Privacy Preferences vs. Settings: A Case Study of Android Permissions

Jacqueline White and Heather Richter Lipford
University of North Carolina at Charlotte

Abstract

Understanding user privacy preferences can be useful for designing and evaluating privacy interfaces, as well as developing personalized or automated privacy decisions and guidance. Yet, as users' privacy preferences and decisions are contextual and nuanced, gaining an accurate picture of what users truly want is challenging. To explore this further, we describe a survey study to compare users expressed comfort, desired, and actual settings for Android app permissions. In this poster, we describe the study and preliminary results regarding the differences between users' perceptions and decisions.

1. Introduction

One of the issues encountered in user privacy is understanding the level of privacy users actually want their privacy settings within an application to reflect. This problem is in part due to users who do not understand how data is used and shared based on their settings or permissions [2]. One method of determining user preferences is by asking for users expressed comfort with sharing different types of information and their expressed preferences for the currently offered settings. These can then be used to build a profile of privacy preferences and coach users on how to modify their settings to best reflect their desires [3][4]. However, there is a disconnect and level of uncertainty between users' stated preferences and their actual behavior and privacy needs [1]. When faced with actual decisions in context, their preferences may be different or more nuanced. Users may also be unwilling or unable to modify settings to better match their preferences. Privacy preferences or behaviors can be used to determine default settings, personal profiles and recommendations for users, to examine other variables related to privacy desires or behaviors, and to design and evaluate privacy interfaces. As such, this leads to the question "How much does expressed comfort and stated preferences differ from actual behavior?" In this poster, we report on a survey study examining this question in the context of Android app permissions.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9 -- 11, 2020, Boston, MA, USA.

2. Method

Android allows users to grant or deny access to various app permissions, limiting what the app can access and do. Thus, Android mobile phone users are faced with a number of privacy decisions as they install and use applications. This study uses the context of Android apps to understand user preferences for permission settings to learn how and where permission preferences differ between expressed comfort, desired settings, and actual permission settings. The permissions classified as dangerous by Android that we considered were Calendar, Camera, Contacts, Location, Microphone, Phone, Call Logs, SMS, and Storage. We choose these permissions as participants were more likely to be familiar with what data each of these permissions request access to and how that data is used by apps.

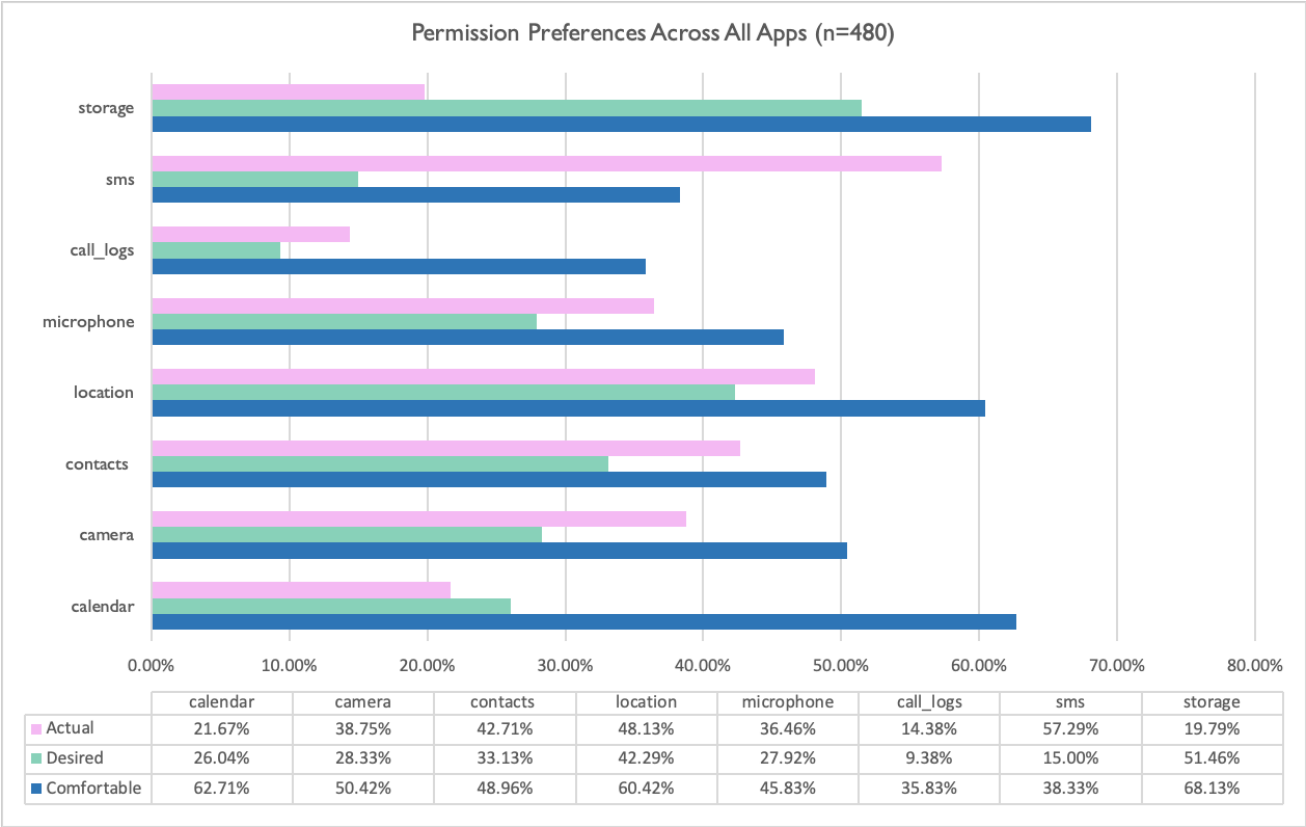
We created a survey on Qualtrics and collected responses from Android users over the age of 18 recruited from Mechanical Turk workers with at least a 95% acceptance rating. In total, we gathered 100 responses, but after removing invalid participant responses, were left with 96 completed surveys. We first asked participants to name 5 apps they used regularly. We then asked questions for each app regarding comfort, desired settings, and actual settings for each of the 9 Android dangerous permissions. Participants were instructed on how to look up their actual permissions on their phone. We added an attention check question for each app regarding the memory size of the app to increase chances participants actually viewed the app settings and entered valid responses. Finally, we ended with several questions regarding changing permissions as well as demographic questions.

2.1. Survey Questions

The comfort question asked participants "*How comfortable are you with [App Name] having access to each of the following permissions or capabilities on your phone?*" This was evaluated using a Likert scale from 1-5, with 1 being uncomfortable and 5 being comfortable with sharing the permission.

The desired permissions question asked participants *"Which of the following permissions would you like to be turned on for [App Name]?"* For each app, participants were shown a list of permissions and had to select each of the permissions they would want to share or indicate they would not like to share any permissions with the app.

The actual permissions question asked participants to *"Please select each of the permissions you currently have turned on."* For this category, participants were shown a list



	calendar	camera	contacts	location	microphone	call_logs	sms	storage
Actual	21.67%	38.75%	42.71%	48.13%	36.46%	14.38%	57.29%	19.79%
Desired	26.04%	28.33%	33.13%	42.29%	27.92%	9.38%	15.00%	51.46%
Comfortable	62.71%	50.42%	48.96%	60.42%	45.83%	35.83%	38.33%	68.13%

Figure 1: Permission preferences across all apps

of permissions that mimicked the appearance of the list of app permissions on their phone, within the limits of the Qualtrics software. Each participant then indicated which permissions they actually had turned on for each app or left all permissions turned off if they were sharing nothing with the app.

We next asked participants how they thought the removal of a permission requested by the app would affect the functionality of the app. We also asked participants if they would make changes to their current permissions and why or why not. These questions were asked to gain insight into why preferences may differ from behavior.

3. Preliminary Results

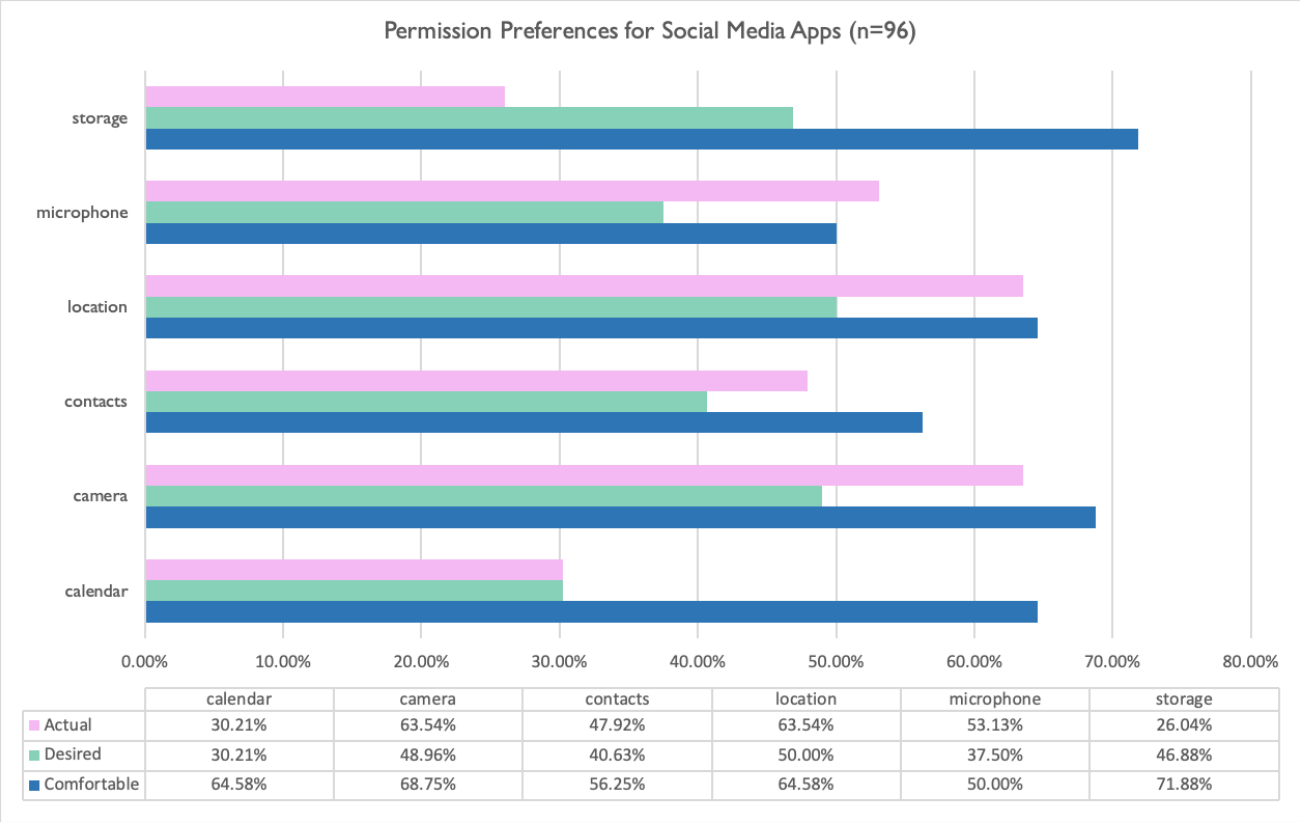
Our goal is to investigate the patterns of where comfort, desire, and actual permissions are similar and differ. Participants were deemed comfortable with a permission if they rated their comfort level as a 3 or higher. All percentages were compiled using the self-reported permissions of users that were not adjusted to remove permissions which are not asked for by an app. Thus far we have compiled descriptive statistics regarding our participants and will use them to direct more quantitative analysis.

Figure 1 is a graph over all participants and apps (n = 96*5 = 480) of each permission and the percentage of users who reported actually allowing that permission, desired to allow the permission, and were comfortable with that permission. As seen in the chart, for the majority of the permissions, more participants granted access to permissions than wanted to grant access. This indicates that while many users would like to share less information with apps or grant access to fewer permissions, they do not remove access to permissions due to constraints such as the requirements of the apps or their own awareness and understanding of the permissions. What is also apparent in Figure 1 is that the comfort and desire differ for many permissions. In many cases, comfort is actually higher than desired permissions and actual permissions.

We also expected that participants would take into account what permissions were needed for a particular application to function. Thus, we are exploring differences within several categories of app type. Figure 2 shows the percentages for the 96 instances of social media apps, namely Facebook, Instagram, Snapchat, and Twitter and the permissions they commonly request. While the percentages differ a bit, overall, this graph reflects the same patterns as Figure 1.

4. Conclusion

Our results thus far indicate that users do desire to share fewer permissions than they are allowing, even in cases where they are comfortable with that app having access to that resource.



	calendar	camera	contacts	location	microphone	storage
Actual	30.21%	63.54%	47.92%	63.54%	53.13%	26.04%
Desired	30.21%	48.96%	40.63%	50.00%	37.50%	46.88%
Comfortable	64.58%	68.75%	56.25%	64.58%	50.00%	71.88%

Figure 2: Permission preferences for social media apps

Thus, comfort does not appear to be the sole basis for permission decisions and may not be the best indicator of users' privacy preferences. We note that the figures here include apps that do not ask for all permissions. Thus, actual permission settings include instances where users have no options to actually enable those permissions. However, users' desired preference would be a more conservative indicator of privacy preferences, particularly if the functional permission needs of each app were addressed. We aim to continue to characterize and investigate these patterns of differences more fully, examining other categories of app, as well as analyzing the responses to the reasons for changing, or not, the permission settings. We aim to provide additional insight into understanding and using users' preferences in privacy research.

5. References

[1] Alex Braunstein, Laura Granka, and Jessica Staddon. 2011. Indirect content privacy surveys: measuring privacy without asking about it. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11), Association for Computing Machinery, Pittsburgh, Pennsylvania, 1–14. DOI:https://doi.org/10.1145/2078827.2078847

[2] Qatrunnada Ismail, Tousif Ahmed, Kelly Caine, Apu Kapadia, and Michael Reiter. 2017. To Permit or Not to Permit, That is the Usability Question: Crowdsourcing Mobile Apps' Privacy Permission Settings. *Proceedings on Privacy Enhancing Technologies* 2017, 4 (October 2017), 119–137. DOI:https://doi.org/10.1515/popets-2017-0041

[3] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. 27–41. Retrieved June 22, 2020 from https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu

[4] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. 399–412. Retrieved June 22, 2020 from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini