Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps

David Harborth, *Goethe University Frankfurt am Main;* Alisa Frik, *ICSI, University of California Berkeley*

https://www.usenix.org/conference/soups2021/presentation/harborth

This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps

David Harborth
Goethe University Frankfurt am Main

Alisa Frik
ICSI, University of California Berkeley

Abstract

Augmented reality (AR), and specifically mobile augmented reality (MAR) gained much public attention after the success of Pokémon Go in 2016, and since then has found application in online games, social media, entertainment, real estate, interior design, and other services. MAR apps are highly dependent on real time context-specific information provided by the different sensors and data processing capabilities of smartphones (e.g., LiDAR, gyroscope or object recognition). This dependency raises crucial privacy issues for end users. We evaluate whether the existing access permission systems, initially developed for non-AR apps, as well as proposed new permissions, relevant for MAR apps, provide sufficient and clear information to the users. We address this research goal in two online survey-based experiments with a total of 581 participants. Based on our results, we argue that it is necessary to increase transparency about MAR apps' data practices by requesting users' permissions to access certain novel and privacy invasive resources and functionalities commonly used in MAR apps, such as speech and face recognition. We also find that adding justifications, contextualized to the data collection practices of the app, improves transparency and can mitigate privacy concerns, at least in the context of data utilized to the users' benefit. Better understanding of the app's practices and lower concerns, in turn, increase the intentions to grant permissions. We provide recommendations for better transparency in MAR apps.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

1 Introduction

The release of Pokémon Go in 2016 increased the public awareness about augmented reality (AR) [41]. AR is defined as a technology which "combines real and virtual objects in a real environment; runs interactively, and in real time; and registers (aligns) real and virtual objects with each other" [4, p.34]. The AR market in general was worth $1.8 billion in 2018, $3.5 billion in 2019 and is expected to increase in value to $18 billion by 2023 [10]. Almost a quarter of the US population, 72.8 million people, used AR at least once a month in 2019. It was projected to increase to 83.1 million people in 2020 (representing 25.3% of the US population) [43].

Currently, the two most popular types of AR are smart glasses and mobile AR (MAR) apps. AR glasses such as the Microsoft Hololens [38] are not yet mature enough products for the end consumer market due to the large weight and size, and high price. This type of AR is primarily used in the Business-to-Business (B2B) environment in which AR could successfully demonstrate its value by saving time and money in numerous processes [28]. However, recent news reveal that Apple is planning to release AR glasses in the near future, which could lead to a major breakthrough of AR smart glasses in the end consumer market [29]. In contrast, MAR apps and AR features within regular mobile apps are already widely available and used within the smartphone ecosystem. One of the most famous examples is the aforementioned MAR game Pokémon Go — one of the most successful mobile apps ever introduced, which generated $1.8 billion revenue in two years [40]. Other popular apps like Snapchat and Instagram integrate AR filters as well, which became even more popular during the COVID-19 pandemic's lockdown among users now spending more of their time in smartphones [52].

In order to create engaging interactive experience, MAR apps require large amounts of data from a variety of sensors, processed using machine learning and artificial intelligence algorithms (e.g., for object recognition, and geometry tracking). Such data-intensive processes inevitably raise concerns about user privacy and security. Based on the analysis of prior

literature, we identify five major differences between MAR apps and non-MAR apps, which amplify privacy and security risks for MAR app users [9, 21]:

1. heavy reliance on the camera input but limited feedback regarding what data is captured by the camera and used by the MAR app;
2. malicious apps can realistically alter digital objects and information presented to the user and deceive them;
3. increased data aggregation capabilities of MAR apps when combining the output of multiple sensors (e.g., location, visual/camera, accelerometer data, etc.), and the opacity of potential inferences and risks associated with such aggregation to the user;
4. privacy breaches in collaborative and shared MAR environments when two or more users work on the same digital objects using separate devices [32];
5. bystanders of MAR systems who are in the field of view and get filmed by the systems without awareness or possibility to control [11].

Therefore, users of MAR apps are exposed to more severe and novel types of privacy risks compared to the ones related to regular, non-MAR, smartphones apps. However, there is a lack of user studies investigating MAR related privacy concerns of users [12, 19]. We contribute research in that field.

While in general data flows in the apps are not transparent to the users [5, 13, 24], a few most common ways in which apps' data collection practices are revealed to the user is through the permission systems and privacy policies. However, not all apps provide privacy policies [47, 49], and even when they do, they are hard to understand for non-expert users which decreases the likelihood that they read the policies [7, 44]. Thus, despite criticism related to a partially ineffective design [17, 26, 56], permissions remain an integral and mandatory element for collecting app user's data. Therefore, we decided to start our analysis of MAR app users' privacy concerns with an investigation of their opinions about the existing permission systems in order to provide recommendations for increased transparency.

Our study addresses the following research questions:

RQ1: How does information provided in smartphone permissions affect users' understanding of what resources and data are accessed by an MAR app? And what are users' expectations about the impact of these permissions on the app's performance?

RQ2: How does information provided in permissions affect users' privacy concerns regarding MAR apps?

RQ3: How do the justifications for requesting smartphone permissions affect users' choices regarding whether to grant such permissions and whether to download an MAR app?

RQ4: How can the transparency of smartphone permissions in MAR apps be improved?

To address these research questions, we conducted two online survey-based experiments with a total of 581 participants (both studies were approved by the university's ethics board). We explored their understanding of a hypothetical MAR app's data practices based on the permissions it requests. We tested both the existing permissions (e.g., to access contacts and camera) and the proposed new ones that are currently not requested in mobile apps, but are commonly accessed by MAR apps without permission, despite having serious privacy implications (e.g., LiDAR, accelerometer and gyroscope, object recognition, etc.). We also added the justifications about how the app will use the data should the permission be granted. In this study, we limited the purposes of data use to the ones relevant to the app's functionalities and overall beneficial to the users (as opposed to malicious or non beneficial data use). We tested whether in addition to the currently used permission labels, the inclusion of such justifications affect participants' understanding of the app's data practices, privacy concerns, and intentions to grant the permission and download the app. Finally, we compared the impact of justifications contextualized to the app's specific functionalities and how it will use the collected data with non-contextualized generic justifications explaining only what data the app will be able to access.

Overall, we find that adding to the existing permission labels the contextualized justifications about app's data practices improves transparency (in Study 1 and 2) and can mitigate privacy concerns (in Study 2), but does not directly affect the willingness to grant the permissions or download the app. In turn, because privacy concerns negatively affect the intentions to grant permissions, while perceived informativeness of the permissions about app's data practices increases such intentions, eventually, the improved transparency and lower perceived privacy danger increase the willingness to grant permissions. Participants said they generally understand what resources and data will be used by the MAR app based on the given permissions. However, in conditions without justifications, they requested more clarifications about what data is collected by the app, how it is used, whether it is possible to decline the permission, and how it would affect the app's performance. Finally, we find that participants are especially concerned about face and speech recognition, but current systems don't request permissions to run such analysis. Based on the results, we provide recommendations for the improved data transparency in MAR apps' mobile permission systems. Our results hold in the context of data utilized to the users' benefit, and future work is needed to explore other contexts.

2 Related Work

There are two main streams of literature relevant to this work. The first one explores user privacy concerns regarding mobile permissions, and the second one explores user privacy concerns regarding Augmented Reality (AR) technologies.

2.1 Privacy Concerns with Permissions

A plethora of prior research on mobile permissions and privacy-related user perceptions about them confirm that the existing permission systems are not fully transparent and clear to the users [15, 27]. Provision of permissions to users in app stores without any contextual information results in users forgetting about permissions later [6]. Moreover, when apps require more sensitive permissions, it increases users' privacy concerns [18] and decreases the ratings and number of downloads of such apps [30]. Thus, these factors have an immediate economic impact and relevance for app developers and the respective companies [18].

Providing participants with relevant information in runtime permissions is shown to increase transparency for the users [57, 58]. However, besides the general question of when to request permissions [14] and how to simplify them [37], it is still unclear whether the communication of apps' data collection practices in the permission systems can and should be presented in more detail. Particularly, users find it hard to identify the reasons why an app uses a specific resource at all [34]. While requesting app permissions helps users become aware of what data is being accessed by the app, users also want to better understand *why* applications need certain information [27]. By by providing the appropriate justifications and meeting users' expectations regarding the reasons for accessing sensitive resources, apps can increase users' trust [34] and alleviate privacy concerns [18]. However, some research shows that meaningless justifications (that pretend to clarify the purpose of data use, but essentially don't provide any meaningful information) also alleviate user concerns, and therefore can be deceptive for the users [51]. Thus, it is important that permission justifications provide accurate and useful information.

2.2 User Privacy Concerns with AR

Research on privacy in MAR apps is important since context-specific privacy concerns can differ greatly from general privacy concerns towards mobile apps [1, 42]. Although there is a large body of technical research about privacy and security in augmented reality technologies [9], there is little research on end user perceptions and privacy concerns regarding AR technologies, especially, among research focused on *mobile* AR [19]. The limited empirical evidence suggests that AR raises privacy concerns among users, for instance, about being filmed by AR devices (as bystanders [11]), surveillance, and distributing data involuntarily [8, 20, 22, 23, 46].

The analysis of permissions in 19 most downloaded MAR apps in Google Play Store shows that they violate users' privacy and do not follow the principle of least privilege, i.e., apps oftentimes require access to more permissions than they actually need for their stated functionalities [21]. Besides the consumer protection concerns, privacy threats can be a hindering factor for technology adoption [3, 48], which could prevent useful AR applications to be accepted by potential users (e.g., for medical purposes like helping Parkinson's disease patients [36, 54]). Therefore, it is important to understand and address MAR apps' users' privacy concerns.

While prior research has investigated user concerns with mobile permissions and AR technologies separately, to the best of our knowledge no prior work has examined users' privacy concerns regarding the permissions of MAR apps, the impact of permission justifications on these concerns, and intentions to grant permissions to such apps and download them. In this study, we attempt at closing this gap.

3 Study 1

3.1 Method

To answer the research questions, we designed an online survey-based experiment with a between-subject design and three conditions. We presented participants with a scenario describing a fictional mobile augmented reality (MAR) app that can help to redesign a room or outdoor space. We told participants that, by using augmented reality, the app can take and save measurements, or display 3D models of the furniture over the image of the real environment. Also, we told them that users can share the new design ideas and measurements with friends, family, designers, or contractors, via email or in social networks. Then we presented participants with a list of permissions this app requires.

In the *Control* group, participants were presented only with the labels of the permissions without any justifications (e.g. Microphone, Contacts). In the *Contextualized Justification* (CJ) condition, along with the label, we showed participants the explanation of what data or device's sensors will the app access or what data processing approaches will it use (e.g., face or speech recognition) and how it is related to the app's specific functionalities, to help participants understand the purpose of data collection in the context of this particular app. For example, the contextualized justification for the *Microphone* permission mentioned that access to the microphone is required to add voice notes to the measurement photos. In the *Non-Contextualized Justification* (NCJ) condition, the explanation was generic, without adding much to the information in the permission label and without adding context to how the requested permission is related to the app's functionalities and data collection needs. For example, the non-contextualized justification for the *Microphone* permission mentioned that access to the microphone is required to record audio, without explaining why a measurement app would need it. Table 6 in Appendix B provides the text of permission justifications.

We included 7 permissions that are commonly requested in MAR and non-MAR apps: *Storage/Photos/Media Library*, *Contacts*, *Network/Internet Access*, *Microphone*, *Camera*, *Location Services*, and *Notifications*. To account for the customs

of iOS and Android device users, when different, we included labels from both operating systems, e.g., Network/Internet Access. Additionally, we included 9 categories of resources and data processing approaches that are often used in MAR apps, but for which MAR apps currently do not explicitly request user permission (except for *Speech Recognition* on iOS): *Accelerometer*, *Gyroscope*, *Magnetometer*, *LiDAR Scanner*, *Geometry Tracking*, *Raw Camera Output*, *Object Recognition*, *Face Recognition*, and *Speech Recognition*. For simplicity, in this paper we refer to all 16 resources and data processing approaches as *permissions*.

After showing the list of permissions, we asked participants, based on that list, to what extent they understand what data and resources on their device the app will be able to use. We also collected open-ended responses about what additional information would help to improve that understanding. Then we asked whether participants would allow or deny our fictional app access to those permissions on their device, how denying that permission would affect the app's performance, and how granting the permission would affect users' privacy. Finally, we asked about demographics, experience with MAR apps and features, and definition of AR. We also included several attention check questions. See survey in Appendix A.

Quantitative Analysis We used an ordered random-effects logistic regression model to analyze participants' choices regarding granting permissions. The "I am not sure" answers were treated as missing. We calculated the model with three specifications. Model 1 is the base model that includes only the main independent variables about the permissions. Model 2 adds control variables like demographics and AR knowledge to the base model. Model 3 adds further variables based on the five most relevant codes from the qualitative analysis (equals 1 if the participant mentioned the code) to model 2.

We used Shapiro-Wilk tests to assess the normality of data distribution, Wilcoxon rank sum tests for pairwise comparisons, and ANOVA and Kruskal-Wallis equality-of-populations rank tests to assess the differences between the treatment groups. We applied Holm's and Hochberg corrections to all pairwise statistical tests and regressions, and report only the significant results.

Qualitative Analysis To analyze the open-text survey responses we used thematic analysis. Two coders independently developed initial codebooks, merged them, discussed and agreed on the final codebook (Appendix D). They independently applied the codes to all the responses, allowing for multiple attributes per response. Kupper-Hafner interrater agreement rate was 0.84 [31]. Finally, the coders discussed and resolved all the disagreements.

3.2 Participants

We recruited 300 participants using Prolific in June 2020. We restricted participation to US residents, over 18 years old, who use mobile devices on a regular basis, and have approval rates on Prolific over 95%. We excluded 6 responses in which participants failed the attention checks, and 2 responses that were fully identical. The resulting sample consists of 292 participants, which are randomly distributed among three groups: Control ($N = 96$), CJ group ($N = 104$) and NCJ group ($N = 92$). Our sample is sufficient, as power analysis suggested to recruit 85 participants per group to achieve 90% power, with 5% error rate and 0.5 effect size.

The resulting sample has diverse demographics. The participants are 18-74 years old ($mean = 29, SD = 11.40$), 48.63% female and 2.4% prefer to self-identify their gender. About 34% have Bachelor's degree, 31% have done some college but no degree, and 14% have only finished high school; and 31.51% of the participants reported to have a technical background in computer science. ANOVA test confirms no difference in age, gender, and education among the three groups.

Slightly more than half (57.19%) of the participants use an iPhone, and the rest use Android smartphones. The majority of participants choose the correct definition of AR (74.66%) and have experienced AR features (79.45%) like photo masks (e.g., bunny ears in messaging apps) or placing digital objects in the real environment (e.g., AR furniture apps).

3.3 Results

The majority of participants (86.30%) agreed that based on the provided list of permissions they understand what resources and data the app will be able to use (Q3 in Appendix A). On average, compared to the Control group, participants in the CJ group expressed better understanding of what functionalities and data on their device the app will be able to use based on the list of permissions (Wilcoxon rank sum test: $p = 0.0012$). However, there was no difference between NCJ and Control, and between CJ and Non-CJ groups. This means that providing contextualized justification about why the app requires a certain permission and what data it will use significantly improves users' understanding of the app's data practices compared to showing just the permission labels. In contrast, providing the explanations that are not put in context of the specific app do not yield better users' understanding of the app's data practices compared to using just permission labels.

To understand the relative impact of different factors on users' intentions to grant permissions, we conducted regression analysis (Table 7 in Appendix C). Despite significant impact on the ability to understand app's practices (based on the test results), after controlling for other effects, we find no significant treatment effects of justifications on the willingness to grant the permissions. In other words, on average, providing justifications, contextualized or not, does not affect

participants' willingness to grant the permissions when other factors are taken in consideration.

On the other hand, participants are 43% less likely to allow the permission when they believe it will negatively affect app's performance or ability to function (Q8), and 33% less likely to grant the permission when they are concerned about the privacy implications of granting the permission (Q9). In contrast, when participants find the permissions informative, i.e., helpful in understanding what resources and data the app will be able to access (Q11), the odds of granting access to the permissions are 1.245 times higher, given all other variables are held constant.

Other controls like the prior use of AR features, familiarity with the definition of AR, gender, age, education, prior technical experience, smartphone use frequency and mobile OS do not have an effect.

3.3.1 Analysis of Individual Permissions

Willingness to grant the permissions Most participants are willing to allow the permissions (Q7) while the app is in foreground and only few participants would allow the permissions at all times (Figure 1). The majority of participants prefers to deny such permissions as *Contacts*, *Microphone* and *Face Recognition*.

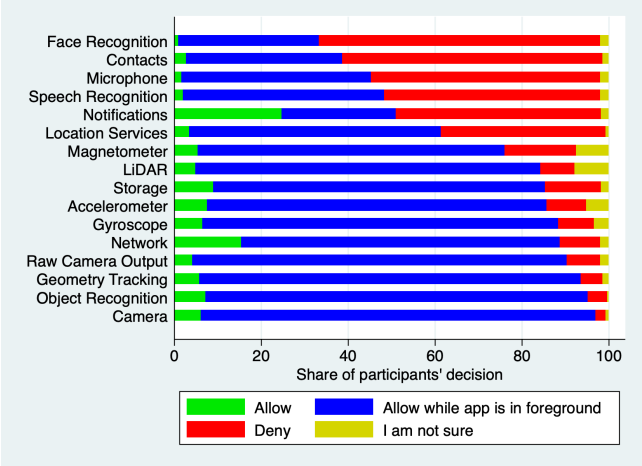

Figure 1: Willingness to grant the permissions (Study 1).

Based on the regression results, we estimated the probabilities for each individual permission to be granted (Table 1). Participants prefer to allow most permissions while in the foreground. However, the likelihood of denying or allowing while in foreground is almost equally split for the following permissions: *Contacts*, *Microphone*, *Location*, *Face Recognition* and *Speech Recognition*.

We also conducted 16 regressions for each of the 16 permissions with the demographic and control variables (same regression model as in Table 7). We did not find any interesting patterns in the results of the individual regressions.

Table 1: Estimated probabilities to deny, allow while in foreground, and allow at all times the permissions (Study 1).

Permissions	Pr_{deny}	$Pr_{foreground}$	Pr_{always}
Storage/Photos/Media Lib.	.239	**.707**	.054
Contacts	**.453**	**.530**	.017
Network/Internet Access	.195	**.728**	.077
Microphone	**.451**	**.533**	.016
Camera	.105	**.772**	.123
Location	**.403**	**.575**	.022
Notifications	.295	**.669**	.036
Accelerometer	.161	**.739**	.100
Gyroscope	.131	**.746**	.123
Magnetometer	.199	**.733**	.068
LiDAR Scanner	.144	**.755**	.101
Geometry Tracking	.111	**.771**	.118
Raw Camera Output	.166	**.750**	.084
Object Recognition	.128	**.759**	.113
Face Recognition	**.506**	**.481**	.013
Speech Recognition	**.433**	**.548**	.019
Total	.257	**.675**	.068

Perceived privacy implications of the permissions To get detailed insights on a permission-specific level, we plot the perceived privacy dangerousness (Q9) of each permission in Figure 2. Participants believe that permissions allowing access to *Face Recognition*, *Contacts*, *Location*, *Microphone*, *Storage* and *Speech Recognition* have the biggest negative impact on their privacy. In contrast, *Magnetometer*, *Accelerometer* and *Gyroscope* are perceived as least privacy invasive.

Participants in the CJ group have, on average, the highest privacy concerns regarding the permissions (mean=4.25 out of 7), followed by the Control group (mean=4.18) and the NCJ group (mean=3.96). The differences between CJ and NCJ as well as Control and NCJ are statistically significant (Wilcoxon rank sum tests: $p = 0.0001$ and $p = 0.0029$, respectively). The difference in the perceived privacy dangerousness between the Control and CJ group is not significant.

Perceived impact on app's performance Overall, participants believe that *denying* the permission would not drastically affect the way the app functions (Q8) (mean=4.03 out of 7). Participants in the NCJ group expected the larger decrease in the app's performance if they deny the permissions, compared to the CJ group (Wilcoxon rank sum tests: $p = 0.0393$; means are 3.95 and 4.12, respectively).

Regarding the effect of *granting* permissions on the device's normal operations (Q10), participants perceive that there is no such negative effect (mean=2.93). There are statistically significant differences between the CJ (mean=3.06) and NCJ (mean=2.72) groups ($p < 0.0001$) and between the Control (mean=2.99) and NCJ groups ($p < 0.0001$).

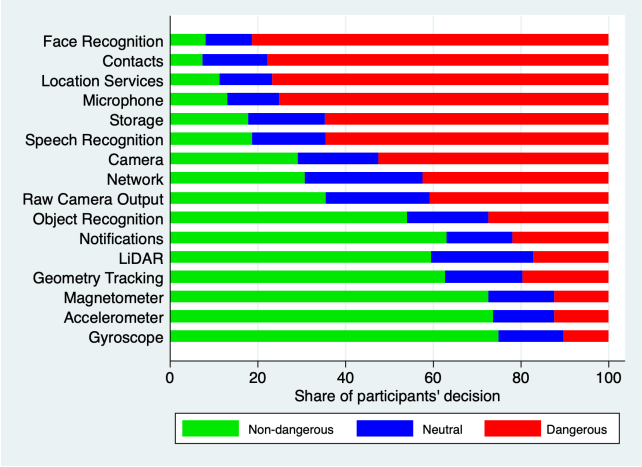

Figure 2: Privacy concerns regarding permissions (Study 1).

Perceived informativeness of the permissions Overall, participants said that they understand what resources and data the app will be able to access if they grant the permissions (Q11) (mean=5.23 out of 7). For example, *Magnetometer* and *LiDAR* are perceived as least informative (means are 3.95 and 4.32, respectively). For all other permissions the means range from 4.95 (*Geometry Tracking*) to 6.22 (*Camera*).

There are statistically significant differences in the participants' perceptions of informativeness (i.e., helpfulness of individual permissions in understanding app's data practices) between the Control (mean=4.78), CJ (mean=5.64) and NCJ (mean=5.25) groups (Wilcoxon rank sum tests $p < 0.0001$ for all three comparisons).

Then, we evaluated the informativeness of the added justifications (compared to solely labels provided in the Control group) according to the following two criteria: 1a) Contextualized justifications should be perceived statistically significantly more informative than the labels alone in the Control group, and 1b) non-contextualized justifications should not. 2) Contextualized justifications should be perceived statistically significantly more informative than non-contextualized ones. We compare the CJ and NCJ group because prior work suggests that practically "meaningless" justifications for the permissions that do not add clarity still may alleviate user concerns [51] as they create a false sense of legitimacy.

We identified that all permissions met Criterion 1, but several permissions did not fulfill Criterion 2. Specifically, our manipulation in the CJ group was effective: compared to the Control group, adding contextualized justifications increases their perceived informativeness, or helpfulness in understanding app's data practices, while non-contextualized justifications do not. Thus, our study provides contrasting evidence compared to the prior work on permission justifications (e.g. [51]).

Criterion 2 is only met by several contextualized justifications: *Face Recognition*, *Speech Recognition*, *Contacts*, *Microphone*, *Storage*, *Network*, and *Accelerometer*. We hypothesized that linguistic complexity [50] might potentially explain that result: some of our contextualized justifications were relatively long and used complex terms in order to provide an informative explanation for the purposes of permission requests.

Thus, it is possible that while contextualized justifications provided more information, this information was harder for the participants to understand than non-contextualized justifications, leading to their reduced perception of informativeness. To address this, in Study 2 we modified the wording of justifications to ensure the equal linguistic complexity so that contextualized and non-contextualized justifications are similar in the required grade level and reading skills to understand them (see Section 4).

3.3.2 Qualitative Results

We asked participants what additional information would help them understand what resources and data on their devices the app will be able to use (Q4). Appendix D provides the codebook, and Table 2 summarizes the most common themes identified in the qualitative analysis of responses. Many participants (74/292), especially in the treatment groups where justifications were provided, said that they do not need any additional information as permission descriptions were already clear enough. However, many other participants said they would like to know more about why the permission is needed and how the data is going to be used (86/292), or requested general clarifications about sensors and features (42/292). Some participants specifically mentioned that they would like the clarifications be concise (17/292), or recommended improving visual representations of the permissions and justifications (11/292), for example, by using demos, screenshots, images, expandable explanations, or grouping the information by topic. Some participants would like to know whether it is possible to deny or restrict individual permissions (18/292) and when the specific data is collected and accessed (13/292).

ANOVA test results indicate that more participants said they do not need additional information in the CJ group ($p < 0.001$) and NCJ group ($p = 0.007$) compared to the Control group. Similarly, the clarifications about sensors or resources were significantly less often requested in the CJ group ($p = 0.023$) and Non-CJ group ($p = 0.031$) than in the Control group. Participants in the CJ group were more often interested to know whether they can deny individual permissions than people in the Control and NCJ group ($p < 0.001$). Participants in the Control group requested information about the purpose of data collection more often than in the CJ ($p < 0.001$) and NCJ group ($p = 0.002$), and they requested this information in NCJ group more often than in CJ group. This result further supports the informativeness of permission justifications, especially the contextualized ones.

In summary, we observed that contextualized justifications

Table 2: Common themes about the additional information needed in the permission justifications, and the ANOVA results of differences between three groups (Study 1, $N = 292$).

Code	Freq., %	ANOVA
Why/how data is used	29.45	F(2)=22.44, p < 0.001
No information needed	25.34	F(2)=8.35, p < 0.001
N/a	15.75	-
Clarifications needed	14.38	F(2)=3.30, p < 0.05
Possibility to deny/ restrict permissions	6.16	F(2)=7.97, p < 0.001
Should be brief / shorter	5.82	F(2)=8.13, p < 0.001
When data is collected/accessed	4.45	-
Visual	3.77	-
Frequency of specifically mentioned permissions		
Microphone	6.51	-
Face recognition	6.51	-
LiDAR	6.16	-
Contacts	5.48	-
Location	3.42	-
Speech recognition	3.42	-

improve the informativeness of the permissions about app's data practices, but do not affect participants' privacy concerns or willingness to grant the permissions, compared to the Control group. However, we observed the need to modify the wording of our justifications to ensure similar linguistic complexity between treatment groups. We also were curious if permissions affect the willingness to download the app. Thus, in Study 2 we modified the wording of our justifications, and added a question about the intention to download the MAR app.

4 Study 2

4.1 Method

The design of Study 2 and its survey (Appendix A) was the same as in Study 1, except several changes. First, to rule out the potential confounding effects due to the difficulty in understanding the justifications' wording, we assessed the linguistic complexity of the contextualized and non-contextualized justifications with the Python library Textstat [45]. This library offers the possibility to measure seven different metrics of a text's readability and complexity levels, and obtain an overall readability score, which combines all seven metrics in one to provide an estimated school grade level required to understand a given text. We used this combined measure to evaluate the complexity of our justifications as it adjusts for biases from single measures such as Flesch-Kincaid or Gunning Fog [45, 49, 55]. Based on the assessment of linguistic complexity, we slightly modified the wording of justifications to simplify and make them similarly easy to understand in the CJ and NCJ conditions (see Table 3).

Second, we added a question about the willingness to download our hypothetical app (Q20) and evaluated factors influencing this download intent using an ordered logistic regression. Finally, we excluded the open-response questions about the participants' suggestions for improving the permissions (Q4-6) as we have already gained enough insights in Study 1 and wanted to keep the survey short.

4.2 Participants

We recruited 306 participants using Prolific in October 2020. We restricted participation to US residents, over 18 years old, who use mobile devices on a regular basis, have approval rates on Prolific over 95%, and have not participated in Study 1. We excluded 16 responses in which participants failed the attention checks, and 1 participant who reported to use a smartphone only about once a year. The resulting sample consists of 289 participants, which are randomly distributed among three groups: Control ($N = 95$), Contextualized Justifications (CJ) ($N = 99$) and Non-Contextualized Justifications (NCJ) ($N = 95$).

The sample composition is similar to Study 1. The participants are 18-69 years old (mean=28.53, SD= 9.59), 57.09% female and 3.81% prefer to self-identify their gender. About a third (30.45%) have a Bachelor's degree, 31.14% have done some college but no degree, and 15.57% have only finished high school; and 29.07% of the participants reported to have a technical background in computer science. ANOVA test confirms that there is no difference in age, gender, and education among the three experimental groups.

Slightly over half of the participants (53%) use Android smartphones, and the rest use Apple's iPhones. The majority of participants choose the correct definition of AR (75.43%) and have experienced AR features (76.12%) like photo masks (e.g., bunny ears in messaging apps) or placing digital objects in the real environment (e.g., AR furniture apps).

4.3 Results

The majority of participants (86.16%) agreed that based on the provided list of permissions they understand what resources and data the app will be able to use (Q3, Appendix A). Participants in the CJ group expressed better understanding than participants in the Control group (Wilcoxon rank sum test: $p = 0.0165$), while there was no significant difference between the NCJ and Control groups, and between the CJ and NCJ groups. These results confirm our findings in Study 1.

Table 3: Permission labels and justifications in Study 2.

Label	Non-Contextualized justification	Contextualized justification
Storage / Photos / Media Library	Access to the smartphone's storage is required to store data processed by the app.	Access to the smartphone's storage is required to save, check, and delete your measurements or furniture ideas.
Contacts	Access to the contacts is required to reach out to your contacts.	Access to the contacts is required to share measurements with your contacts.
Network / Internet Access	Internet access is required to connect the app with the Internet.	Internet access is required to download the images of furniture.
Microphone	Access to the microphone is required to record audio.	Access to the microphone is required to add voice notes to your measurement photos.
Camera	Access to the camera is required to take pictures and videos.	Access to the camera is required to take pictures and videos of the room you are measuring and show the furniture ideas in it.
Location services	Access to location is required to find out where you are.	Access to location is required to filter furniture ideas for those that deliver to your area.
Notifications	Access to notifications is required to send you notifications.	Access to notifications is required to inform you about contacts' comments on furniture ideas.
Accelerometer	Access to the accelerometer is required to improve image stabilization.	Access to the accelerometer is required to improve the image quality and measurements of your room.
Gyroscope	Access to the gyroscope is required to improve image stabilization.	Access to the gyroscope is required to improve the image quality and measurements of your room.
Magnetometer	Access to the magnetometer is required to improve image stabilization.	Access to the magnetometer is required to improve the image quality and measurements of your room.
LiDAR Scanner	Access to the LiDAR scanner is required to illuminate the target with laser light and measure the reflection with a sensor.	Access to the LiDAR scanner is required to measure your room more accurately in low light.
Geometry Tracking	Allowing the app to use geometry tracking is required to create a schematic outline of the environment.	Allowing the app to use geometry tracking is required to measure a schematic outline of a room instead of a real image of it.
Raw Camera Output	Allowing the app to use raw camera output is required to gather and process the real images captured by the camera.	Allowing the app to use raw camera output is required to measure a real image of a room instead of a schematic outline of it.
Object Recognition	Allowing the app to use object recognition is required to detect physical objects.	Allowing the app to use object recognition is required to check if the new furniture (e.g. chairs) would fit with the existing furniture (e.g. table).
Face Recognition	Allowing the app to use face recognition is required to detect faces.	Allowing the app to use face recognition is required for you to log into the app without a password.
Speech Recognition	Allowing the app to use speech recognition is required to identify words and phrases in spoken language.	Allowing the app to use speech recognition is required to turn your voice notes about furniture ideas into text.

The regression analysis (Table 8 in Appendix C) confirms the results from Study 1 as well. We find no treatment effects. Based on the calculations of odds ratios, we find that participants are 40% less likely to grant the permissions when they believe it will negatively affect the app's performance and ability to function (Q8) and 33% less likely when they are concerned about the impact of granting the permissions on their privacy (Q9). Furthermore, they are 1.15 times more likely to grant the permissions when they find them informative (Q11). Moreover, frequent use of the smartphone is negatively associated with the intention to grant the permission (odds ratio = 0.29). Other controls do not have an effect.

4.3.1 Analysis of Individual Permissions

Willingness to grant the permissions As in Study 1, most participants are willing to allow the permissions (Q7) while the app is in foreground and only few participants would allow the permissions at all times (Figure 3). The majority of participants are willing to deny such permissions as *Contacts*, *Microphone*, *Location*, *Face Recognition* and *Speech Recognition* (Table 4). We also find statistically significant negative effects of perceived privacy dangerousness on the intention to grant permissions for several permissions: *Location*, *Contacts*, *Microphone*, *Storage*, *Face Recognition* and *Speech Recognition*, and *Raw Camera Output*. This is not surprising as most of these permissions are perceived especially invasive (Figure 4).

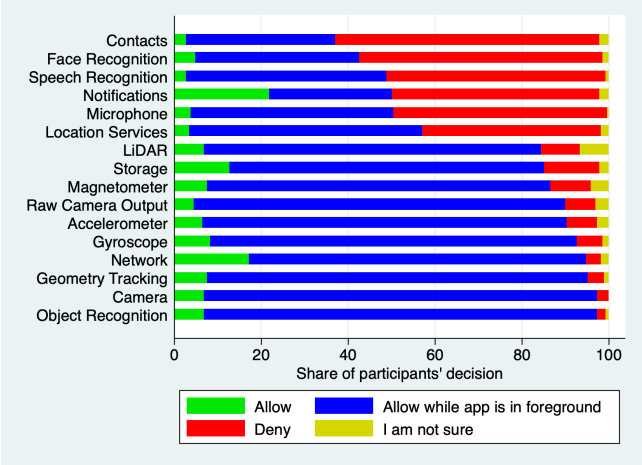

Figure 3: Willingness to grant the permissions (Study 2).

Table 4: Estimated probabilities to deny, allow while in foreground, and allow at all times the permissions (Study 2).

Permissions	Pr_{deny}	$Pr_{foreground}$	Pr_{always}
Storage/Photos/Media Lib.	.229	**.701**	.070
Contacts	**.445**	.534	.021
Network/Internet access	.169	**.732**	.099
Microphone	**.411**	**.562**	.027
Camera	.114	**.754**	.132
Location	**.407**	**.564**	.029
Notifications	.272	**.682**	.046
Accelerometer	.146	**.738**	.116
Gyroscope	.126	**.737**	.137
Magnetometer	.166	**.734**	.100
LiDAR Scanner	.153	**.738**	.109
Geometry Tracking	.120	**.740**	.140
Raw Camera Output	.156	**.743**	.101
Object Recognition	.119	**.747**	.134
Face Recognition	**.438**	**.536**	.026
Speech Recognition	**.408**	**.562**	.030
Total	.242	**.675**	.082

Perceived privacy implications of the permissions Overall, participants believe that the permissions have a moderate effect on their privacy (Q9) (mean=3.94 out of 7). In contrast to Study 1, participants in the CJ group have on average the lowest privacy concerns (mean=3.75), followed by the NCJ group (mean=3.99) and the Control group (mean=4.095). The differences between CJ and NCJ ($p = 0.0031$) as well as Control and CJ ($p < 0.0001$) are statistically significant, while the difference between the Control and NCJ group is not. In other words, while privacy perceptions elicited in the NCJ and Control groups are similar between Study 1 and 2, the modified contextualized justifications in Study 2 elicited less privacy concerns than in the CJ group in Study 1 and than in NCJ and Control groups in Study 2. This suggests that the privacy perceptions regarding permissions can be sensitive to the wording of contextualized justifications.

In line with Study 1, Figure 4 shows that participants perceive permissions allowing access to *Location Services*, *Contacts*, *Face Recognition*, *Microphone*, *Speech Recognition* and *Storage* to have the biggest negative impact on their privacy. *Magnetometer*, *Accelerometer*, *Gyroscope* and *Notifications* are perceived as least privacy invasive. We discuss whether our findings match the categorization of the Android Developer Guide into *normal* and *dangerous* permissions in Section 5.

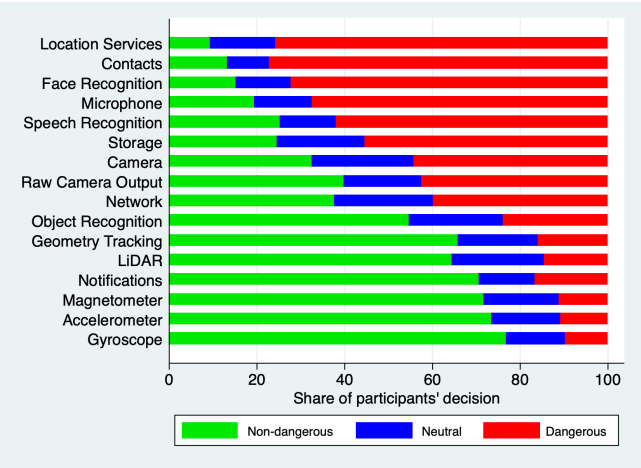

Figure 4: Privacy concerns about the permissions (Study 2).

Perceived impact on app's performance Overall, participants believe that *denying* the permission would not drastically affect the way the app functions (Q8) (mean=3.94 out of 7). As in Study 1, after denying the permission, participants expect the app to function better in the CJ group (mean=4.13) than in the NCJ group (mean=3.82, $p = 0.0001$) and the Control group (mean=3.86, $p = 0.0014$).

Participants perceive that there is no negative effect (mean=2.75) of *granting* permissions on the device's normal operations (Q10). In contrast to Study 1, participants in the CJ condition expected the least negative effect (mean=2.58) compared to the NCJ group (mean=2.7, $p = 0.0492$) and the Control group (mean=2.97, $p < 0.0001$). The difference between the Control and NCJ groups is also significant ($p < 0.0001$). The difference with Study 1 is likely related to the modifications in the wording of justifications in Study 2.

Perceived informativeness of the permissions Overall, participants said that they understand what resources and data the app will be able to access if they grant the permissions (Q11) (mean=5.35 out of 7). *Magnetometer* and *LiDAR* are perceived as least informative (means are 4.22 and 4.49, respectively). For all other permissions the means range from 4.82 (*Accelerometer*) to 6.26 (*Camera*).

We also evaluated to what extent participants' perceptions of informativeness (i.e., helpfulness of individual permissions in understanding app's data practices) differ between treatment and control groups. In line with Study 1, there are statistically significant differences between the Control (mean=4.93), CJ (mean=5.74) and NCJ (mean=5.37) groups (Wilcoxon rank sum tests are $p < 0.0001$ for all three comparisons).

In the next step, we evaluate whether our changes in the wording of justifications based on the insights from Study 1 resulted in any changes in the perceived informativeness of the *individual* permissions. As in Study 1, all permissions with contextualized justifications are perceived as significantly more informative than using only labels (Control group) and there are no statistically significant differences between permissions with non-contextualized justifications and labels only. Contextualized justifications are perceived as significantly more informative than non-contextualized ones only for several permissions: *Network*, *Microphone*, and *Notifications* (Kruskal-Wallis test, p<0.05).

4.3.2 Analysis of Willingness to Download the App

Slightly more than a third of participants (37.72%) said they would be willing to download the app based on the list of permissions. As we assessed the impact of the entire list of permissions, instead of the individual permissions, on the willingness to download the app, there was only one response per participant (i.e. it is not a permission-specific dependent variable). Thus, we could not use the panel structure of the data as in the regressions on the willingness to grant the permissions. Therefore, we created indices for the permission-specific categorical variables Q8-Q11, to estimate the participants' overall perspectives on those variables across all permissions. We calculated a polychoric correlation matrix for each variable and predicted the number of factors for each variable based on the eigenvalues larger than 1, similarly to the procedures of the exploratory factor analysis. The resulting indices and values for Cronbach's α ($0.80 - 0.94$) are shown in Table 5. We then included those indices in the ordered logistic regression models on the willingness to download the app as the dependent variable (see Table 9 in Appendix C).

The only significant variable after the Holm's and Hochberg corrections is the general understanding of the app's data practices. It has a significant positive effect, increasing the intentions to download the app by 1.54 times.

5 Discussion and Conclusions

Overall, prior research suggests that justifications are useful in helping users understand permissions in regular mobile apps [18, 27, 34, 51]. While our work confirms that it is also useful in the MAR apps, it illustrates that justifications are not equally useful, and that they are most effective when explained in the context of a particular app. In addition to the interest in knowing the purpose of data collection, also found in [27], our participants wanted to know which permissions they can restrict/deny and how it would affect the functionality. In contrast to [51], our study finds that non-contextualised justifications do not significantly improve users' understanding of the app's practices. Therefore, justifications should be meaningful and tailored to the context of a particular app to be truly helpful and increase transparency. The share of our participants who chose to deny permissions were similar to prior work conducted in the wild [57, 58], confirming that the intentions observed in our study are likely to be representative of actual users' decisions (however, future work is needed to validate it). Moreover, we explore users' opinions about permissions that are currently not requested in either regular or MAR apps, yet raise significant concerns (e.g. face and speech recognition). In conclusion, our findings have important contributions and practical implications for MAR app developers and permission system design.

5.1 Users' Understanding of and Expectations about Permissions

With respect to our first research question (RQ1), we found that, overall, based on the list of permissions, participants were confident that they understand what resources and data the MAR app will be able to access. However, participants expressed the willingness to know why the MAR app requires certain permissions, and how it is going to use them. We also find that contextualized justifications can increase users' understanding of the app's data practices compared to using just permission labels and could be a useful tool for increasing app transparency. This is especially true for the new permissions that we suggest to add to cover advanced sensors, resources, and functionalities especially common in MAR apps, currently absent in mobile permission systems (e.g., *Magnetometer*, *LiDAR*, *Geometry Tracking* or *Object Recognition*). In other words, adding contextualized justifications to these permissions resulted in the biggest increase in participants' understanding of the app's data practices, compared to the group where only permission labels were used. Open-ended responses confirmed that participants expressed the need for more clarifications about these advanced or novel sensors and data processing approaches (especially *Magnetometer*, *Geometry Tracking* and *LiDAR*).

Participants believed that refusing to grant certain non-essential permissions (e.g., send notifications) would not impair the app's ability to perform its primary functionalities. In the open-text responses, participants also said that they would like to know whether they can decline some of the permissions. Thus, we recommend to have a clear labeling of which permissions are required and which permissions are optional, and how declining of such permissions would affect the app's functionalities (e.g., if users were to decline the *Notifications* permissions, they would not be able to receive

Table 5: Indices created from variables Q8-Q11 and Cronbach's α

Variable	Index	Permissions	Alpha
Q8: App functioning w/o accessing permission X	1	Storage, network, camera, accelerometer, gyroscope, magnetometer, LiDAR, geometry tracking, raw camera tracking, object recognition	0.8442
	2	Contacts, microphone, location, notifications, face recognition, speech recognition	0.7977
Q9: Privacy dangerousness of permission X	1	Notifications, accelerometer, gyroscope, magnetometer, LiDAR, geometry tracking, raw camera output, object recognition	0.8890
	2	Storage, contacts, network, microphone, camera, location, face recognition, speech recognition	0.8852
Q10: Negative effects on performance of permission X	1	All 16 permissions	0.9438
Q11: Perceived informativeness of permission X	1	Storage, contacts, network, microphone, camera, location, notifications, face recognition, speech recognition	0.8569
	2	Accelerometer, gyroscope, magnetometer, LiDAR, geometry tracking, raw camera output, object recognition	0.8934

notifications about the comments that the designer has left about their measurements in the MAR app).

Similarly, participants did not believe that granting the permissions could negatively affect the device's normal operations. This question was inspired by the Android Developer Guide, which classifies dangerous permissions as those that have an impact on user's privacy and the device's normal operations [2]. As we discuss in Section 5.2, participants expressed privacy concerns about certain permissions, but did not expect a negative impact on device's normal operations. However, it is possible that the assessment of the impact on the device's normal operations may require more advanced technical knowledge than the assessment of privacy implications. Without proper guidance on how to evaluate the impact of permissions on the device's normal operations, it would be hard to decide whether the new permissions, such as *LiDAR* and *Geometry Tracking*, should be categorized as dangerous or not. Thus, we recommend the Android Developer Guide (and other similar documentations) to include more details about the metrics used to make such assessments, and how to reconcile the contradictions between negative impact on user's privacy and no impact on device's normal operations.

5.2 Privacy Concerns about Permissions

Regarding our second research question (RQ2), some permissions (e.g., *Location*, *Contacts*, *Microphone*, *Speech and Face Recognition*) raise substantial privacy concerns among users. Prior work found that users are concerned about access to location and microphone in non-AR apps as well [15, 39, 59]. However, most apps do not request the permissions to use *Speech and Face Recognition*, although users in our study find it concerning. It is possible that participants are especially concerned about *Speech and Face Recognition* due to the general lack of understanding of what information is collected for it, at what point in time, and how it is processed. Media coverage of the privacy invasions by companies relying on face recognition technologies such as Clearview AI [25] could also trigger privacy concerns among our participants.

In contrast, other permissions, such as *Accelerometer*, *Magnetometer*, *Gyroscope*, *Notifications*, *LiDAR*, and *Geometry Tracking*, did not raise high privacy concerns. However, it has been shown that accelerometer data, which is collected by several MAR apps like Pokémon Go, can be used to infer the phone's password [16] or to eavesdrop on the audio output of the device [35]. This findings indicates a gap between users' understanding of the threat models and actual privacy and security risks. This kind of knowledge-concern gap is critical for MAR apps. The variety of sensors required by MAR apps and the technical possibilities to exploit these sensors make it important to inform the users about the potential privacy implications, and request the permissions to access those resources. Clarifications and justifications for the sensors could further help to bridge this gap. The accuracy and informativeness of these justifications should be enforced and monitored, for example, by the app stores and regulators.

We also checked if users' privacy perceptions align with the Android Developer Guide classification of permission dangerousness [2]. We only considered the responses of participants in the Control groups (in both Studies 1 and 2), as currently the permission systems use only the labels, without justifications. We categorized participants' responses based on the median values for the individual permissions into two groups: (1) Dangerous permissions, if they are perceived on average as privacy invasive (median value larger than 4 out of 7), and (2) Non-Dangerous permissions, if they are perceived on average as not privacy invasive or neutral (median value less than or equal to 4 out of 7). The results indicate that the Android's classifications match the participants' evaluations for the currently used permissions. However, it also suggests that if new permissions were added, some of them (such as *Face and Speech Recognition*) would be considered dangerous and would need to be requested in the run time.

5.3 The Impact of Justifications

Regarding the third research question (RQ3), our results indicate that contextualized justifications, which describe what information the app will be able to access and how it will use it if the user grants the permission, improve users' understanding of the app's data practices, and reduce their privacy concerns, but do not impact users' intentions to grant such permissions or download the app. In turn, privacy concerns reduce the intentions to grant the permissions, but not to download the app. This might be due to the fact that users' decisions to download an app are more dependent on other factors, such as app's functionalities and utility. We find that main results are similar in Study 1 and 2, indicating the robustness of the effects against the modifications in the wording of the permission justifications. Thus, we recommend app developers and platforms to include contextualized justifications to the existing permission systems to improve the transparency about MAR apps' data practices. As discussed in Section 5.5, while our study explores the opinions about only one type of MAR apps, future work is encouraged to validate the results with other categories of MAR apps, and different levels of invasiveness of their data practices.

5.4 Suggestions for Improved Transparency

Regarding our fourth research questions (RQ4), we provide a number of recommendations for improved transparency in the permission systems of MAR apps based on all our results. First, we recommend app platforms to require developers to provide justifications for the permissions requested by their apps. Second, we encourage app developers to contextualize those justifications to the specific practices and functionalities of their apps. For example, instead of using vague statements about the app's need to access the *Microphone* in order to transmit audio input, we suggest explaining how it will be used by the app (e.g., to record voice messages).

Third, we recommend requesting user permissions to access the resources and sensors that are commonly used in MAR apps and often raise privacy concerns, but are not currently included in the mobile permission systems, such as *Face and Speech Recognition*. Similarly, as technology advances very fast, we recommend including a short description of the novel functionalities and sensors, such as *LiDAR*, *Geometry Tracking* and *Object Tracking*, avoiding technical terminology that can be hard to understand for the people with limited technological background or experience. We also recommend testing the linguistic complexity of the justifications (e.g., by using the library we used in this study [45]), and the overall comprehension and informativeness of the justifications in user studies.

Fourth, based on the participants' comments, we recommend improving the visual appearance of the permission systems. For instance, we suggest:

- Group the permissions by the type of information they access or by the purpose of use;
- Avoid permission fatigue and allow customisation of the level of detail in permission justifications, for example, by using expandable clarifications text boxes, larger or higher-contrast text for labels and less prominent justification text to allow users to quickly scan the permissions and easily read the additional information where they need more clarifications;
- Include images, videos, or animations to demonstrate how advanced or novel sensors work;
- Make it clear *when* certain functionalities, sensors or data are being accessed;
- Clearly indicate whether a certain permission can be denied or restricted, and how the restrictions of certain permissions can affect the performance of the app;
- Clarify privacy implications of the permissions.

5.5 Limitations and Future Work

Our study has several limitations. First, while our sample is diverse in terms of demographics, it only includes US citizens. Incorporating cultural factors can provide additional insights for privacy-related predictions [33, 53]. In the future work, we would like to expand the diversity of the sample and conduct a cross-country comparison of users' perceptions and understanding of MAR apps' mobile permissions.

Second, to keep high internal validity, we tested only one treatment dimension related to the permission justifications (contextualized and non-contextualized), while keeping other parameters constant. Future work can experiment with other dimensions, such as the number and composition of requested permissions, their relevance or importance to the app's functionalities, purposes of data use (including the purposes that primarily benefit the companies more than users, such as targeted advertising), or visual design of the permission menus.

Finally, we used a hypothetical scenario about a MAR app in our study. However, the use of hypothetical scenario in a controlled experiment allowed us to achieve high internal validity, and future work can test the generalizability and ecological validity of the results in a field experiment. Moreover, the app we used in our scenario can be categorized as a utilitarian app with primarily utilitarian incentives for individuals to use it. In contrast, hedonic (or pleasure and entertainment oriented) MAR apps, such as games, could be judged differently by participants regarding their privacy implications, willingness to grant permissions, or download intentions. Thus, future work can explore the differences in users' opinions and intentions regarding various categories of MAR apps.

Acknowledgments

We thank Julia Bernd, Serge Egelman, other BLUES members, and CLTC Research Symposium participants for their comments on the study design and suggestions about the paper. This work was supported by the Center for Long-Term Cybersecurity at UC Berkeley, and National Science Foundation grants CNS-1514211 and CNS-1528070.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[2] Android Developers. Android Permissions Overview. https://developer.android.com/guide/topics/permissions/overview#permission-groups, 2019.

[3] Corey M. Angst and Ritu Agarwal. Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Ouarterly*, 33(2):339–370, 2009.

[4] Ronald T. Azuma, Yohan Baillot, Steven Feiner, Simon Julier, Reinhold Behringer, and Blair Macintyre. Recent Advances in Augmented Reality. *IEEE Computer Graphics And Applications*, 21(6):34–47, 2001.

[5] Gökhan Bal, Kai Rannenberg, and Jason I. Hong. Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns. *Computers & Security*, 53(September):187–202, sep 2015.

[6] R. Balebako, F. Schaub, I. Adjerid, A. Acquisti, and L. Cranor. The impact of timing on the salience of smartphone app privacy notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 63–74, 2015.

[7] Rochelle A Cadogan. An imbalance of power: the readability of internet privacy policies. *Journal of Business & Economics Research (JBER)*, 2(3), 2011.

[8] Scott G. Dacko. Enabling smart retail settings via mobile augmented reality shopping apps. *Technological Forecasting and Social Change*, 124:243–256, 2017.

[9] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and Privacy Approaches in Mixed Reality: A Literature Survey. 2018.

[10] Dejan G. 29+ Augmented Reality Stats to Keep You Sharp in 2020. https://techjury.net/blog/augmented-reality-stats/, 2020.

[11] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, pages 2377–2386, 2014.

[12] Arindam Dey, Mark Billinghurst, Robert W Lindeman, and J. Edward Swan II. A Systematic Review of Usability Studies in Augmented Reality between 2005 and 2014. In *2016 IEEE International Symposium on Mixed and Augmented Reality (ISMAR-Adjunct)*, pages 49–50, Merida, 2016.

[13] W. Enck, P. Gilbert, B. 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 *9th ACM USENIX Conference on Operating Systems Design and Implementation*, pages 393–407, 2010.

[14] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, David A Wagner, et al. How to ask for permission. *HotSec*, 12:7–7, 2012.

[15] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 1–14, 2012.

[16] Duncan Geere. Scientists find a way to crack your phone's password using just the accelerometer. https://www.techradar.com/uk/news/scientists-find-a-way-to-crack-your-phones-password-using-\just-the-accelerometer, 2017.

[17] Alessandra Gorla, Ilaria Tavecchia, Florian Gross, and Andreas Zeller. Checking app behavior against app descriptions. In *Proceedings of the 36th international conference on software engineering*, pages 1025–1035, 2014.

[18] Jie Gu, Yunjie (Calvin) Xu, Heng Xu, Cheng Zhang, and Hong Ling. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, 94:19–28, 2017.

[19] David Harborth. Augmented Reality in Information Systems Research: A Systematic Literature Review. In *Twenty-third Americas Conference on Information Systems (AMCIS)*, pages 1–10, Boston, 2017.

[20] David Harborth. Unfolding Concerns about Augmented Reality Technologies: A Qualitative Analysis of User Perceptions. In *Wirtschaftsinformatik (WI19)*, pages 1262–1276, 2019.

[21] David Harborth, Majid Hatamian, Welderufael B. Tesfay, and Kai Rannenberg. A Two-Pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality Applications. In *Hawaii International Conference on System Sciences (HICSS) Proceedings*, pages 5029–5038, 2019.

[22] David Harborth and Sebastian Pape. Privacy Concerns and Behavior of Pokémon Go Players in Germany. In M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner, editors, *Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017. IFIP Advances in Information and Communication Technology, vol 526*, pages 314–329. Springer, Cham, 2018.

[23] David Harborth and Sebastian Pape. Investigating Privacy Concerns related to Mobile Augmented Reality Applications. In *International Conference on Information Systems (ICIS)*, pages 1–9, 2019.

[24] Majid Hatamian, Jetzabel Serna, Kai Rannenberg, and Bodo Igler. FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps. In *International Conference On Trust, Privacy & Security In Digital Business (TrustBus 2017)*, pages 1–16, 2017.

[25] Kashmir Hill. The Secretive Company That Might End Privacy as We Know It. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, 2020.

[26] Patrick G. Kelley, Sunny Consolvo, Lorrie F. Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A conundrum of permissions: installing applications on an android smartphone. In *Proceedings of the 26th International Conference on Fin. Cryptography and Data Security*, pages 68–79, 2012.

[27] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. *SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*, pages 3393–3402, 2013.

[28] Vanessa Kohn and David Harborth. Augmented reality – A game changing technology for manufacturing processes? In *Twenty-Sixth European Conference on Information Systems (ECIS2018)*, pages 1–19, Portsmouth, UK, 2018.

[29] Kate Kozuch. Apple Glasses: Release date, price, features and leaks. https://www.tomsguide.com/news/apple-glasses, 2021.

[30] M. Kummer and P. Schulte. When private information settles the bill: Money and privacy in Google's market for smartphone applications. *Management Science*, 65(8):3470–3494, 2019.

[31] Lawrence L Kupper and Kerry B Hafner. On assessing interrater agreement for multiple attribute responses. *Biometrics*, pages 957–967, 1989.

[32] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *2018 IEEE Symposium on Security and Privacy*, pages 392–408, 2018.

[33] Yao Li, Alfred Kobsa, Bart P Knijnenburg, and MH Carolyn Nguyen. Cross-cultural privacy prediction. *Proceedings on Privacy Enhancing Technologies*, 2017(2):113–132, 2017.

[34] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*, pages 501–510, 2012.

[35] Malwarebytes Labs. The little-known ways mobile device sensors can be exploited by cybercriminals. https://blog.malwarebytes.com/iot/2019/12/the-little-known-ways-mobile-device-sensors-can-be-exploited-by-cybercriminals/, 2019.

[36] Rísin McNaney, John Vines, Daniel Roggen, Madeline Balaam, Pengfei Zhang, Ivan Poliakov, and Patrick Olivier. Exploring the Acceptability of Google Glass as an Everyday Assistive Device for People with Parkinson's. In *32nd annual ACM Conference on Human factors in Computing Systems*, pages 2551–2554, 2014.

[37] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L Mazurek, and Jeffrey S Foster. User Interactions and Permission Use on Android. *SIGCHI Conference on Human Factors in Computing Systems (CHI '17)*, pages 362–373, 2017.

[38] Microsoft. Microsoft HoloLens. https://www.microsoft.com/microsoft-hololens/en-us/buy, 2017.

[39] Alexios Mylonas, Marianthi Theoharidou, and Dimitris Gritzalis. Assessing Privacy Risks in Android : A User-Centric Approach. In *International Workshop on Risk Assessment and Risk-driven Testing*, pages 21–37. Springer, Cham, 2013.

[40] Randy Nelson. Pokémon GO Revenue Hits $1.8 Billion on Its Two Year Launch Anniversary. https://sensortower.com/blog/pokemon-go-revenue-year-two, 2018.

[41] Jack Nicas and Cat Zakrzewski. Augmented Reality Gets Boost From Success of 'Pokémon Go'. https://www.wsj.com/articles/augmented-reality-g

ets-boost-from-success-of-pokemon-go-\1468402203, 2016.

[42] Helen Nissenbaum. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford University Press, Palo Alto, 2010.

[43] Victoria Petrock. US Virtual and Augmented Reality Users 2020. https://www.emarketer.com/content/us-virtual-and-augmented-reality-users-2020, 2020.

[44] Robert W Proctor, M Athar Ali, and Kim-Phuong L Vu. Examining usability of web privacy policies. *Intl. Journal of Human–Computer Interaction*, 24(3):307–328, 2008.

[45] Python Software Foundation. textstat 0.7.0. https://pypi.org/project/textstat/, 2021.

[46] Philipp A. Rauschnabel, Jun He, and Young K. Ro. Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research*, 92:374–384, 2018.

[47] Lisa Rosenfeld, John Torous, and Ipsit V Vahia. Data security and privacy in apps for dementia: an analysis of existing privacy policies. *The American Journal of Geriatric Psychiatry*, 25(8):873–877, 2017.

[48] Craig Van. Slyke, Richard Johnson, James Jiang, and J.T. Shim. Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, 7(6):415–444, 2006.

[49] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22(e1):e28–e33, 2015.

[50] Benedikt Szmrecsanyi. An informationtheoretic approach to assess linguistic complexity. *Complexity, isolation, and variation*, 57:71, 2016.

[51] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*, pages 91–100, 2014.

[52] Kaitlyn Tiffany. It's cool to look terrifying on pandemic instagram. https://www.theatlantic.com/technology/archive/2020/05/augmented-reality-instagram-zoom/611494/, 2020.

[53] Sabine Trepte, Leonard Reinecke, Nicole B Ellison, Oliver Quiring, Mike Z Yao, and Marc Ziegele. A cross-cultural perspective on the privacy calculus. *Social Media + Society*, 3(1):2056305116688035, 2017.

[54] Erik van der Meulen, Marina-Anca Cidotã, Stephan G Lukosch, Paulina J M Bank, Aadjan J C van der Helm, and Valentijn T Visch. A Haptic Serious Augmented Reality Game for Motor Assessment of Parkinson's Disease Patients. In Eduardo E Veas, Tobias Langlotz, José Martinez-Carranza, Raphaël Grasset, Maki Sugimoto, and Alejandro Martin, editors, *International Symposium on Mixed and Augmented Reality, ISMAR 2016 Adjunct*, pages 102–104. IEEE, 2016.

[55] Tiffany M Walsh and Teresa A Volsko. Readability assessment of internet-based consumer health information. *Respiratory Care*, 53(10):1310–1315, 2008.

[56] Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. Permission evolution in the android ecosystem. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 31–40, 2012.

[57] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. Android Permissions Remystified: A Field Study on Contextual Integrity. In *Proceedings of the 24th USENIX Security Symposium*, 2015.

[58] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy*, pages 1077–1093. IEEE, 2017.

[59] Yixin Zhang and Ryan Gilbert Garcia. Do users really care about privacy? Mobile applications' popularity, user satisfaction, and permission requests. In *Twenty-Eight European Conference on Information Systems (ECIS2020)*, 2020.

All websites were last accessed January 11, 2021.

A Questionnaires

All questions are the same in both studies, except: Q4-6 are included only in Study 1, Q20 are included only in Study 2.

Part I. AR Knowledge

Q1. What is the definition of Augmented Reality? *[if answered incorrectly, participants get the correct definition of AR]* 1. Augmented Reality is the perception of a completely virtual environment in which the user is fully immersed. 2. Augmented Reality is the real environment enhanced by virtual information and objects in which the user is able to perceive the real environment. 3. Augmented Reality combines controlled steering of laser beams with a laser rangefinder in order to measure surfaces or bodies to generate a picture.

Q2. Some mobile applications (apps) have Augmented Reality features, which augment the real environment by virtual information and objects, like photo masks. These features may be required for the app to function (e.g. an AR game which is impossible to play without using AR features), or may be optional (e.g. a photo filter in a messaging app). What Augmented Reality features do you use in the apps installed on your phone? Choose all that apply: 1. Photo masks which add digital objects to the photo (e.g. bunny ears to your face, stars, special effects). 2. Digital representations of objects in real environments (e.g. furniture added into existing view of a room). 3. Displaying digital game characters and game worlds' objects in the real environments (e.g. Pokémon Go's). 4. Other (please specify).

AC1. Please choose the answer option 'always' here. (1. Never. 2. Sometimes. 3. About half of the time. 4. Most of the time. 5. Always.)

Part II. Permission Overview

We would appreciate your feedback on an Augmented Reality app that we are developing for mobile devices. Please read the description of the app carefully before answering the following questions.

The new 'Measure it! Augmented Reality App' allows you to redesign a room or outdoor space. Using Augmented Reality it can take and save measurements, or try out new furniture by displaying its 3D models over the image of the real environment. Plus, with just a few clicks, you can easily share the new design ideas and measurements with friends, family, your designer, or contractors, via email or in social networks! The app requires access to the following functionalities and data on your device: (See the list of permissions in Appendix B and Table 3.)

Q3. Based on the list of permissions above, to what extent do you understand what functionalities and data on your device the app will be able to use? (7pt Likert scale from "I don't understand at all" to "I fully understand")

Q4.* What additional information would help you to understand what functionalities and data on your device the app will be able to use? (open text)

Q5.* What other functionalities of your device do you think the app may be using that are not included in the listed permissions? (open text)

Q6.* What other data do you think the app may be using that are not included in the listed permissions? (open text)

Part III. Evaluating Individual Permissions

AC2. This question is not part of the survey and just helps us to detect bots and automated scripts. To confirm that you are a human, please choose 'strongly agree' here. (7pt Likert scale from "Strongly disagree" to "Strongly agree")

The following questions are iterated for each permission. Imagine that you received the following notification on your phone: "The app Measure it! Augmented Reality needs to access [permission] on your device."

Q7. Would you allow or deny the app to access your device's [permission]? 1. Deny. 2. Allow while app is in foreground. 3. Allow. 4. I'm not sure (if this is selected: "Under what circumstances would you allow or deny this permission?").

Q8. How well do you think the app can function without accessing [permission] on your device? (Consider that 1 star is when the app cannot function without it at all, and 7 starts is when the app can function perfectly without it.)

Q9. To what extent do you think that granting permission to access [permission] on your device can potentially affect your privacy? (7pt Likert scale from "No effect" to "Very big effect")

Q10. To what extent do you think that granting permission to access [permission] on your device can potentially affect your device's normal operations (i.e. performance)? (7pt Likert scale from "No effect" to "Very big effect")

Q11. To what extent do you understand what functionalities and data the app will be able to use, if you allow it to access [permission] on your device? (7pt Likert scale from "I don't understand at all" to "I fully understand")

Q20.* How likely are you to download this app? (7pt Likert scale from "Extremely unlikely" to "Extremely likely").

Part IV. Demographics

Q12. What is your gender? 1. Male. 2. Female. 3. Prefer to self-identify. 4. Prefer not to say.

Q13. What is your age? (numeric entry field)

Q14. What is your country of residence (US or other)

Q15. What is the highest level of school you have completed or the highest degree you have received? 1. Less than high school degree. 2. High school graduate (high school diploma or equivalent including GED). 3. Some college but no degree. 4. Associate degree in college (2-year). 5. Bachelor's degree in college (4-year). 6. Master's degree. 7. Doctoral degree. 8. Professional degree (JD, MD).

Q16. Do you have experience in any of the following (choose all that apply)? 1. Computer science education / work experience2. 2. Software engineering education / work experience. 3. App development education / work experience. 4. Other technical education / work experience (please specify). 5. None of the above.

Q17. How often do you use a smartphone? (from "Never" to "Once or several times a day")

Q18. Which operating system do you use on your smartphone? (Android, iOS, other)

Q19. Do you have any feedback regarding the questionnaire or the study? (open text)

B Permissions and Justifications (Study 1)

Table 6: Permission labels and justifications in Study 1.

Label	Non-Contextualized justification	Contextualized justification
Storage / Photos / Media Library	Access to the smartphone's storage is required to store data processed by the app.	Access to the smartphone's storage is required to browse and edit (save, erase) the photographs of the taken measurements.
Contacts	Access to the contacts is required to enable social features of the app.	Access to the contacts is required to share photos of the measurements with the contacts via email or messages (for example, with your designer, contractors, partner, or friends).
Network / Internet Access	Internet access is required to connect the app with the Internet.	Internet access is required to share your measurement photos via email, messengers, or in social networks (for example, with your designer, clients, contractors, partner, or friends).
Microphone	Access to the microphone is required to record audio.	Access to the microphone is required to add voice notes to your measurement photos.
Camera	Access to the camera is required to take pictures and videos.	Access to the camera is required to take photos and videos of the environments you are measuring. These photos and videos allow the app to visualize your furniture and other objects in those environments.
Location services	Access to location information is required to detect the approximate position (based on network data) and precise position (based on GPS and network data) of the device.	Access to location information is required to link your measurement photos to location data. This information allows the app to automatically create albums in your gallery based on location, which makes it easier to navigate through your measurements.
Notifications	Access to notifications is required to notify you about messages.	Access to notifications is required to notify you when new messages or comments about measurements or furniture ideas are received from your contacts (e.g., designer, clients, contractors, partner, or friends).
Accelerometer	Access to the accelerometer is required to measure the acceleration of your smartphone movements.	Access to the accelerometer is required to provide image stabilization based on the speed your phone is moving, which improves the quality of your measurement photos.
Gyroscope	Access to the gyroscope is required to measure the rotation of the smartphone.	Access to the gyroscope is required to provide image stabilization based on the position of your device and the vibrations of your hands.
Magnetometer	Access to the magnetometer is required to measure magnetic fields.	Access to the magnetometer is required to detect nearby magnetic fields, which can reduce the accuracy and quality of your measurement photos.
LiDAR Scanner	Access to the LiDAR scanner is required to use light to measure distances.	Access to the LiDAR scanner is required to provide detailed 3D measurements of your environment. This allows the app to more accurately represent the location of furniture and other objects.
Geometry Tracking	Allowing the app to use geometry tracking is required to generate a geometrical schematic outline of the environment.	Allowing the app to use geometry tracking is required to generate a geometrical schematic outline of the environment for measuring distances between objects, instead of using the raw camera output of that environment (i.e. real views of the environments, such as rooms, or outdoor spaces and objects in them).
Raw Camera Output	Allowing the app to use the raw camera output is required to gather and process the raw output of the camera while you use the app.	Allowing the app to use the raw camera output is required to present you with a realistic presentation of the pieces of furniture in the real environment, instead of just a geometrical schematic outline.
Object Recognition	Allowing the app to use object recognition is required to recognize details of the objects in the environments.	Allowing the app to use object recognition is required to identify objects in your environment (e.g. the existing furniture in the room). This allows the app to remove or substitute those objects with augmented reality objects, such as viewing how a new couch would fit in the room, or whether new chairs would fit with the existing table.
Face Recognition	Allowing the app to use face recognition is required to identify or verify the identities of people using their face.	Allowing the app to use face recognition is required to verify the identity of people in your measurement photos. This allows the app to automatically identify people in your device's contacts list if they appear in your measurement photos, so that you can easily share among people in the environment for easy sharing of the measurements and furniture ideas.
Speech Recognition	Allowing the app to use speech recognition is required to identify words and phrases in spoken language and convert them to a machine-readable format.	Allowing the app to use speech recognition is required to transcribe voice notes into text for the taken measurements or furniture ideas.

C Regression Analyses, Factor Analysis

Table 7: Random-effects ordered logistic regression models on the willingness to grant permissions in Study 1.

	(1) Base Model	(2) With Controls	(3) With Qual. Vars
Dependent variable: Would you allow or deny the app to access your device's permission X? (Q7)			
Contextualized Justifications experimental group (control group is omitted)	0.190	0.166	0.268
	(0.95)	(0.85)	(1.14)
Non-Contextualized Justifications experimental group	0.175	0.211	0.259
	(0.83)	(1.03)	(1.19)
Q8: App functioning w/o accessing permission X	**-0.567*** **	**-0.567*** **	**-0.566*** **
	(-12.40)	(-12.40)	(-12.38)
Q9: Privacy dangerousness of permission X	**-0.396*** **	**-0.396*** **	**-0.397*** **
	(-12.03)	(-12.01)	(-12.00)
Q10: Negative effects on performance of permission X	0.038	0.041	0.040
	(0.87)	(0.94)	(0.92)
Q11: Perceived informativeness of permission X	**0.218*** **	**0.218*** **	**0.219*** **
	(5.33)	(5.30)	(5.32)
Q3: General app understanding	0.011	-0.006	0.004
	(0.15)	(-0.08)	(0.06)
Q1: Definition of AR correct		-0.120	-0.080
		(-0.66)	(-0.44)
Q2: AR features on smartphones used		0.475*	0.526*
		(2.13)	(2.40)
Q12_1: Gender - male ("female" is omitted)		0.084	0.061
		(0.47)	(0.34)
Q12_2: Gender (prefer to self-identify)		-0.162	-0.193
		(-0.36)	(-0.42)
Q13: Age		0.001	-0.000
		(0.09)	(-0.01)
Q15: Education		-0.119*	-0.118*
		(-2.12)	(-2.13)
Q16: Technically experienced		-0.033	-0.047
		(-0.17)	(-0.24)
Q17: Smartphone used once or several times a day		-0.626	-0.743
		(-0.67)	(-0.81)
Q18: Mobile OS (1=Android)		0.073	0.130
		(0.41)	(0.74)
Q4_1: Why and how data is used			-0.169
			(-0.86)
Q4_2: No information needed / clear what the permission(s) is and does			-0.249
			(-1.07)
Q4_3: Clarification about sensors / features needed			0.112
			(0.57)
Q4_4: Possibility to deny / restrict individual permissions			**-0.828*** **
			(-3.59)
Q4_5: When data is collected			0.257
			(0.72)

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; t statistics in parentheses. **Values in bold font indicate statistical significance that hold after applying Holm's and Hochberg corrections.**

Table 8: Random-effects ordered logistic regression models on the willingness to grant permissions in Study 2.

	(1) Base Model	(2) With Controls
Dependent variable: Would you allow or deny the app to access your device's permission X? (Q7)		
Contextualized Justifications experimental group (control group is omitted)	0.077	0.023
	(0.37)	(0.11)
Non-Contextualized Justifications experimental group	-0.064	-0.125
	(-0.28)	(-0.55)
Q8: App functioning w/o accessing permission X	**-0.504*** **	**-0.504*** **
	(-12.21)	(-12.21)
Q9: Privacy dangerousness of permission X	**-0.400*** **	**-0.399*** **
	(-10.86)	(-10.88)
Q10: Negative effects on performance of permission X	0.012	0.008
	(0.27)	(0.17)
Q11: Perceived informativeness of permission X	**0.140*** **	**0.140*** **
	(3.80)	(3.80)
Q3: General app understanding	**0.210** **	0.191**
	(3.01)	(2.76)
Q1: Definition of AR correct		-0.359
		(-1.73)
Q2: AR features on smartphones used		0.353
		(1.73)
Q12_1: Gender - male ("female" is omitted)		0.084
		(0.42)
Q12_2: Gender (prefer to self-identify)		**-1.118** **
		(-3.43)
Q13: Age		-0.005
		(-0.53)
Q15: Education		0.072
		(0.94)
Q16: Technically experienced		-0.170
		(-0.83)
Q17: Smartphone used once or several times a day		**-1.234*** **
		(-3.92)
Q18: Mobile OS (1=Android)		-0.398*
		(-2.21)

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; t statistics in parentheses. **Values in bold font indicate statistical significance that hold after applying Holm's and Hochberg corrections.**

Table 9: Ordered logistic regression models on intentions to download the app in Study 2.

	(1) Base Model	(2) With Controls
Dependent variable: How likely are you to download this app? (Q20)		
Contextualized Justifications experimental group (control group is omitted)	0.070	-0.048
	(0.26)	(-0.17)
Non-Contextualized Justifications experimental group	0.134	0.025
	(0.49)	(0.08)
Q8: App functioning w/o accessing permission X		
Index 1	0.038	0.067
	(0.55)	(0.97)
Index 2	-0.113	-0.121
	(-1.36)	(-1.47)
Q9: Privacy dangerousness of permission X		
Index 1	-0.121	-0.122
	(-1.26)	(-1.24)
Index 2	**-0.213****	-0.198*
	(-2.88)	(-2.49)
Q10: Negative effects on performance of permission X		
Index	0.001	-0.053
	(0.01)	(-0.46)
Q11: Perceived informativeness of permission X in understanding app functions and data use		
Index 1	0.081	0.074
	(0.90)	(0.81)
Index 2	0.106	0.098
	(1.34)	(1.18)
Q3: General app understanding	**0.401****	**0.431****
	(3.08)	(3.19)
Q1: Definition of AR correct		-0.360
		(-1.31)
Q2: AR features on smartphones used		0.569*
		(2.18)
Gender - male ("female" is omitted)		0.011
		(0.04)
Gender (prefer to self-identify)		-0.973
		(-1.69)
Q13: Age		0.001
		(0.12)
Q15: Education		0.174*
		(2.00)
Q16: Technically experienced		-0.110
		(-0.42)
Q18: Mobile OS (1=Android)		-0.085
		(-0.37)

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; t statistics in parentheses. **Values in bold font indicate statistical significance that hold after applying Holm's and Hochberg corrections.**

D Codebook

Table 10: Codebook for the additional information that participants thought would help them understand what functionalities and data on their device the app will be able to use in Study 1.

Code	Description
No information needed (Q4_2)	Participants do not need additional information, the given information given is clear or sufficient.
N/a	Participants do not offer to add any information (but they do not say the provided information is sufficient like in the "No information needed" code.
General app's functionalities	Functionalities of the apps, not related to privacy/security, e.g. how does the app measure distance, where does the furniture come from, etc.
Instructions	Manual, instructions, help page, FAQ, tutorial
Resources used by the app	Data usage, memory
Clarification about sensors / features (Q4_3)	Definitions of terms, explanations of what the sensors and features are. Indicates insufficient information (when participants provide more details about what kind of information they need to know, e.g. when they require the clarification of how the data collected by these sensors is used, it is "Why/how data is used (purpose)" code).
Possibility to deny/ restrict individual permissions (Q4_4)	Is it possible to deny individual permissions; are the permissions optional/mandatory.
Impact on functionality	How denial of access permissions would affect the functionality (Note: comments about the general app's functionalities are in the "General app's functionalities" code).
Privacy Policies / Terms of services	Privacy policy, terms of services. Includes Privacy Rating / Privacy Ranking.
Privacy concerns (explicit)	Not comfortable with giving access to certain things.
(General) Data handling information	Participants want to know what will happen to the data without specifying whether they are interested in processing, storage, or use conditions.
What data is collected	What specific piece of information are collected.
When data is collected/accessed (Q4_5)	When the data is collected or accessed; common example – while app not in use or all the time.
Where/how data is stored	How data is stored, how long, where it is stored, is it stored at all.
Why/how data is used (Q4_1)	Purpose for data collection, how it is used, how it is processed. Is this data actually required, or is it optional.
How data is shared	Whether the data is going to be shared and with whom (e.g. marketers are mentioned a few times). Specifically, whether the data is going to be sold to the third parties is mentioned often.
How security of my data is ensured	Is the app going to make sure the collected data is secure, and if so how. What security and privacy mechanisms (e.g. anonymization) do they use.
Brief / shorter	When participants mention that the want a short/brief description, or when they want the description to be shorter (note: separate code for "Simpler").
Simpler	Too much detail, or too technical/difficult/jargon-y language. When participants wish the description to be simpler.
Visual	Visual representation, demo, images, video, etc.
One of the specific permissions	Whenever this specific functionality is mentioned (e.g. LiDAR).