]. The advertisement used by professor Ariely is shown in Figure 1.



SUBSCRIPTIONS

Welcome to
The Economist Subscription Centre

Pick the type of subscription you want to buy or renew.

□ **Economist.com subscription** - US $59.00
One-year subscription to Economist.com.
Includes online access to all articles from *The Economist* since 1997.

□ **Print subscription** - US $125.00
One-year subscription to the print edition of *The Economist*.

□ **Print & web subscription** - US $125.00
One-year subscription to the print edition of *The Economist* and online access to all articles from *The Economist* since 1997.

Figure 1: The advertisement professor Ariely’s used [12]

2.2 Decoy Effect in information privacy

2.2.1 Decoy effect as dark pattern

Dark patterns are defined as a user interface strategy that is commonly used in websites and applications to lead the users to do the things that users did not intend to do [2]. According to Celia's argument, the use of the decoy effect can be seen as an example of a dark pattern because companies can make extra profit by applying the decoy effect to nudge users to spend more money on their products than users plan to pay at the first place that the benefits for companies are more than the users [6]. As we can see from the definition of the dark patterns and professor Ariely's experiment, the beneficiaries are always the companies and the users are the victims. However, research made by Tobias shows the different side, the study is based on the fact that the decoy effect can affect people's choices that the group with the "decoy option" is more likely to choose the target option, where the target option is the passphrase that is considered as the strongest in all three options they provided[11]. This proves that both website companies and users can get benefits because first users can protect their data by setting a strong password. Secondly, the website company can gain the trust from users that can attract more users to use their website because the social reputation is the most effective factor to make users trust a web[10]. In Tobias' study, they also point out there is future study space for studying the decoy effect in application permissions[11]. In this research, we are going to stick in this direction.

2.3 Exist permission options

2.3.1 The problem of application permissions requests

As Android indicates in their developer page[4], application permissions are used to protect users' privacy by restricting the amount of sensitive data that applications can access. Additionally, Android also points out that depending on the sensitivity of desired data there are two types of permission Install-time permissions and Runtime permissions, where Install-time permissions are declared in the app store when users download the application and once the users download it successfully those permissions will be given by default and Runtime permissions are permissions that when users are asked to perform the tasks that need to use more sensitive data than Install-time permissions[4]. Such that we are interested in Runtime permissions.

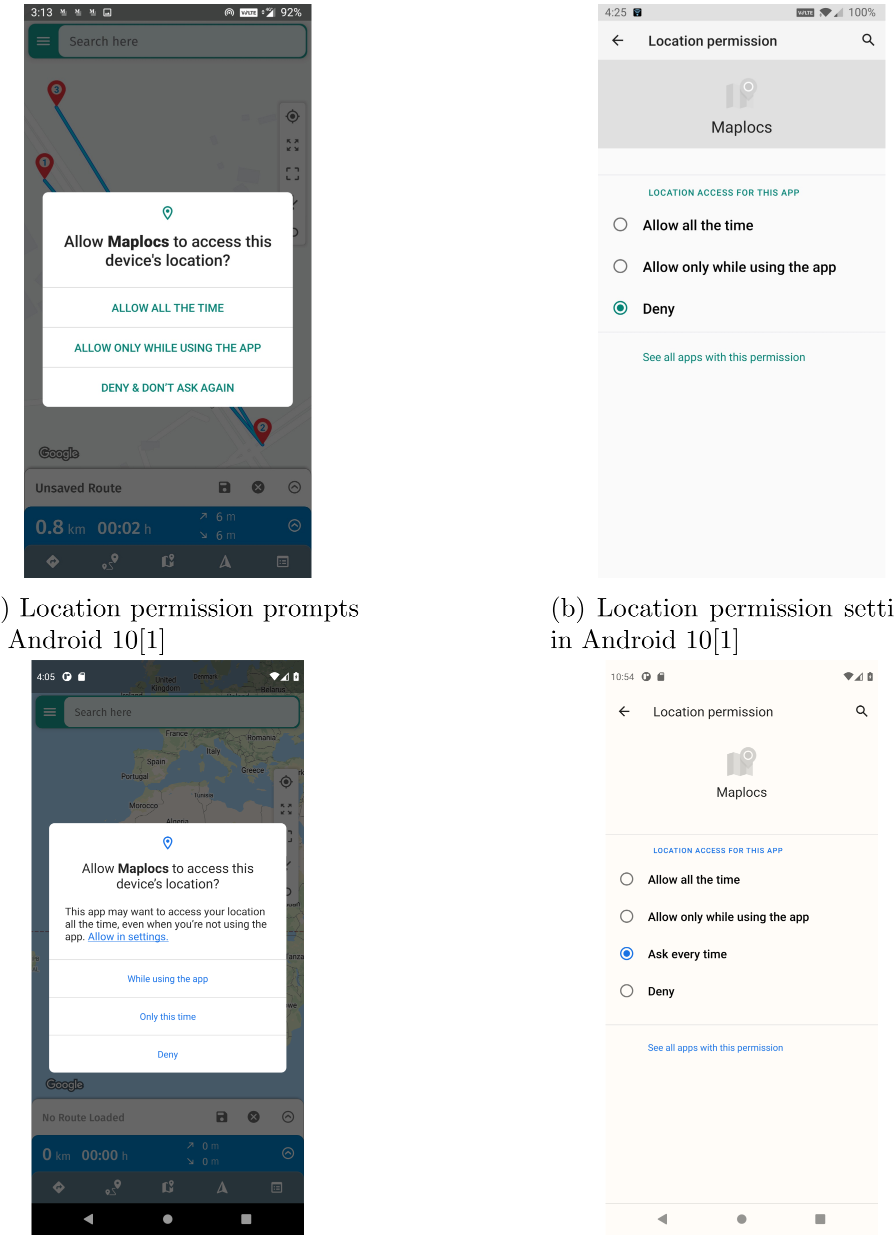
Nowadays, there are around 54.1% of applications from the Google Play Store over ask the permissions, which can cause unnecessary privacy problems[7]. There is a possible reason is found that since the permission prompts are lacking attention as the permission window is designed by OS that

UX(user experience) designers do not need to pay too much attention to it[9]. In our research, we are going to study about the current Location permission prompt in Android that is asked the most frequently.

2.3.2 Location permission prompt and decoy effect

From Android 11 and it's higher version operating system there are updates in their location permission prompt. One of the changes is that replaces the prompt option "Allow all the time" in Android 10 with "Only this time" in Android 11, where "Only this time" stands for one-time permission. Such that the "Allow all the time" will only be shown if the user chooses "While using the app" at first [3].

The advantages of the changes are users can have more flexibility to control their data and can be well informed about the usage of their data as the "Always Allow" will not appear in the default prompt that applications need to give proper reason to convince users to give their background permission [3]. Therefore, we are curious if the decoy effect exists in the location permission prompt of Android 10 and Android 11 because they fit the definition of decoy effect, which is three options, and one asymmetrical option occurs in all three options. Additionally, this update can influence location-based marketing as it can increase the difficulty for application developers to ask users for accessing their location data at any time to apply geofences technology[5].



Allow **Maplocs** to access this device's location?

ALLOW ALL THE TIME

ALLOW ONLY WHILE USING THE APP

DENY & DON'T ASK AGAIN

(a) Location permission prompts in Android 10[1]

Location permission

Maplocs

LOCATION ACCESS FOR THIS APP

○ Allow all the time

○ Allow only while using the app

● Deny

See all apps with this permission

(b) Location permission settings in Android 10[1]

Allow **Maplocs** to access this device's location?

This app may want to access your location all the time, even when you're not using the app. Allow in settings.

While using the app

Only this time

Deny

(c) Location permission prompts in Android 11 [1]

Location permission

Maplocs

LOCATION ACCESS FOR THIS APP

○ Allow all the time

○ Allow only while using the app

● Ask every time

○ Deny

See all apps with this permission

(d) Location permission settings in Android 11 [1]

Figure 2: Comparison of Android 10 and Android 11 in location permission

2.4 Literature search

The references are found by interests keyword searing such as "dark patterns", "UX design","decoy effect", "information privacy", "application permissions", "application privacy", "decoy effect in the information privacy", "personal data privacy", "location permission", "mobile user" and etc. When we searching for the relevant researches search engines SmartCat, Google and Google scholar are used as our main search engines.

3 Methodology

Based on the previous research, we are going to investigate if the decoy effect has already been implemented on the location permission prompt in Android 10 and Android 11.

This leads to the following research questions:

- What is the most common option that users of Android 10 and Android 11 choose when they are asked to permit their devices?
- Why do mobile users think the choice they make was a good choice?
- If the decoy effect has already existed in the permission prompts of the Android system.

The following items are our expected contributions after implementing methods:

- Have an overview of which permission option is the most given by mobile users when they open an app for the first time
- Understand why mobile users make those permission choices
- Find out if the decoy effect has already existed in the permission prompts of the Android system.

3.1 Hypothesis

Android 10

We identify the option based on the functionality that a use can access.

- Competitor & Target option: We chose ”Deny” as competitor because we believe the reason for asking permission is to get permission to access users sensitive data that there are simply two options, ”Allow” or ”Deny”. When a user chooses ”Deny” then he/she cannot get the full experience of an app, but if he/she choose ”Allow all the time” then he/she all the functionality of that app can work properly that's the reason why we chose ”Allow all the time” as target option.

- Decoy option: According to the concept of decoy option, ”Allow only while using the app” is a much better option than ”Deny”, but it's slightly worse than ”Always allow” because it can make part of an app's functionality works properly.

Android 11

- Competitor option & Target option : We chose ”Deny” as competitor and ”While using the app” as target. The reason is same as for the Android 10

- Decoy option:We chose ”Only this time” as decoy option because even if this option can let a user access same amount of functionalities, but it's only for a short period of time.

Therefore, we have following hypothesis:

- $H1$: If the decoy option is implemented in the location permission prompts for Android 10, then the majority of users should choose ”Always allow”($prop\_a$).

- H_2: If the decoy option is implemented in the location permission prompts for Android 11, then the majority of users should choose ”While using the app”($prop\_b$).

prop_a: Proportion of users who choose ”Allow all the time” in Android 10's location permission prompt.

prop_b: Proportion of users who choose ”While using the app” in Android 11's location permission prompt.

3.2 Participants

We found 61 participants to join this research, 31 participants for Android 10 and 30 participants for Android 11. We asked each participant to join our research by first sending a short instruction about our study, it's good to mention we did not tell them the real purpose of this research in the first place because we do not want the participants to have any bias when they are making location permission decision. And then the participants can access our app through the link of the emulator in the instruction that the survey link will show in the emulator based on the location permission decision they make.

In this study, we do not ask the specific age of our participants instead we ask their generation for example, under 20, 20-39, 40-59, and over 60.

The difficulty of finding participants is the current online emulators has to buy their membership to get the unlimited access time and run multiple tasks at the same time, which causes the problem that we have to contact our participants one by one.

3.3 Design of apps and online surveys

We built two apps for this study because we want to find out if the decoy effect has already been deployed in Android 10 and Android 11.

Architecture of app for Android 10:

As shown in Figure 3, when a user clicks the link of the emulator, he/she will see the location permission prompt pop up to ask for his/her location permission, and then the user can give their choice such as "Allow all the time", "Allow only while using the app" and "Deny". After he/she makes the decision, the user's choice will be recorded into our database with a unique id that is generated by our app, and then our app will show the different survey links to the user based on the option they clicked in the permission prompt. The participants' id filed is pre-filled by us as well. The screenshot can be found in Figure 4.

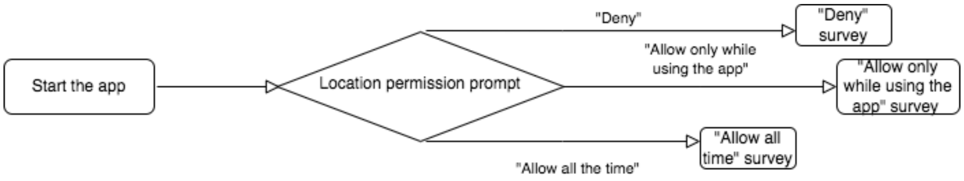
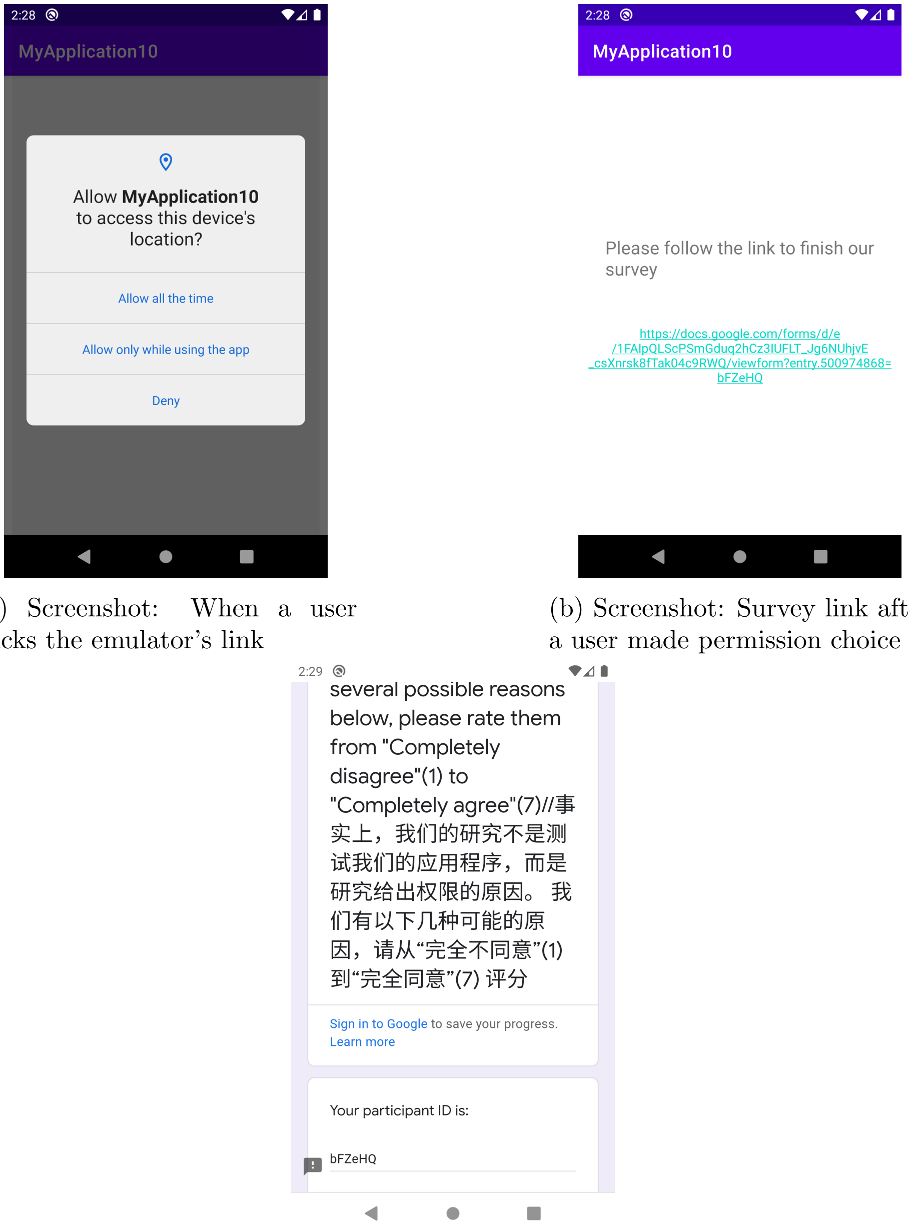

Start the app
Location permission prompt
"Deny"
"Deny" survey
"Allow only while using the app"
"Allow only while using the app" survey
"Allow all the time"
"Allow all time" survey

Figure 3: App architecture in Android 10



Allow **MyApplication10** to access this device's location?

(a) Screenshot: When a user clicks the emulator's link

Please follow the link to finish our survey

https://docs.google.com/forms/d/e/1FAIpQLScPSmGduq2hCz3IUFLT_Jg6NUhjvE_csXnrsk8fTak04c9RWQ/viewform?entry.500974868=bFZeHQ

(b) Screenshot: Survey link after a user made permission choice

several possible reasons below, please rate them from "Completely disagree"(1) to "Completely agree"(7)//事实上，我们的研究不是测试我们的应用程序，而是研究给出权限的原因。 我们有以下几种可能的原因，请从“完全不同意”(1) 到“完全同意”(7) 评分

Sign in to Google to save your progress. Learn more

Your participant ID is:

bFZeHQ

(c) Screenshot: Survey with pre-filled participant's ID

Figure 4: Screenshots of our app on emulator with Android 10

Architecture of app for Android 11

The basic idea of this app is the same as the one for Android 11 except we added one more step when they either choose ”While using the app” or ”Only this time” to ask the user to clarify his/her choice because when a user clicks ”While using the app” or ”Only this time” the system will get the result that the user has granted the permission request the only difference is the permission request of one-time permission will be set back to not granted after the user finishes the session. And after the user’s clarification, they will get the different survey links as the app for Android 10.

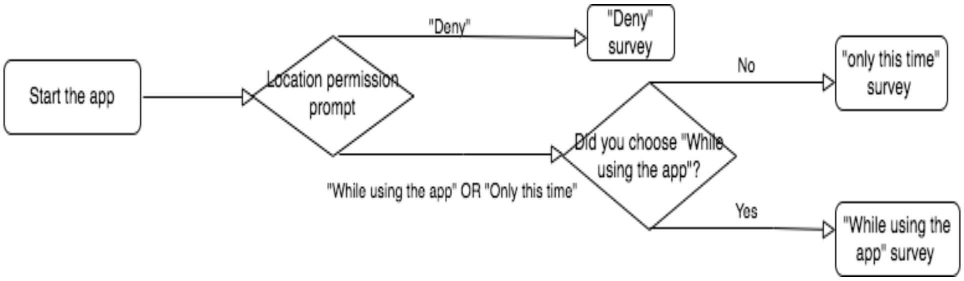
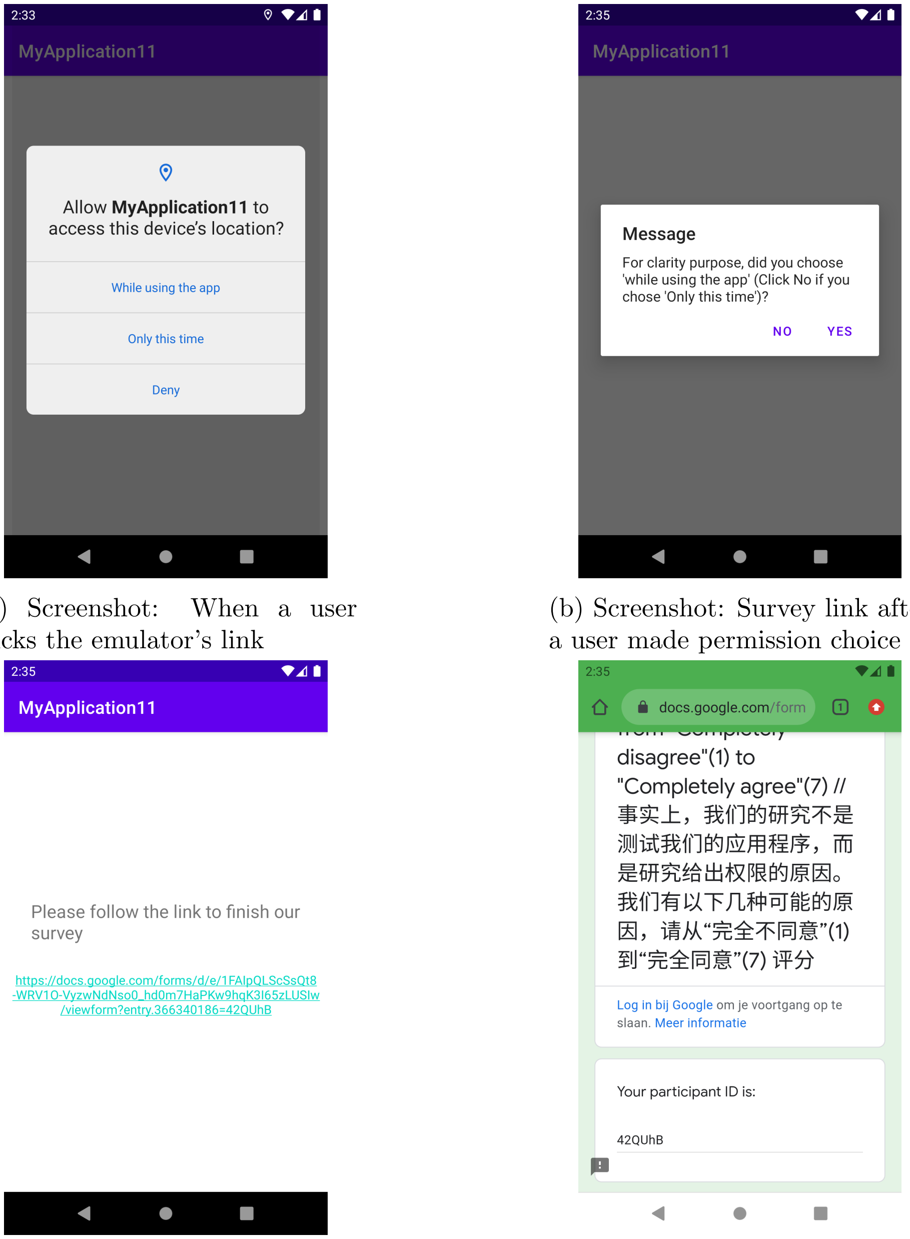

Start the app
Location permission prompt
"Deny"
"Deny" survey
"While using the app" OR "Only this time"
Did you choose "While using the app"?
No
"only this time" survey
Yes
"While using the app" survey

Figure 5: App architecture in Android 11



Allow **MyApplication11** to access this device's location?

(a) Screenshot: When a user clicks the emulator's link

Message

For clarity purpose, did you choose 'while using the app' (Click No if you chose 'Only this time')?

(b) Screenshot: Survey link after a user made permission choice

Please follow the link to finish our survey

https://docs.google.com/forms/d/e/1FAIpQLScSsQt8-WRV1O-VyzwNdNso0_hd0m7HaPKw9hqK3I65zLUSIw/viewform?entry.366340186=42QUhB

(c) Screenshot: A user's choice and ID in database

disagree"(1) to "Completely agree"(7) // 事实上，我们的研究不是测试我们的应用程序，而是研究给出权限的原因。我们有以下几种可能的原因，请从“完全不同意”(1) 到“完全同意”(7) 评分

Log in bij Google om je voortgang op te slaan. Meer informatie

Your participant ID is:

42QUhB

(d) Screenshot: Survey with pre-filled participant's ID

Figure 6: Screenshots of our app on emulator with Android 11

Online Surveys design

We constructed 6 Google forms because as we mentioned before the user will get different survey link based on his/her permission choice, there are 3 and 3 options in Android 10's and Android's location prompts respectively, which is 6 in total. The contents of the surveys are the reasons that we thought are possible to relate their choice and if they are going to do the same choice when the location prompt shows on their own phone. More details can be found in the section: Analyze of possible reason. There is one sample of our survey for users who use the emulator link with Android 10 and one sample survey for users who use the emulator link with Android 11 in appendix.

3.4 Technology Slack

We used Android studio to build our two apps and Firebase Realtime database as our database to store all participants' ID and their choices that we used to show the different survey link based on their choice. The surveys were constructed by Google form and the data was analyzed by R in R studio.

The report paper was constructed in Latex by overleaf. The devices for this research were our own laptop.

3.5 Additional information

This research belongs to the information system research group within the Bernoulli Institute of the RUG and was supervised by Fadi Mohsen who I had weekly meeting with.

Besides, although this research requires user data this is going to be anonymous and does not collect any sensitive data. All the data we collected were only used for the research.

4 Results

4.1 Data analyze

We found 31 participants and sent them the emulator link of Android 10. There are 16 participants who chose ”Allow all the time”, 14 participants who chose ”Allow only while using the app” and 1 person who chose ”Deny” in the prompt of location permission on an emulator with Android 10. The bar plot can be found in Figure 7.

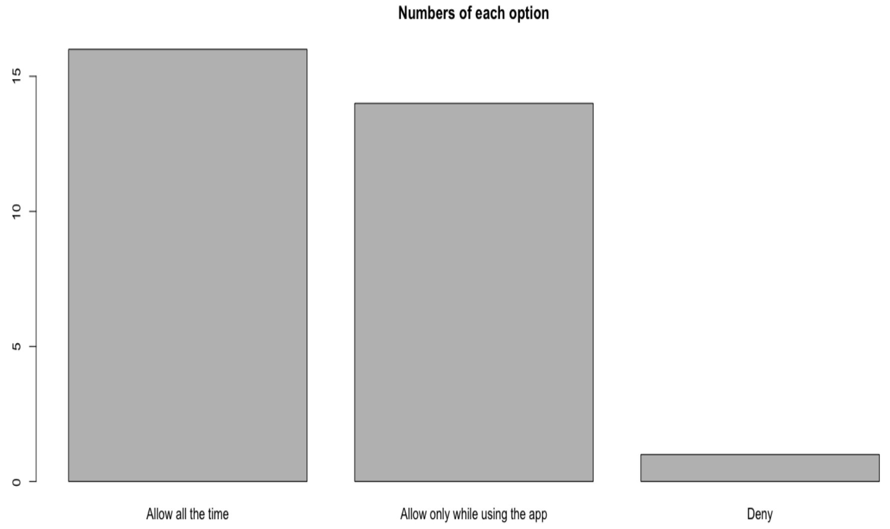


Figure 7: Bar plot of each option in Android 10

We sent out 30 times the link of the emulator with Android 11. As shown in Figure 8, the number of users who chose ”While using the app” is significantly more than the other two options, which have 22 participants, however, there are only 5 and 3 participants who chose ”Only this time” and ”Deny” respectively.

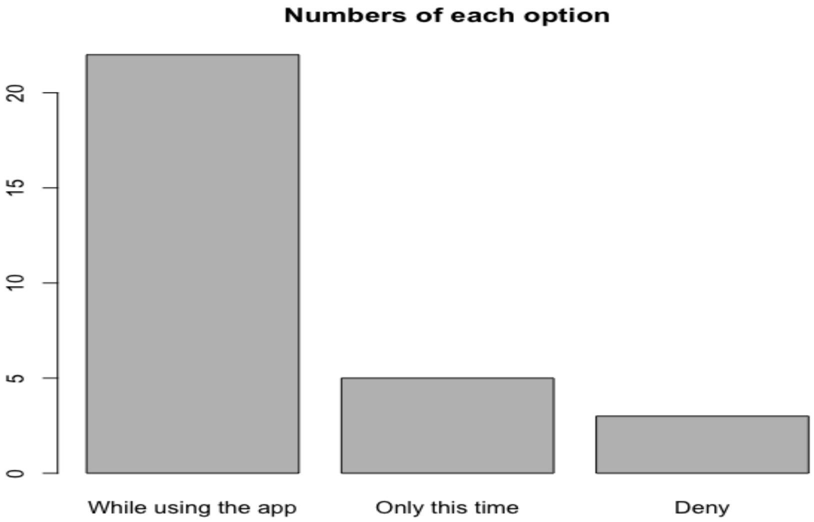


Figure 8: Bar plot of each option in Android 11

We chose the one-sample proportions test to test our hypothesis because we are interested in if the largest proportion of users choose the target option that we want to know if there are at least 51 % of users choose the target option. Additionally, We choose significance level $\alpha = 0.05$

As the proportions test result for Android 10, the $p - value$ is 0.5 which is bigger than our α. Thus, we decide to reject the decoy effect is implemented in the location permission prompt on Android 10(H_1) However, the $p-value$ for Android 11 is 0.01 is smaller than 0.05 that we conclude the decoy effect is employed in the location permission prompt on Android 11(H_2) is accepted by us.

4.2 Analyze of possible reason

We sent the survey to each user about the possible reasons that he/she made that decision on the emulator and if they are going to make the same choice on his/her own phone. We use a scale of 7(1 represents completely disagree and 7 means completely agree, where score 4 is a neutral score) to let participants rate how they agree or disagree with our given reasons.

From the responses of our surveys, we have following conclusion.

In Android 10

- Firstly, we asked our participants if the reason they chose ”Allow all the time” or ”Allow only while using the app” is that they cannot recognize the difference between them. The mean value for ”Allow all the time” is 5.2 which shows they somewhat agree with this reason, however, the mean value for ”Allow only while using the app” is 3.8, which means they somewhat disagree with this reason. It also shows the users who chose ”Allow only while using the app” are more clear about the meanings behind each option in the location permission prompt.

- And then, we asked users if they trust the app that they tested on the emulator, the users who chose ”All all the time” agree with this reason, whereas the users who selected ”All only while using the app” stand neutral because they have the mean value of 5.7 and 4.6 respectively and we rounded up to 6 and 5.

- Finally, is the different reasons for participants who chose ”Allow all the time” and ”All only while using the app”. The participants who chose ”Allow all the time” agree that they made this choice because they do not like the prompt shown over and over again. However, the users who chose ”Allow only while using the app” agree with the reason that they made the choice is because they think they share part of their location data to use the most of app’s functionality.

In Android 11

- The main reason that the users who chose ”Allow all the time” is because they do not want to see the location permission prompt shows every time, which has an average score of 6.2.

- The reason users choose ”Only this time” is because they doubt the safety of our app, but they still want to give a chance to try it.

- They don’t trust our app and they thought our research is irrelevant to their location is the main reason that the participants chose ”deny”, which has an average score of 6.7 and 6.3 individually.

5 Conclusion

In conclusion, our results show there is no decoy effect implemented in the location permission prompt of Android 10, which is a good sign for the users of Android 10 because it's dangerous to let an app can access users' location anytime without notifying once the users choose "Allow all the time". In addition, it shows us we should not only use our mobile device but also learn how to protect it because as our survey results there are still many people who do not know the meaning behind each permission option.

However, the decoy effect is employed in the location permission prompt of Android 11 to protect users' private data, which shows it's possible to lead the users to choose a relatively "safer" option that shares less data but can access the most of functionality. This phenom in Android 11 can give a warning to the app developers as well that they have to think carefully if their app needs access of the users' background location and also shown the decoy effect is not always the bad thing.

References

[1] Abhi. *Understanding permissions for background location on Android 11 and below.* 2020. URL: https://medium.com/@ty2/understanding-permissions-for-background-location-on-android-11-and-below-bc3ad9be320a.

[2] Harry Brignull. *WHAT ARE DARK PATTERNS.* URL: https://www.darkpatterns.org/.

[3] Android Developer. *Location updates in Android 11.* URL: https://developer.android.com/about/versions/11/privacy/location#change-details.

[4] Google Developer. *Permissions on Android.* URL: https://developer.android.com/guide/topics/permissions/overview.

[5] Todd Grennan. *The Changing Face of Location-Based Marketing: What iOS 13 and Android 10 Mean for Customer Engagement.* 2019. URL: https://www.braze.com/resources/articles/ios-13-android-10-location-based-marketing.

[6] Celia Hodent. *The Psychology of Video Games.* Reading, Massachusetts: Taylor Francis Ltd, 2020, p. 79.

[7] Ryan Johnson et al. *Analysis of android applications' permissions.* 2012, pp. 45–46.

[8] Abhishek Kumar et al. "Social networking sites and their security issues". In: *International Journal of Scientific and Research Publications* 3.4 (2013), pp. 1–5.

[9] Maria Rosala. "3 Design Considerations for Effective Mobile-App Permission Requests". In: (2019). URL: https://www.nngroup.com/articles/permission-requests/.

[10] Mirjam Seckler et al. "Trust and distrust on the web: User experiences and website characteristics". In: *Computers in Human Behavior* 45 (2015), pp. 39–50. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.11.064. URL: https://www.sciencedirect.com/science/article/pii/S0747563214006827.

[11] Tobias Seitz. "The Decoy Effect for Passwords – A First Exploration". In: (2016). URL: https://www.medien.ifi.lmu.de/pubdb/publications/pub/seitz2016decoytechreport/seitz2016decoytechreport.pdf.

[12] Ari Shpanya. *Why pricing experiments prove our assumptions are wrong*. 2013. URL: https://econsultancy.com/why-pricing-experiments-prove-our-assumptions-are-wrong/.

Appendix

Sample Android 10 Google form for ”Allow all the time”

In fact, instead of testing our app, our research is to study the reason of your permission decision. We have several possible reasons below, please rate them from "Completely disagree"(1) to "Completely agree"(7)//事实上，我们的研究不是测试我们的应用程序，而是研究给出权限的原因。 我们有以下几种可能的原因，请从“完全不同意”(1) 到“完全同意”(7) 评分

x.guan.1@student.rug.nl (not shared) Switch account

Your participant ID is:

Your answer

Please select your age group // 请选择您的年龄区间

○ Under 20 // 低于 20

○ 20-39

○ 40-59

○ 60+

Reason 1 : "I followed my intuition as I don't know the difference between "Allow all the time" and "Allow while only using the app"."// 原因 1：“我遵循直觉，因为我不知道“始终允许”和“仅使用应用程序时允许”之间的区别。”

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

Reason 2: " "Allow only while using the app" seems a compromise choice for me as I only need to share my location data when it's needed and still ensure the app works functionally." // 原因 2：““仅在使用应用程序时允许”对我来说似乎是一个折衷的选择，因为我只需要在需要时共享我的位置数据，并且仍然确保应用程序正常运行。”

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

Reason 3: "I trust this app that I would like to share my location."// 原因 3：“我信任这个app所以我愿意分享我的位置给这个app。”

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

Are you going to make the same choice if our app was downloaded on your own phone?// 如果我们的app是在您自己的手机上下载的，您会做出同样的选择吗?

○ Yes

○ No

Submit Clear form

Never submit passwords through Google Forms.

This form was created inside of University of Groningen. Report Abuse

Google Forms

Sample Android 11 Google form for ”While using the app”

In fact, instead of testing our app, our research is to study the reason of your permission decision. We have several possible reasons below, please rate them from "Completely disagree"(1) to "Completely agree"(7) // 事实上，我们的研究不是测试我们的应用程序，而是研究给出权限的原因。 我们有以下几种可能的原因，请从“完全不同意”(1) 到“完全同意”(7) 评分

1. Your participant ID is:

____

2. Please select your age group // 请选择您的年龄区间

Mark only one oval.

○ Under 20

○ 20-39

○ 40-59

○ 60+

3. Reason 1 : "I followed my intuition as I don't know the difference between "While using the app" and "Only this time"." // 原因 1：“我遵循直觉，因为我不知道“在使用应用程序时”和“仅这一次”之间的区别。”

Mark only one oval.

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

4. Reason 2: "I trust this app that I would like to share my location." // 原因 2：“我相信这个app所哟我想分享我的位置给这个应用程序。”

Mark only one oval.

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

5. Reason 3: "I hate the prompt shows over and over again while I'm using the app, "While using the app" can ensure it only appear once."" // 原因3：“我讨厌在使用应用程序时一遍又一遍地显示提示，“在使用应用程序时”可以确保它只出现一次。”

Mark only one oval.

	1	2	3	4	5	6	7	
Completely disagree (完全不同意)	○	○	○	○	○	○	○	Completely agree (完全同意)

6. Are you going to make the same choice if our app was downloaded on your own phone?// 如果我们的app是在您自己的手机上下载的，您会做出同样的选择吗?

Mark only one oval.

○ Yes

○ No

This content is neither created nor endorsed by Google.

Google Forms