Evaluating and Redefining the Permissions for Mobile Augmented Reality Apps

David Harborth
Goethe University Frankfurt
Frankfurt am Main, Germany
david.harborth@m-chair.de

Alisa Frik
International Computer Science Institute, UC Berkeley
Berkeley, USA
afrik@icsi.berkeley.edu

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. AR is highly dependent on real time context-specific information provided by advanced sensors and machine learning techniques (e.g. object recognition, LiDAR). This dependency raises crucial privacy issues for end users. In an online experiment with 292 participants, we evaluate whether the existing access permission systems initially developed for non-AR apps and new AR-relevant permissions provide sufficient and clear information to the users. Based on the results, we suggest improvements in the access permissions for AR apps.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing** → *Empirical studies in ubiquitous and mobile computing*; Smartphones.

KEYWORDS

augmented reality apps, usability, online experiment

ACM Reference Format:
David Harborth and Alisa Frik. 2020. Evaluating and Redefining the Permissions for Mobile Augmented Reality Apps. In *CLTC Research Symposium'20, September 11, 2020, Berkeley, CA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The release of Pokémon Go Pokémon Go in 2016 increased public awareness about augmented reality (AR) [31]. 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" [2, p.34]. The AR market in general was worth $1.8 billion in 2018, $3.5 billion in 2019 and an expected increase in value to $18 billion in 2023 [8]. Recent reports on AR users report that there were 72.8 million people in the US who used AR at least once a month on any kind of device. This number is projected to increase to 83.1 million people in the US (representing 25.3% of the whole US population) [33].

Currently, the two most popular types of AR are smart glasses and mobile AR (MAR) apps. AR glasses such as the Microsoft Hololens [29] are currently not 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 saves time and money [22]. In contrast, MAR apps and AR features within regular mobile apps are currently widely available and used within the smartphone ecosystem. The most famous example is the aforementioned MAR game Pokémon Go , which is one of the most successful apps ever introduced with $1.8 billion in revenue after two years in the market [30]. However, there are also other regular apps like Snapchat or Instagram which integrate AR filters in their services which gained a lot of attention during the Covid-19 pandemic in which many users tried to escape their quarantine by augmenting all kinds of digital objects in their environment and on their bodies [40].

This paper focuses on the end user privacy issues related to MAR apps. MAR apps require massive amounts of data from a variety of sensors in order to create an interactive user interaction with a real time alignment of digital objects with the real environment), which is then processed using data-intensive machine learning and artificial intelligence algorithms (e.g. for object recognition, and geometry tracking).

Literature identified five major differences between MAR apps and non-MAR apps that amplify the privacy risks for MAR apps' users [7, 17]:

(1) due to heavy reliance on the camera input but limited feedback regarding what data is captured by the camera, the user cannot know what is captured by the MAR app.
(2) malicious apps could alter the digital objects and information presented to the user.
(3) Increasing data aggregation capabilities of MAR apps due to simultaneous deployment of multiple privacy-invasive sensors (e.g. location, visual/camera, accelerometer data, etc.), and the opacity of potential inferences and risks associated with such aggregation.
(4) Risks related privacy breaches in collaborative and shared AR environments when two or more users work with separate AR devices on the same digital objects [25].
(5) Risks for bystanders of AR systems who are in the field of view and get filmed by the systems without awareness or possibility to control [9].

Therefore, users of MAR apps are exposed to more severe and novel types of privacy risks compared to the ones related to regular

CLTC Research Symposium'20, September 11, 2020, Berkeley, CA

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

(non-MAR) smartphones apps. However, there is a lack of user studies investigating AR related privacy concerns of users [10, 15].

Although in general data flows in the apps are not transparent to the users [3, 11, 18], a few most common ways in which app's data collection practices are revealed to the user is through the permission systems and privacy policies. Not all apps provide privacy policies [36, 37], and even when they do, they are hard to understand for non-expert users which decreases the likelihood that they read the policies [5, 34]. Thus permissions remain an integral and mandatory element of the user interaction with the app. Yet, not the most effectively designed [13, 20, 42]. Therefore, we decided to start our analysis of MAR users' privacy concerns with an investigation of their opinions about permission systems.

Our study addresses the following research questions:

(1) To what extent is the information provided in access permissions sufficient for the users to understand what data is accessed by a MAR app?
(2) How could the transparency of access permissions in MAR apps be improved?

The remainder of the paper is structured as follows. We describe related work on permissions in the smartphone ecosystem and user privacy in AR technologies in Section 2. We consequently present our method in Section 3 followed by the results in Section 4. Section 5 provides a discussion of the results in light of the research questions, presents the limitations of our study and future work opportunities. We conclude this paper by highlighting the key findings and implications in Section 6.

2 RELATED WORK

There are two main streams of literature relevant to our research agenda. The first one deals with user privacy concerns regarding mobile permissions, and the second one with user privacy concerns regarding Augmented Reality (AR) technologies.

2.1 User privacy concerns with mobile permissions

There is a plethora of research on mobile permissions and privacy-related user perceptions about them [4, 12, 21, 28, 43]. A number of studies investigate the specific factors that affect users' concerns with mobile permissions, such as justification of the purpose of data collection, and how sensitive is the requested data, or how dangerous are the permissions. For instance, while making permissions of an app clear and apparent helps users become aware of these permissions, users also want to better understand why applications need certain information [21]. Users' expectations regarding the reason why sensitive resources are used have a major impact on users' trust. At the same time users find it hard to identify the reasons why an app uses a specific resource [27].

Thus, users' privacy concerns regarding access permissions are alleviated by the presence of permission justifications (explaining users why apps need certain permissions) [14]. However, there is also contrasting research showing that meaningless justifications can also alleviate concerns [39]. Thus, great attention should be paid to the accuracy of purpose description to avoid user deception.

On the other hand, when apps require more sensitive permissions [14], privacy concerns increase [14] and the demand (number of ratings and installations) for such apps decreases [23].

2.2 User privacy concerns with AR technologies

There is a body of technical research about privacy and security in augmented reality technologies [7]. However, there is little research on end users' perceptions and privacy concerns regarding AR technologies, especially, among research focused on mobile AR [15]. The limited empirical evidence suggests that AR raises privacy concerns among users, for instance, about being filmed by AR devices (as bystanders [9]), distributing data involuntarily and being surveilled due to using the devices [6, 16, 35]. Research on privacy for AR technologies is especially important since context-specific privacy concerns can differ greatly from general privacy concerns [1, 32].

Specific research on permissions of a selection of the 19 most downloaded MAR apps of the 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 features [17].

While prior research has investigated users' 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, and the impact of permission justifications on users' concerns and intentions to grant permissions to such apps. In this study, we attempt at closing this gap.

3 METHOD

To answer the research questions, we designed an online survey-based experiment, approved by the university's ethics board, with 3 conditions in which we presented participants with a scenario describing a fictional MAR app that can help to redesign a room or outdoor space. We told participants that using augmented reality (AR) the app can take and save measurements, or try out new furniture by displaying its 3D models over the image of the real environment; also, users can share the new design ideas and measurements with friends, family, designer, or contractors, via email or in social networks. Then we presented participants with a list of permissions this app requires. While permissions were the same across the experimental conditions, we modified the explanatory text providing justification for requesting each of the permissions. In the *Control* group, participants were presented only with the labels of the permissions without any justification (e.g. Microphone, Contacts). In the *Helpful Justification* condition (HJ), along with the label, we showed participants a justification explaining why the app requires access to a specific device functionality that was designed to help users understand the purpose of data collection. For example, the "helpful justification" for the *Microphone* permission mentioned that access to the microphone is required to add voice notes to the measurement photos. In the *Non-Helpful Justification* condition (NHJ), the explanation didn't contain meaningful information on how the requested permission is related to the app's

functionalities and data collection needs. For example, the "non-helpful justification" for the Microphone permission mentioned that access to the microphone is required to record audio (see the permission justification text in Appendix A)

We included seven 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. Additionally, we included nine categories of resources and functionalities that are more specific to and are often used in MAR apps, but are not explicitly requesting 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 functionalities as permissions.

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

3.1 Quantitative analysis

For the regressions analysis, we used an ordered random-effects logistic models 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 the control variables based five most relevant codes from the qualitative analysis. These five variables are binary and equal 1 if the respective participant mentioned the code.

We estimated the marginal effects for each model specification against a predefined outcome to interpret the regression coefficients as the change in percentage points following a one unit increase (or the discrete change from the base level for categorical levels like gender or the experimental group) in the independent variable, i.e. the likelihood of having a predefined outcome (e.g. deny, allow while in foreground or allow).

We also 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 test to assess the differences between the treatment groups.

3.2 Qualitative analysis

To analyze the open-text responses from the survey we used thematic analysis. Two coders independently developed initial codebooks, merged them, discussed and agreed on the final codebook (cf. Appendix C). Then they independently applied the codes to all the responses, allowing for multiple attributes per response. Kupper-Hafner interrater agreement rate is 0.84 [24]. Finally, the coders discussed and resolved all the disagreements.

3.3 Participants

We recruited 300 participants using Prolific crowdsourcing platform. We restricted participation to US residents, over 18 years old, who use mobile devices on regular basis, and have approval rate 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 3 groups: Control (N = 96), Helpful Justifications, HJ (N = 104) and Non-Helpful Justifications, NHJ (N = 92).

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 that there is no difference in age, gender, and education among 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).

4 RESULTS

The majority of participants (86.30%) agreed that based on the provided list of permissions they understand what functionalities and data the app will be able to use (Q3, appendix A). Only 5.82% said they do not understand and 7.88% are not sure. On average, people in HJ 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 than in the control group (Wilcoxon rank sum test: $p = 0.0012$). Next, we will describe the responses regarding the individual permissions.

To understand the relative impact of different factors on users' intentions to allow or deny permissions, we used the regression analysis (Table 3 in Appendix B). Participants are less likely to allow the permission when they believe it will negatively affect the app's ability to function (Q8) and when they are concerned about the impact of granting the permission on their privacy (Q9). Similarly, participants who expressed in open-text comment (Q4) their interest to know whether they can deny or restrict individual permissions based . Participants' understanding of what functionalities and data the app will be able to access if the permission is granted (Q11) positively affected their willingness to grant that permission.

Participants who use AR features on their device are more likely to allow the permissions, and more educated participants are less likely to allow the permissions.

Other controls like, familiarity with the definition of AR, gender, age, prior technical experience, smartphone use frequency and mobile OS don't have an effect on the DV.

4.1 Analysis of Individual Permissions

Most participants tend to allow the permissions (Q7) while the app is in foreground and only few participants would allow the permissions at all times (Figure 1). A few permissions such as *Contacts*, *Microphone* and *Face Recognition* are likely to be denied by the majority of participants.

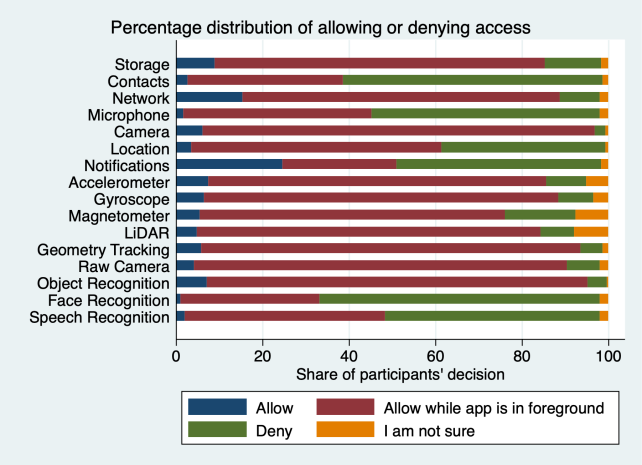

Figure 1: Share of participants who allow, allow while in foreground, deny or are not sure about granting access for permissions.

Based on the regression results, we estimated the probabilities for each individual permission to be allowed at all times, while in foreground, or denied (Table 1). Participants tend 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*.

A Kruskal-Wallis equality-of-populations rank test and regression analysis showed no treatment effects. In other words, there are no statistically significant differences in willingness to grant the permissions between the control and treatment groups.

Participants perceived that permissions allowing access to *Face Recognition*, *Contacts*, *Location Services*, *Microphone*, *Storage* and *Speech Recognition* have the biggest negative impact on their privacy (Figure 2). In contrast, *Magnetometer*, *Accelerometer* and *Gyroscope* are perceived as least privacy invasive.

4.2 Qualitative Results

Table **??** and Table 2 summarise the most common themes from the qualitative analysis of responses about additional information that participants thought would help them understand what functionalities and data on their device the app will be able to use (Q4). Many participants, especially in the treatment groups where justifications were provided, said they don't need any additional

Table 1: Estimated probabilities to deny (1), allow while in foreground (2) and allow at all times (3) the permission accesses based on the random-effects ordered logistic regression model

Permissions	Pr_{deny}	$Pr_{foreground}$	Pr_{always}
Storage /...	.239	**.707**	.054
Contacts	**.453**	**.530**	.017
Network /...	.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 ...	.166	**.750**	.084
Object Recog.	.128	**.759**	.113
Face Recog.	**.506**	**.481**	.013
Speech Recog.	**.433**	**.548**	.019
Total	.257	**.675**	.068

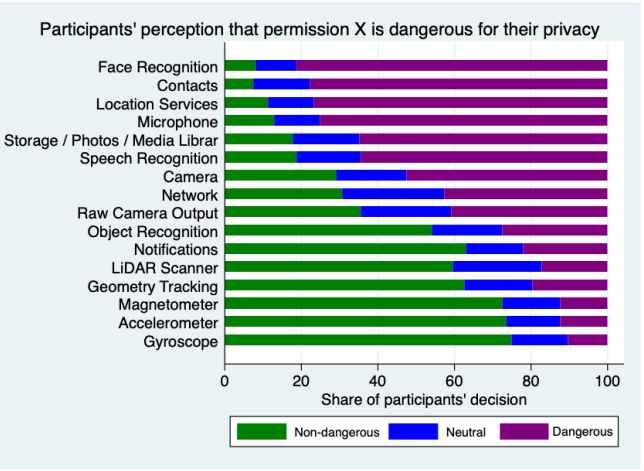

Figure 2: Participants' perceived privacy concerns related to the tested permissions. The three categories are generated by summarizing the answers on the 7-point likert scale (non-dangerous: 1-3, neutral: 4, dangerous: 5-7).

information as permission descriptions were clear enough ($N = 74$). However, many other participants said they would like to know why the permission is needed and how the data is going to be used ($N = 86$), or requested general clarifications about sensors and features ($N = 42$). Some participants specifically mentioned that they would like the clarifications be concise ($N = 17$), or recommended improving visual representations helping them to understand sensors or features, for example, 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 ($N = 18$) and when the specific data is collected and accessed ($N = 13$).

Table 2: Most common codes of the qualitative analysis and results of the one-way ANOVA tests checking for differences for the most relevant codes between three groups

Code	Count	ANOVA results
Why/how data is used (purpose)	86	F(2)=22.44, p < 0.001
No information needed	74	F(2)=8.35, p < 0.001
N/a	46	-
Clarification about sensors / features	42	F(2)=3.30, p < 0.05
Possibility to deny/restrict individual permissions	18	F(2)=7.97, p < 0.001
Brief / shorter	17	F(2)=8.13, p < 0.001
When data is collected/accessed	13	-
Visual	11	-
Codes related to sensors / features		
Microphone	19	-
Face recognition	19	-
LiDAR	18	-
Contacts	16	-
Location	10	-
Speech recognition	10	-

ANOVA test results indicate that more participants said they don't need additional information in the HJ group ($p = 0.000$) and Non-HJ group ($p = 0.007$) compared to the control group. Similarly, the clarifications about sensors or features were significantly less often requested in the the HJ group ($p = 0.023$) and Non-HJ group ($p = 0.031$) than in the control group. Participants in the HJ group were more often interested to know whether they can deny individual permissions than people in the control and Non-HJ groups ($p = 0.000$). Participants in the control group requested information about the purpose of data collection more often than in the HJ ($p = 0.000$) and Non-HJ groups ($p = 0.002$), and they requested this information in Non-HJ group more often than in HJ group. This result suggests that justifications, especially the meaningful ones, are effective in addressing this issue.

5 DISCUSSION

We introduced two research questions in the beginning of this article which we will discuss in this section. First, we address the question to what extent the information provided in access permissions is sufficient for the users to understand what data is accessed by a MAR app. We found that app understanding is relatively high across the experimental groups (mean=5.579 out of 7). However, we also found that functionalities like geometry tracking or LiDAR need more clarifications about how the app is using them and why the app needs them in order to be properly understood by users. While commonly used in MAR apps, user's permission to access these functionalities is not requested in the current mobile permission systems. Moreover, some permissions, and especially face recognition, raise privacy concerns among users. It could be related to the general lack of understanding of what information is collected for face recognition, and at what point in time. It could also be related to the general privacy concerns emerging due to the media coverage on companies relying on face recognition technologies such as Clearview AI [19].

The second research questions deals with possible improvements in the transparency of access permissions in MAR apps. The insights from the quantitative and qualitative part show that helpful justifications can increase understanding and could be a useful tool for increasing transparency. This is especially true for complex permissions like those eventually needed for MAR apps. More importantly, our results indicate that such information can have an impact on the intentions to grant permissions.

Based on our results, we recommend requesting user permissions to access the functionalities 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. As technology develops very fast, we recommend including a short description of the novel functionalities and sensors, such as LiDAR, geometry and object tracking, face and speech recognition, avoiding the technical terminology that can be hard to understand for the people with limited technological background or experience. Based on the participants' comments, we also recommend improving the visual appearance of the permission systems. For instance, we suggest 1) grouping the permissions by the type of information they access or by the purpose of use, 2) including images, videos, or animations to demonstrate how certain sensors work, 3) making it clear when a certain functionality, sensor or data being accessed, and 4) clearly indicating whether a certain permission can be denied, how it can restricted, and how the restrictions of certain permissions can affect the performance of the app.

5.1 Limitations and Future Work

Our study has three main limitations. First, the sample only includes US citizens. Prior work shows that incorporating cultural factors can provide additional insights for privacy-related predictions [26, 41]. 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, we tested only one treatment dimension related to the permission justifications (helpful and non-helpful). Future work can experiment with other dimensions, such as the number and composition of requested permissions.

The third limitation relates to the wording and complexity of the chosen permission justifications. Some differences (or unexpected similarities) between the effects of helpful and non-helpful justifications might be due to the fact that our chosen formulations differs in their linguistic complexity [38]. For example, this might cause participants to perceive non-helpful justifications as "easier" to understand and, therefore, as more helpful compared to the helpful justifications (which could possibly be harder to read). Thus, future work should evaluate the linguistic complexity of the chosen justifications, and experiment with the wording to provide practical suggestions regarding most effective way to communicate

the purpose of accessing a certain functionality or data on a user's device.

6 CONCLUSIONS

We conducted an online survey-based experiment with 292 participants to investigate how permission systems for the mobile Augmented Reality apps can be improved. Our results show that a set of permissions for a hypothetical MAR app consisting of seven existing and nine new permissions overall provides an acceptable level of understanding about what functionalities and data the app will be able to use on a user's device. However, participants' understanding is significantly better when helpful justifications for accessing certain functionalities or data is provided.

The results are not homogeneous among individual permissions. For example, participants perceive certain permissions as more dangerous to their privacy than others which leads to higher probabilities to deny these permissions. In our study, participants were especially concerned about access to *Contacts*, *Microphone*, *Face Recognition* and *Speech Recognition*. These results are also reflected in our qualitative analysis. Based on their open-text comments, it is often related to participants' belief that these functionalities are not critically needed for a fictional MAR app measuring distances and rendering furniture.

The key contributions of this article are as follows. First, we introduced nine new permissions which can provide the needed level of transparency for MAR apps which heavily rely on context-dependent information. Second, we tested the permission set along several different dimensions (e.g. tendency to grant permission, privacy concerns, helpfulness) and could show that there are indeed permissions which seem to be considered more critical regarding user privacy than others. Third, in contrast to earlier research indicating that explanations or justification for permission accesses can lead to unwanted behavior (i.e. disclosing personal information without really reading the explanations) [39], we could show that helpful justifications actually are perceived as more helpful to understand why an app needs this type of access. Thus, providing useful explanations for app accesses would be an important first step for creating more transparency for MAR app users.

ACKNOWLEDGMENTS

We thank Julia Bernd, and other BLUES members 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, National Science Foundation grants CNS-1514211 and CNS-1528070.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514. https://doi.org/10.2139/ssrn.2580411

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

[3] Gökhan Bal, Kai Rannenberg, and Jason I. Hong. 2015. Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns. *Computers & Security* 53, September (sep 2015), 187–202. https://doi.org/10.1016/j.cose.2015.04.004

[4] R. Balebako, F. Schaub, I. Adjerid, A. Acquisti, and L. Cranor. 2015. 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*. 63–74.

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

[6] Scott G. Dacko. 2017. Enabling smart retail settings via mobile augmented reality shopping apps. *Technological Forecasting and Social Change* 124 (2017), 243–256. https://doi.org/10.1016/j.techfore.2016.09.032

[7] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2018. Security and Privacy Approaches in Mixed Reality: A Literature Survey. (2018). https://doi.org/arXiv:1802.05797v2 arXiv:1802.05797

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

[9] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14* (2014), 2377–2386. https://doi.org/10.1145/2556288.2557352

[10] Arindam Dey, Mark Billinghurst, Robert W Lindeman, and J. Edward Swan II. 2016. 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)*. Merida, 49–50. https://doi.org/10.1109/ISMAR-Adjunct.2016.29

[11] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. 2010. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *the Proceedings of the the 9th ACM USENIX Conference on Operating Systems Design and Implementation*. 393–407.

[12] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*. 1–14. https://doi.org/10.1145/2335356.2335360

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

[14] Jie Gu, Yunjie (Calvin) Xu, Heng Xu, Cheng Zhang, and Hong Ling. 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems* 94 (2017), 19–28. https://doi.org/10.1016/j.dss.2016.10.002

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

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

[17] David Harborth, Majid Hatamian, Welderufael B. Tesfay, and Kai Rannenberg. 2019. 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*. 5029–5038.

[18] Majid Hatamian, Jetzabel Serna, Kai Rannenberg, and Bodo Igler. 2017. FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps. In *International Conference On Trust, Privacy & Security In Digital Business (TrustBus 2017)*. 1–16. https://doi.org/10.1007/978-3-319-64483-7_1

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

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

[21] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. *CHI '13 Proceedings* (2013), 3393–3402. https://doi.org/10.1145/2470654.2466466

[22] Vanessa Kohn and David Harborth. 2018. AUGMENTED REALITY – A GAME CHANGING TECHNOLOGY FOR MANUFACTURING PROCESSES?. In *Twenty-Sixth European Conference on Information Systems (ECIS2018)*. Portsmouth, UK, 1–19.

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

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

[25] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *IEEE Symposium on Security and Privacy*. 392–408. https://doi.org/10.1109/SP.2018.00051

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

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

501–510.
[28] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L Mazurek, and Jeffrey S Foster. 2017. User Interactions and Permission Use on Android. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17* (2017), 362–373. https://doi.org/10.1145/3025453.3025706
[29] Microsoft. 2017. Microsoft HoloLens. https://www.microsoft.com/microsoft-hololens/en-us/buy.
[30] Randy Nelson. 2018. Pokémon GO Revenue Hits $1.8 Billion on Its Two Year Launch Anniversary. https://sensortower.com/blog/pokemon-go-revenue-year-two
[31] Jack Nicas and Cat Zakrzewski. 2016. Augmented Reality Gets Boost From Success of 'Pokémon Go'. https://www.wsj.com/articles/augmented-reality-gets-boost-from-success-of-pokemon-go-\1468402203.
[32] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life.* Stanford University Press, Palo Alto.
[33] Victoria Petrock. 2020. US Virtual and Augmented Reality Users 2020. https://www.emarketer.com/content/us-virtual-and-augmented-reality-users-2020
[34] Robert W Proctor, M Athar Ali, and Kim-Phuong L Vu. 2008. Examining usability of web privacy policies. *Intl. Journal of Human–Computer Interaction* 24, 3 (2008), 307–328.
[35] Philipp A. Rauschnabel, Jun He, and Young K. Ro. 2018. Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research* 92 (2018), 374–384. https://doi.org/10.1016/J.JBUSRES.2018.08.008
[36] Lisa Rosenfeld, John Torous, and Ipsit V Vahia. 2017. Data security and privacy in apps for dementia: an analysis of existing privacy policies. *The American Journal of Geriatric Psychiatry* 25, 8 (2017), 873–877.
[37] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. 2015. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* 22, e1 (2015), e28–e33.
[38] Benedikt Szmrecsanyi. 2016. An informationtheoretic approach to assess linguistic complexity. *Complexity, isolation, and variation* 57 (2016), 71.
[39] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagne. 2014. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14).* 91–100. https://doi.org/10.1145/2556288.2557400
[40] Kaitlyn Tiffany. 2020. It's Cool to Look Terrifying on Pandemic Instagram. https://www.theatlantic.com/technology/archive/2020/05/augmented-reality-instagram-zoom/611494/
[41] Sabine Trepte, Leonard Reinecke, Nicole B Ellison, Oliver Quiring, Mike Z Yao, and Marc Ziegele. 2017. A cross-cultural perspective on the privacy calculus. *Social Media+ Society* 3, 1 (2017), 2056305116688035.
[42] Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. 2012. Permission evolution in the android ecosystem. In *Proceedings of the 28th Annual Computer Security Applications Conference.* 31–40.
[43] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android Permissions Remystified: A Field Study on Contextual Integrity. In *Proceedings of the 24th USENIX Security Symposium.* arXiv:1504.03747 http://arxiv.org/abs/1504.03747

A QUESTIONNAIRE

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. AR Features
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)

Part II. Permission Overview. Participants get randomly distributed into the control group, the group with helpful justifications or the group with no helpful justifications for the required permissions.

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:

(List of permissions here. See appendix A.)
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? (7-point likert scale ranging 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. The following questions are iterated for each one of the 16 permissions (treatment groups see permissions with the respective helpful or non-helpful justification).
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) Allow
(2) Allow while app is in foreground
(3) Deny
(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? (7-point likert scale ranging 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)? (7-point likert scale ranging 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? (7-point likert scale ranging from "I don't understand at all" to "I fully understand")

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 experience
(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? (ranging 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)

LISTS OF PERMISSIONS BY CONDITION

Control group

(1) Storage / Photos / Media Library
(2) Contacts
(3) Network / Internet Access
(4) Microphone
(5) Camera
(6) Location Services
(7) Notifications
(8) Accelerometer
(9) Gyroscope
(10) Magnetometer
(11) LiDAR Scanner
(12) Geometry Tracking
(13) Raw Camera Output
(14) Object Recognition
(15) Face Recognition
(16) Speech Recognition

Helpful Justification treatment group

(1) Storage / Photos / Media Library (Access to the smartphone's storage is required to browse and edit (save, erase) the photographs of the taken measurements.)
(2) Contacts (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).)
(3) Network / Internet Access (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).)
(4) Microphone (Access to the microphone is required to add voice notes to your measurement photos.)
(5) Camera (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.)
(6) Location Services (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.)
(7) Notifications (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).)
(8) Accelerometer (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.)
(9) Gyroscope (Access to the gyroscope is required to provide image stabilization based on the position of your device and the vibrations of your hands.)
(10) Magnetometer (Access to the magnetometer is required to detect nearby magnetic fields, which can reduce the accuracy and quality of your measurement photos.)
(11) LiDAR Scanner (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.)
(12) Geometry Tracking (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).)
(13) Raw Camera Output (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.)
(14) Object Recognition (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.)
(15) Face Recognition (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.)
(16) Speech Recognition (Allowing the app to use speech recognition is required to transcribe voice notes into text for the taken measurements or furniture ideas.)

Non-Helpful Justification treatment group

(1) Storage / Photos / Media Library (Access to the smartphone's storage is required to store data processed by the app.)
(2) Contacts (Access to the contacts is required to enable social features of the app.)
(3) Network / Internet Access (Internet access is required to connect the app with the Internet.)
(4) Microphone (Access to the microphone is required to record audio.)
(5) Camera (Access to the camera is required to take pictures and videos.)
(6) 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.)
(7) Notifications (Access to notifications is required to notify you about messages.)
(8) Accelerometer (Access to the accelerometer is required to measure the acceleration of your smartphone movements.)
(9) Gyroscope (Access to the gyroscope is required to measure the rotation of the smartphone.)
(10) Magnetometer (Access to the magnetometer is required to measure magnetic fields.)
(11) LiDAR Scanner (Access to the LiDAR scanner is required to use light to measure distances.)
(12) Geometry Tracking (Allowing the app to use geometry tracking is required to generate a geometrical schematic outline of the environment.)
(13) 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.)
(14) Object Recognition (Allowing the app to use object recognition is required to recognize details of the objects in the environments.)
(15) Face Recognition (Allowing the app to use face recognition is required to identify or verify the identities of people using their face.)
(16) 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.)

B REGRESSION ANALYSIS

Table 3: Random-effects ordered logistic regression models on the responses about willingness to grant individual permissions.

	(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)			
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: Helpfulness of permission X to understand app functions and data use	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)
Experimental Group "helpful justifications" ("control" is omitted)	0.190	0.166	0.268
	(0.95)	(0.85)	(1.14)
Experimental Group "non-helpful justifications"	0.175	0.211	0.259
	(0.83)	(1.03)	(1.19)
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)
Gender - male ("female" is omitted)		0.084	0.061
		(0.47)	(0.34)
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)
1: No information needed / clear what the permission(s) is and does			-0.249
			(-1.07)
2: Clarification about sensors / features needed			0.112
			(0.57)
3: Possibility to deny / restrict individual permissions			-0.828***
			(-3.59)
4: When data is collected			0.257
			(0.72)
5: Why and how data is collected			-0.169
			(-0.86)
N	4549	4549	4549

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; t statistics in parentheses

C CODEBOOK

Code	Description
No information needed	Participants do not need additional information, the given information given is clear or suffficient.
N/a	When participants don't really offer to add any information (but they don't say the provided information is sufficient like in the 'No information needed' code. Includes examples when participants say "none", "nothing", "not sure". Also you can use it when you are not sure what participant wants to say; when you cannot interpret their answer.
General app's functionalities	Functionalities of the apps, not related to privacy/security, e.g. how does the app measure distance, would it work on my phone, 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	Definitions of terms, explanations of what the sensors and features are. Indication of insufficient information. (When participants provide more details about what kind of information they need to know, try to apply the most relevant codes from the list; e.g. when require the clarification of how the data collected by these sensors is used, it's 'Why/how data is used (purpose)' code.)
Possibility to deny/restrict individual permissions	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 that comments about general app's functionalities are in 'General app's functionalities' code. instead, 'Impact on functionality' code talks specifically about the impact from denial certain permissions.)
Privacy Policies / Terms of services	Privacy policy, terms of services. It includes Privacy Rating / Privacy Ranking.
Privacy concerns (explicit)	Not comfortable with giving access to certain things.
(General) Data handling information	Sometimes (rarely) participants just want to know what will happen to the data without specifying whether they are interested in processing, storage, or use conditions. In this case apply this high level code; otherwise try to use more specific codes
What data is collected	What specific piece of information are collected.
When data is collected/accessed	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 (purpose)	Purpose for data collection, how it is used, how it is processed. Is this data actually required, or is it optional (note that concerns about whether the app will work without it is a separate 'Impact on functionality' code). What are the benefits of providing the data.
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 that there is a 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).