Understanding User Prioritization and Comprehension of Smartphone Permissions

MANILA DEVARAJA, University of Utah, USA
SAMEER PATIL, University of Utah, USA

Smartphones allow users to control the sharing of their data with apps according to their privacy preferences. Yet, users struggle to enact their privacy preferences via the available permission settings. To understand whether these difficulties result from inaccurate understanding and/or suboptimal interface design of the permissions manager, we designed and administered an online questionnaire to smartphone users from the United States ($n = 151$). We asked the participants to rate and rank the importance of the permissions commonly available on smartphones and to describe their understanding of what each setting controls. We found that a majority of users deem some permissions as important or unimportant, with the importance of other permissions varying across users based on use and privacy concerns. Our findings indicate that users misunderstand several permissions and express unfamiliarity with how some of them operate. We apply the insight from our study to derive suggestions to enhance smartphone permission managers by promoting personalized and efficient user interaction and more accurate user comprehension of functional operation.

CCS Concepts: • **Security and privacy** → **Usability in security and privacy**; **Privacy protections**; • **Human-centered computing** → **Empirical studies in HCI**; Graphical user interfaces.

Additional Key Words and Phrases: Smartphone permissions, Permissions manager, Privacy, User Experience, UX, Usability, User Interface, UI, User interaction

ACM Reference Format:
Manila Devaraja and Sameer Patil. 2025. Understanding User Prioritization and Comprehension of Smartphone Permissions. *Proc. ACM Hum.-Comput. Interact.* 9, 5, Article MHCI035 (September 2025), 46 pages. https://doi.org/10.1145/3743739

1 Introduction

The volume of personal data that users produce, consume, and store on their devices continues to grow rapidly [21]. Because of the mobile and individual nature of the devices, user data stored on smartphones is often quite private and sensitive [1]. As a result, users report being far more concerned about threats to their data on their smartphones than that on other mobile devices [26].

Smartphones enable users to address their privacy concerns by specifying access permissions that control how various types of data are shared with the operating system (OS) and individual apps. However, users typically find it confusing and difficult to manage permissions for the numerous data types across an ever-growing number of apps [2, 42]. Moreover, end users may not fully grasp the implications of granting a permission [2, 35].

Research efforts focused on the User Interface (UI) or User Experience (UX) of permissions specification indicate that users could benefit from tailoring the user interaction to their specific needs and contexts [35, 47]. However, research on user interactions with permissions-related UIs is typically limited to specific permissions, such as `Location` (e.g., [13, 49]), specific apps, such as

Authors' Contact Information: Manila Devaraja, manila.devaraja@utah.edu, University of Utah, Salt Lake City, Utah, USA; Sameer Patil, sameer.patil@utah.edu, University of Utah, Salt Lake City, Utah, USA.

ACM 2573-0142/2025/9-ARTMHCI035
https://doi.org/10.1145/3743739

social media (e.g., [41, 50]), or specific contexts, such as runtime (e.g., [31, 63]). There is relatively little research on managing permissions via the smartphone permissions manager embedded in the device settings to present a list of all permissions available for users to control data access by apps. The few studies that do include the permissions manager have investigated user awareness of default settings [35] or the permissions they chose to grant [61]. Researchers have additionally examined user perceptions of sensitivity and risk of data accessed via the granted permissions [16] as well as their intentions to revoke the granted permissions [61].

The findings of existing research indicate that permissions managers currently lack a UX that can facilitate accurate comprehension of the practical implications of adjusting a permission [35] and enable smooth and efficient permissions management [17]. Moreover, current permissions managers lack personalization as they present all available permissions in a predefined order to all users. To enable a less burdensome, easily understandable, and personalized UX for the permissions manager requires that we first understand similarities and differences across users in terms of how they prioritize and comprehend each of the permissions included in the current permissions managers. To that end, we formulated the following research questions:

RQ1: How do users prioritize the permissions available in the permissions manager?
RQ2: Why do users consider specific permissions important or unimportant?
RQ3: Do users accurately comprehend what each permission controls?

To answer the above research questions, we designed a questionnaire that covered all permissions included in the permissions managers in modern versions of Android and iOS [8, 12], the OSes of the majority of smartphones. We obtained responses to the questionnaire from 151 participants from the United States recruited via the crowdwork platform Amazon Mechanical Turk (AMT) from May 2024 to March 2025. We found that a majority of the participants considered some of the permissions as highly important and some others as unimportant. For instance, participants rated and ranked the `Camera` and texttttContacts permissions as the top two most important and considered `Body Sensors`, `HomeKit`, and `Nearby Interactions` as generally unimportant. Our findings indicate that the participants tended to ascribe importance to permissions based on whether the corresponding data is needed by the apps they use often and whether they consider the data to be privacy-sensitive. For permissions deemed important, the participants expressed desires for greater control over the operation and clearer justification behind the permission request. Moreover, the participants did not wish to waste time and effort in adjusting the settings for the permissions they considered unimportant or unfamiliar. In addition, we found a few notable discrepancies in participant understanding of the data associated with a few of the permissions.

Based on the findings of our study, we make the following contributions:

- We identify specific permissions that a majority of users deem highly important or mostly unimportant.
- We uncover that user assessments of the importance of a permission vary based on their use of apps that seek the permission and their privacy concerns regarding the data accessed through the permission.
- We describe gaps in user understanding and familiarity with the functional operation of some of the permissions.
- We apply the insight from the findings to propose UX enhancements for a more personalized and efficient permissions manager that can facilitate more accurate user comprehension of what a permission controls.

In the sections that follow, we first situate our work within the literature on the UX of permission settings. We then describe the design and deployment of our study, along with the characteristics of the sample and the data analysis procedures. We proceed to present the answers to the above research questions based on the analysis of the data we collected. Next, we connect our findings to the broader context of the UX of privacy management. We apply the insight to propose several user-centered recommendations to enhance the design of privacy management interfaces and conclude by offering thoughts on future directions.

2 Related Work

Our research intersects with the literature on user interaction with permissions specification UIs and user understanding of the functional operation of permission settings. We cover each of these in turn.

2.1 User Interaction with Permissions UIs

Users interact with permissions UIs on mobile devices via dialogs that present permission requests from apps at runtime. In addition, users can adjust the permission settings for an app via the permissions manager [6, 12]. Researchers have examined user interaction with permissions UIs in the above two contexts.

2.1.1 Runtime Permission Requests. Several studies have found that app developers tend to collect more data than necessary and ask users to grant superfluous permissions that may not be needed for the functioning of their apps [40, 45, 53]. Researchers have found that users tend to grant such permissions when requested, without fully understanding the implications of the decision [53], often providing ongoing access to their data without their knowledge [37]. Habituation [68] and the desire to use the app [46] can contribute to accepting permission requests at runtime.

Several research efforts have explored techniques to help users make more informed privacy-related decisions when asked to grant permissions at runtime. Andriotis et al. [4] grouped apps based on advertised functionality and assessed the privacy intrusiveness of an app by comparing the permissions it requests to those requested by apps with similar functionality. Diamantaris et al. [28] analyzed apps in real-time to differentiate between permissions *required* by the app itself and those requested by third-party libraries. In a similar vein, Hong et al. [38] designed explanations of runtime permission requests that clearly differentiate between first-party and third-party use of the collected data. Elbitar et al. [30] showed that permission requests with better rationales can benefit users as well as app developers [31]. Including rationales when requesting permissions can even reduce denial rates for runtime permission requests [25]. Similarly, messages such as “You can change permissions from device settings anytime,” can enhance the user’s sense of control [30].

Cao et al. [25] found that users often wish to grant permissions only *temporarily*. Researchers have explored various techniques to enable granular control to enact such limits. For instance, Bemmann et al. [17] designed granular options to fine-tune the `Location` permission beyond a binary decision (i.e., grant or deny). Momen et al. [58] have proposed partial consent, such as a ‘Maybe’ option, to address the difficulties users face in understanding the consequences of permissions-related choices. Relatedly, Olejnik et al. [59] implemented an ‘Obfuscate’ option to reveal the requested information only partially. However, the obfuscated data caused multiple apps to stop functioning [59]. To maintain app functionality without sharing personal data, Zhou et al. [71] developed the ‘bogus’ option that sends fake information when data is accessed via the requested permission.

Research on interaction with runtime permissions has typically involved studying individual permissions in isolation. For a long time, research on user interaction with permissions predominantly covered highly sensitive permissions, such as `Camera`, `Location`, and `Microphone` [27, 29, 32]. The `Camera`, `Location`, `Microphone` permissions were specifically highlighted in the Permission Dashboard introduced in Android 12.0 [8]. In contrast to investigating permission choices for specific permissions or apps or studying interfaces for runtime permission requests, our research focuses on the UX of the permissions manager, considering *all* permissions made available to users *as a whole*, without limiting to specific permissions, apps, or runtime contexts.

2.1.2 Permissions Manager. The permissions manager, typically embedded in the Settings menu of the device, presents users with all permissions in a single place, independent of the runtime context of any app. Permissions managers enable users to change privacy settings as their privacy preferences evolve [69]. However, many users find the options available in the permissions manager UI to be limited [66]. Moreover, the UI of the permissions manager is difficult to navigate and makes it challenging to get an overview of granted permissions [17]. Bemmann et al. [17] found that requiring multiple steps to find and adjust settings in the permissions manager can be perceived as a lack of transparency.

Prange et al. [61] showed that users leverage the permissions manager to manage privacy. Cao et al. [25] found that 60% of the decisions made through the permissions manager were for granting permissions. The high number resulted from the participants having denied the permissions at runtime because they knew that they could change their decision later via the permissions manager. In contrast, other studies have shown that users forget to use the permissions manager to revoke granted permissions or forget that they granted them in the first place [72]. Moreover, users may be unaware of the existence of the permissions manager and may not realize that it is possible to revoke a permission [35]. Prange et al. [61] have suggested reminding users to review important permissions at opportune moments. Our research can be helpful for the practical implementation of the suggestion by surfacing which permissions users find important.

Tsai et al. [66] proposed a redesign of the Android permissions manager to reduce the number of permission-related decisions users need to make by applying machine learning to automate the decision-making. The redesign improved the UX for four key tasks: identifying apps that recently accessed permissions, finding granted permissions, distinguishing between foreground and background permissions use, and enabling users to limit background permission access [66]. However, the redesign covered only the subset of the permissions identified as sensitive by prior research or by the latest Android version at the time. In contrast, our research covers *all* permissions available in the permissions manager.

2.2 User Comprehension of Privacy Permissions

Users expect to be informed about the collection of their data [55, 64]. Being aware of data collection can affect user judgments regarding privacy [37, 67]. For example, awareness of data privacy can influence whether users adopt an app [16]. Yet, as several studies have pointed out, the UIs for specifying permissions tend to lack sufficient information to help users understand the implications of the choices [33, 40, 42, 70]. Users may never use some of the permissions because of a lack of understanding [33].

To improve user understanding, researchers have explored mechanisms to communicate *why* apps access data through permissions [53, 54]. Li et al. [52] devised the PERUIM model to communicate the purpose of requested permissions by mapping permissions to UI components of an app. Recently, smartphone manufacturers have mandated that app developers justify their permission requests [10] and include concise privacy labels [44, 55] describing how data is collected and used by their apps [5, 34]. However, the requirement to provide a rationale is not consistent across permissions [25]. For example, Schmidt et al. [62] showed that app developers can request access to the `Local Network` without providing a rationale. Moreover, many app developers do not provide sufficient information to *justify* the need, instead simply *stating* that a permission is needed or employing terminology that can create incorrect impressions about which data is accessed or lead to misconceptions about the function and scope of the data access [30].

Although permissions are meant to give users control over their privacy, permissions specification UIs often fail to convey information with sufficient clarity [2]. As Schmidt et al. [62] have pointed out, an accurate understanding of how a permission operates is essential for making an informed decision about granting a permission. However, the information in permission request dialogs can be confusing, making it difficult for users to understand the implications of granting a permission [42]. Moreover, the limited information typically included in runtime permission requests can cause users to misperceive the scope of the permission [63]. For instance, Schmidt et al. [62] found that 85% of their participants, including those with technical backgrounds, misunderstood the underlying functionality of the `Local Network` permission and struggled to grasp all relevant concepts needed to make an informed decision.

Our examination is most closely related to Shen et al. [63]'s study on user understanding of permission requests. However, Shen et al. [63] investigated comprehension of only a few permissions, whereas we included the entire set of permissions available in the permissions manager. Moreover, Shen et al. [63] judged user comprehension by providing participants with several choices and asking them to choose the correct answer. In contrast, we obtained more detailed and nuanced data regarding user comprehension by asking participants to describe their understanding via open-ended text responses, an approach similar to that used by Schmidt et al. [62] to capture user understanding of the `Local Network` permission.

Research on user comprehension of permissions has so far been limited to the runtime context [30, 51, 63]. Such studies typically focus exclusively on *specific* permissions, often within the context of *specific* apps. In contrast, our research covers the broader system-wide scope of the permissions manager and investigates user understanding in relation to the description of the permission functionality provided by the OS. Such an investigation is valuable because the permissions manager enables users to examine and manage *all* adjustable permissions across *all* apps in a single place.

3 Method

To answer our research questions (see Section 1), we developed a questionnaire that we used to collect responses from participants on AMT. In the following subsections, we explain the design of the questionnaire, provide information on study deployment, report the characteristics of our sample, and describe our data analysis procedures. All study procedures were reviewed and approved by the Institutional Review Board (IRB) of the University of Utah.

3.1 Questionnaire Design

We designed an online questionnaire to capture how users prioritize and comprehend the permissions listed in the permissions managers of the latest versions of Android and iOS at the time. Since the permissions and corresponding labels differ slightly across the two OSes [8, 12], we consolidated them into a single superset of 26 permissions (see Table 1). Using a consolidated superset was a reasonable approach given that it is not uncommon for individuals to have experienced using both of the dominant mobile OSes across the various devices they own.

In the few cases where the same permission was labeled slightly differently in Android and iOS, we combined the variations into a label that could be generally understood independent of OS. For example, we used the label `Music and Audio / Media` to represent the permission labeled by Android as `Music and audio` and iOS as `Media & Apple Music`. However, in case there were large semantic differences in the labels for a permission across the two OSes, we kept both in the superset used in the questionnaire. For example, even though `Nearby Devices` in Android and `Local Network` in iOS are connected to the same function, we included both separately in

Table 1. List of permissions used in the study created by consolidating the permissions available in Android 13.0 and iOS 17.4.1.

Android 13.0	iOS 17.4.1	Questionnaire
–	Bluetooth	Bluetooth
Body sensors	–	Body Sensors
Calendar	Calendars	Calendar
Call logs	–	Call Logs
Camera	Camera	Camera
Contacts	Contacts	Contacts
Files	Files and Folders	Files and Folders
Do Not Disturb*	Focus	Focus / Do Not Disturb
Health Connect	Health	Health
–	HomeKit	HomeKit
–	Local Network	Local Network
Location	Location Services	Location
Microphone	Microphone	Microphone
Music and audio	Media & Apple Music	Music and Audio / Media
Nearby devices	–	Nearby Devices
–	Nearby Interactions	Nearby Interactions
Notifications	Notifications*	Notifications
Phone	–	Phone
Photos and videos	Photos	Photos and Videos
Physical activity	Motion & Fitness	Physical Activity / Motion & Fitness
–	Reminders	Reminders
–	Research Sensor & Usage Data	Research Sensor & Usage Data
SMS	–	SMS
–	Speech Recognition	Speech Recognition
–	Tracking	Tracking
–	Wallet	Wallet

*The permission is included as a setting external to the permissions manager.

the questionnaire, given their semantic distinctness. The `Notifications` permission in Android and the `Focus` permission in iOS are included in the respective permissions managers, but the corresponding functionality in the other OS is provided via settings external to the permissions manager. Since these two settings are included in the permissions manager of at least one of the two OSes, we included them in the list of permissions we used in the questionnaire.

At the beginning, we provided detailed information about the study to seek informed consent and commitment to answer diligently, followed by screening questions to check that participants met the inclusion criteria of being adults who had lived in the United States for at least five years and used a smartphone running Android or iOS.

Eligible individuals who consented to participate diligently proceeded to answer the rest of the questionnaire organized into various sections in the following order:

Rating and Ranking the Importance of Permissions (*RQ1*): Participants rated the importance of each of the 26 permissions listed in the third column of Table 1 on a five-point Likert-type scale, with 1 being 'Least important' to 5 being 'Most important.' Participants could instead choose 'I do not know this setting' to indicate being unfamiliar with the permission. Next, we asked participants to provide the five *most* important and five *least* important permissions in rank order from 1 to 5. The ratings and rankings enabled us to capture how participants prioritize permissions in absolute (rating) as well as relative (ranking) terms based on the importance of each permission to them. We did not define the term "important" to avoid priming participants. Instead, our approach enabled participants to characterize ‘importance’ as appropriate for themselves and to tell us what they deem important and why.

Reasoning for the Importance of Permissions (*RQ2*): For each permission, participants ranked as being among the three most or least important to them, we asked them to explain the reason for the ranking via open-ended text responses. We asked only about the top three out of the five that the participants ranked to keep the questionnaire to a manageable length.

Operational Comprehension (*RQ3*): Next, participants provided open-ended text responses to describe what they believed a given permission controls. To avoid overly burdening participants, we asked for their comprehension of three permissions chosen randomly from the full set of 26. We ensured that the random selection avoided any permissions for which participants had selected ‘I do not know this setting’ when rating the permissions previously.

Permissions-related Practices: To place the responses of participants regarding the importance and comprehension of permission within the broader context of their smartphone use, we asked about various permissions-related practices, such as screen locking, sideloading apps, checking app descriptions for permissions information prior to installation, frequency of modifying app permissions, and dealing with unjustified app permission requests at runtime. In addition, we asked Android users about the recently introduced feature to remove permissions from unused apps [7] and iOS users about the App Privacy Report feature in iOS that details how often apps access the data connected with a permission [11].

Individual Characteristics: To understand how differences between individuals might influence responses, we included the Application Information Privacy Concern (AIPC) scale [24] to capture baseline privacy concern about apps and the General Digital Difficulties (GDD) and Worries about Future Digital Difficulties (WFDD) subscales of the Digital Difficulties Scale (DDS) [9] as measures of technical efficacy. In addition, we collected standard demographics, such as age, gender, ethnicity, education, employment status, income, relationship status, number of children, etc.

Concluding Remarks: In the end, we asked participants to indicate whether they responded attentively, provide feedback on the study, and mention anything else they wished to convey.

To flag inattentive participants, we embedded two attention checks within the questionnaire, one within the items for the AIPC scale and the other within the demographic questions. The questionnaire design was based on iterative refinements to the questions, answer choices, presentation, and flow based on multiple pilot rounds with people unconnected to the research, including undergraduate and graduate students. Apart from the initial questions about consent, commitment, and screening, participants were free to skip answering any questions they did not wish to answer. The complete questionnaire is available in Appendix C.

3.2 Study Deployment

We deployed the study as a Human Intelligence Task (HIT) on the AMT platform from May 9th, 2024 to March 25th, 2025. To ensure responses of sufficiently high quality, we recruited adults based in the United States who had completed at least 100 approved HITs, with a HIT approval rate of at least 95%. The HIT description included a link to the questionnaire hosted on the Qualtrics platform.[1]

To control for variation in privacy-related preferences and practices because of cultural differences among participants, we restricted participation to those who had lived in the United States for at least five years, which is a reasonable period to achieve sufficient acculturation [43]. Given our focus on smartphone permissions, we additionally required that participants be users of

[1] https://www.qualtrics.com

smartphones running Android or iOS. Those who consented to participate and met the inclusion criteria proceeded to answer the rest of the questionnaire.

As stated in the HIT description, we asked those who did not meet the screening criteria or failed an attention check embedded within the questionnaire to return the HIT without completing the study. At the end, we provided the participants with a randomly generated 8-digit code that they entered on AMT to indicate successful completion. Based on relevant criteria for statistical analyses [56], we gathered data until we had obtained at least 15 responses about comprehension of each of the 26 permissions included in the study.

We paid US $3.00 to those who completed the study and submitted the correct completion code on AMT. With a median study completion time of 20 minutes, the compensation equates to US $9.00/hour, which is above the minimum wage of US $7.25 in the United States.

3.3 Sample

Initial inspection of the responses indicated some may have been copied from external sources or generated using Large Language Model (LLM) based Artificial Intelligence (AI) tools. Therefore, we manually scrutinized the responses to flag and filter the responses of those who did not participate in good faith [60]. In particular, we flagged open-ended answers regarding comprehension of specific permissions as inauthentic if they were identical or highly similar to the answers we obtained by querying the web and prompting LLMs ourselves. Instead of providing personal views, understanding, or experiences, such responses typically included decontextualized generic information, such as:

> “Choose location access (Android 4.1, 4.3). You can control what location information your phone can use. Open your phone’s Settings app. Under ‘Personal,’ tap Location.”
>
> “1) The sound waves generated by a microphone are more accurate than those produced by a keyboard because the sound waves can be processed in real-time. 2) When used in conjunction with voice-activated systems, it can be useful in improving driver and rider safety.”
>
> “The camera setting on smartphones is indispensable for modern life, allowing us to capture precious moments, document important events, and share experiences instantly. It empowers creativity, enhances communication, and serves as a convenient tool for self-expression in our interconnected world.”

After excluding the data of the participants whose answers we flagged as inauthentic, we were left with 216 complete responses. We excluded 65 of these 216 responses based on applying additional validity checks in the following sequence:

(i) providing matching answers when asked about the year of birth at the beginning of the questionnaire and the age at the end of the questionnaire (27 excluded);
(ii) being located in the United States based on the location of the Internet Protocol (IP) address (28 excluded); and
(iii) answering the questionnaire with sufficient attentiveness by taking at least one third of the median time across all participants (10 excluded).

All 151 remaining participants stated that they completed the study with commitment by choosing the options ‘I answered all questions according to the provided instructions’ and ‘I completed the study with full attention’ for the two commitment verification questions we asked at the end of the study.

Of the 151 valid and complete responses retained after applying the above filters, 97 (64%) were from women, 53 (35%) from men, and one from a non-binary participant (1%). The ages of the participants ranged from 21 to 72, with a median of 29. More than two thirds of the participants (n = 106; 70%) were younger than 36. A large majority (n = 120; 79%) primarily used Android, with only about a fifth of the participants (n = 31; 21%) reporting primarily using iOS. Most participants (n = 134; 88%) were white/Caucasian. The sample was highly educated, with 140 (93%) having completed college. Nearly all participants reported being employed, with 139 (92%) employed full-time and 7 (5%) part-time. A majority of the participants (n = 107; 71%) were married.

3.4 Data Analysis

We conducted statistical analyses of the numeric responses coupled with thematic analysis [22] of the open-ended text responses.

3.4.1 Statistical Analyses. We analyzed the ratings and rankings of importance using descriptive statistics and plots of the distributions. In addition, we employed Spearman's rank correlation to check for relationships between the importance ratings for each permission and relevant participant characteristics. Since the Shapiro–Wilk test indicated that the ratings were not normally distributed, we used non-parametric statistical tests when examining differences between different participant groups. As applicable, we applied the Bonferroni correction to the p values to account for multiple testing.

3.4.2 Thematic Analysis. As mentioned in Section 3.1, the participants provided open-ended text responses to explain their rankings for the three most and least important permissions and describe their understanding of the operation of three randomly chosen permissions. In addition, we asked Android users to share their thoughts on the feature that automatically removes permissions from unused apps.

To perform thematic analysis [22] of the open-ended responses, we first engaged in early theme development by following the coding reliability approach [23]. The first author inspected all open-ended responses to identify preliminary themes. The themes were not mutually exclusive, i.e., a response could be coded under multiple themes. The two authors then discussed and refined the preliminary themes and formulated corresponding descriptions for each theme, along with illustrative examples (see Table 2).

The first author and two undergraduate research assistants independently coded all open-ended responses according to the refined set of themes. When coding the responses regarding operational comprehension, we checked the responses against the functionality of the corresponding permission as described in the short descriptive text for that permission included in the UI of the permissions managers of Android and iOS (see Appendix B).

After consolidating the independent coding of the three coders, we found that there was 83% agreement with the first author. The three coders then discussed and resolved all disagreements until there was full consensus among the three coders. Subsequently, we repeated the above process to identify and assign lower-level subthemes within several themes.

3.5 Limitations

A few methodological and sampling limitations may affect the broader applicability of our findings. We rely on self-reported data from a self-selected sample. Moreover, the sample includes only individuals based in the United States, with an overrepresentation of Android users. Future work with data obtained from samples from other locales or via observations of real-world user interaction with the permissions manager can complement our approach and help verify the generalizability of our findings.

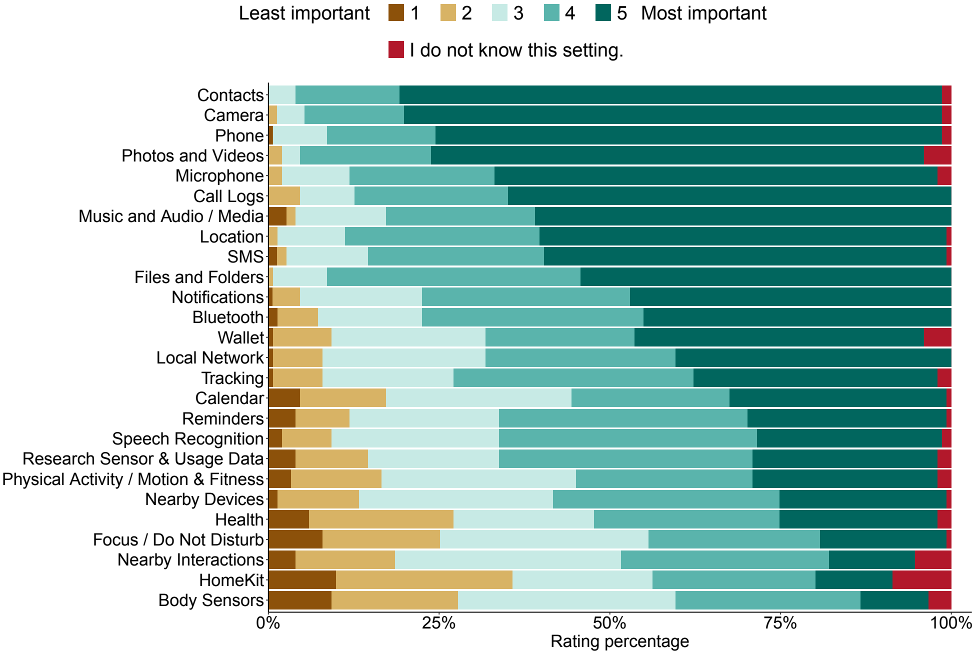


Fig. 1. A stacked bar chart showing the distribution of the ratings of the participants for the importance of each of the 26 permissions included in the study on a scale of 1 to 5, with 1 being the least important and 5 being the most important. The figure includes responses in which the participant did not rate a permission because of unfamiliarity. The bars indicate that some permissions were considered important or unimportant by a majority of the participants, while the importance of the rest varied across participants.

4 Findings

We used the results of the analyses described in Section 3.4 to answer the three research questions listed in Section 1. In addition, we examined the responses of the participants regarding their interactive practices related to smartphone permissions and checked for differences based on major demographic characteristics. We present our findings in the following subsections, supported by relevant numerical data and illustrative participant quotes.[2]

4.1 User Prioritization of Smartphone Permissions (*RQ1*)

To understand the prioritization of permissions in absolute terms, we plotted the distribution of the responses of the participants rating the personal importance of each permission on a 5-point scale from 1 to 5, with 1 being the least important and 5 being the most important. If the participants were not aware of a permission, they could indicate their unfamiliarity by selecting ‘I do not know this setting’ instead of rating the importance of the permission. Figure 1 shows a stacked bar chart with the bars showing the proportional distributions of the participant responses among the five points of the rating scale for each of the 26 permissions included in the study. The bars in Figure 1 are ordered by decreasing proportion of responses that rated the permission with the highest importance rating of 5.

[2] Note that we have fixed typos and grammar in a few quotes without affecting the semantics.

Each of the 26 permissions received at least a few ratings at the highest level of importance. However, Figure 1 indicates a few notable patterns. The permissions toward the top of Figure 1, such as `Contacts`, `Camera`, and `Phone`, were considered nearly universally important. For instance, 93% of the participants ($n = 141$) rated the `Camera` permission at the highest importance ratings of 4 and 5, with a similar number ($n = 143$; 94%) of participants rating the importance of `Contacts` as 4 or 5. In contrast, the permissions toward the bottom of Figure 1, such as `HomeKit` and `Body Sensors`, were rated at or below the mid-point 3 of the 5-point importance scale by a majority of the participants ($n = 85$; 56% for `HomeKit` and $n = 90$, 60% for `Body Sensors`). Moreover, larger proportions of participants indicated unfamiliarity with the permissions at the bottom of Figure 1. The distributions of ratings for the permissions in the middle of Figure 1 tend to be more varied than those at the top or the bottom, suggesting greater individual variation among participants regarding how they perceived the importance of these permissions.

To understand the relative prioritization of the permissions in relation to each other, we examined the permissions that the participants ranked as the five most important and the five least important to them. Figure 2 shows a stacked bar chart of proportional distributions of the top and bottom five ranks among the 26 permissions included in the study. We ordered the bars in Figure 2 by decreasing number of responses that rated the permission among the five most important.

Each of the 26 permissions appeared in the top or bottom rankings of importance of at least one participant. While the relative prioritization of permissions captured in Figure 2 does not precisely match the absolute perception of importance depicted in Figure 1, the overall groupings of permissions deemed highly important, highly unimportant, or variable across individuals are quite similar. For instance, five permissions (i.e., `Call Logs`, `Camera`, `Contacts`, `Phone`, and `Photos and Videos`) out of the top six in terms of ratings and rankings of importance are the same, with the top two being identical regardless of whether the importance of permissions is considered in absolute or relative terms. Similarly, four permissions (i.e., `Body Sensors`, `HomeKit`, `Nearby Devices`, and `Nearby Interactions`) were in the bottom six in terms of ratings as well as rankings of importance. In both absolute and relative terms, the participants deemed `Camera` and `Contacts` as highly important and `Body Sensors` and `HomeKit` as highly unimportant. `Camera` and `Contacts` ranked in the five most important permissions of 96 (64%) and 90 (60%) participants, respectively, while 70 (46%) and 104 (69%) participants included `Body Sensors` and `HomeKit` in their the five least important permissions, respectively.

4.2 User Reasoning for Personal Importance of Permissions (*RQ2*)

We asked the participants to explain why they ranked a permission among their three most important or three least important permissions. We used thematic analysis [22] to analyze the open-ended responses of the participants following the procedures described in Section 3.4. Table 2 lists the nine themes we identified among the responses, along with corresponding descriptions of the criteria used to categorize a response under a theme. For added depth, we identified subthemes within three of the themes. Table 2 includes the subthemes and corresponding descriptions of the criteria we used to code whether a subtheme was applicable to a response.

We found that 63 of the responses that provided reasons for the highest three rankings for important ($n = 39$; 8%) and unimportant ($n = 24$; 6%) permissions indicated a misunderstanding of the operation of the permission. For a more comprehensive characterization of misunderstandings, we analyzed these responses separately by combining them with those that contained misunderstandings when explaining how a given permission operates.

Overall, we found that participants ascribed relative priority to permissions based on a combination of factors, such as use of specific apps, frequency of use, privacy concerns or lack thereof,

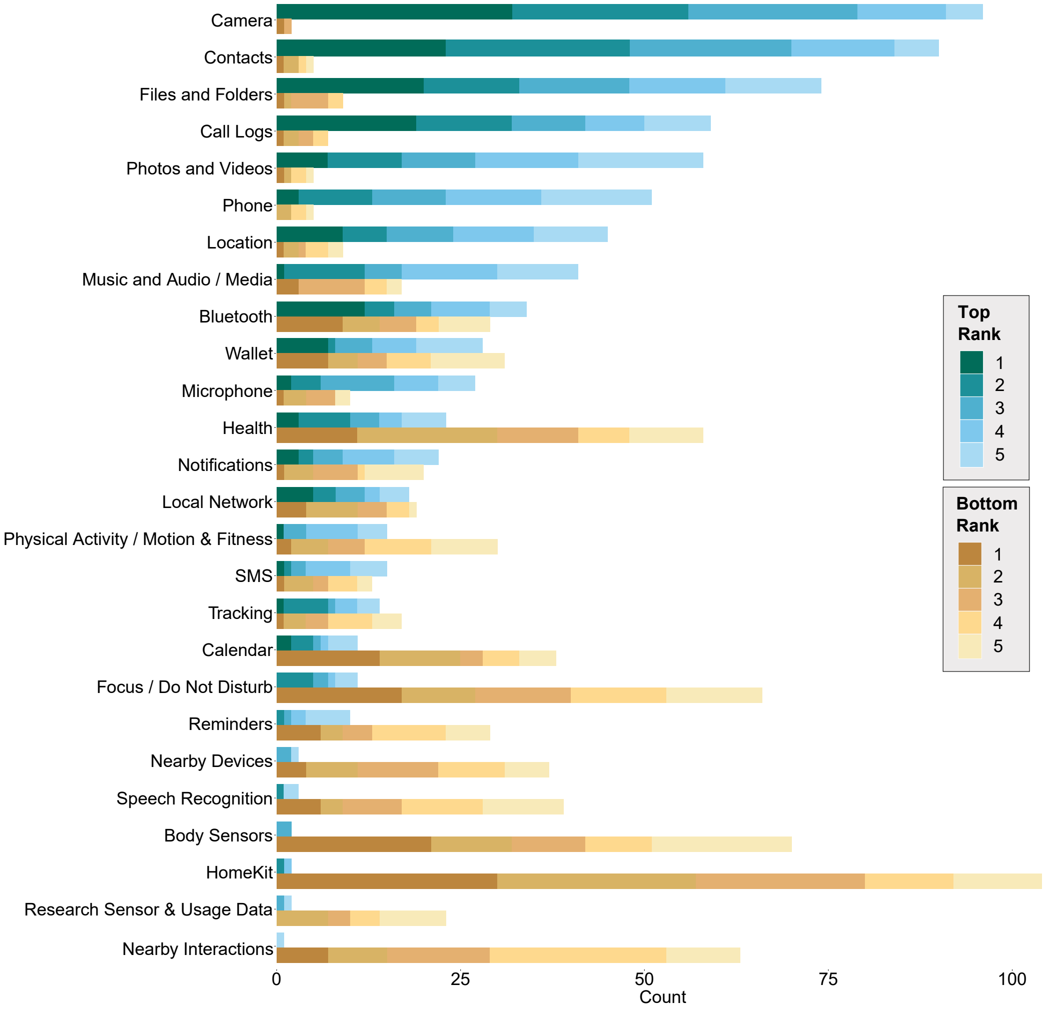


Fig. 2. A stacked bar chart showing the distribution of the rankings of the participants for the five most and five least important permissions across the 26 permissions included in the study. The bars show that the top and the bottom rankings are typically aligned with the ratings for the importance of permissions, with permissions deemed more important ranked among the top and vice versa.

familiarity, knowledge of functional operation, etc. We first provide the results of coding the reasons behind ranking permissions as important and unimportant, respectively.

4.2.1 Top-Ranked Permissions. We found that 358 of the 440 responses (81%) explained the rationale for ranking a permission among the three most important, while the remaining were either unrelated to what was asked ($n = 39$; 9%) or reflected a misunderstanding of the permission ($n = 43$; 10%). Table 3 presents the results of coding the 358 relevant answers according to the themes and subthemes described in Table 2.

Table 2. The themes, subthemes, and corresponding descriptions used for coding open-ended responses.

Themes	Subthemes	Descriptions
Personal use of a permission and/or of apps requiring the permission	Specific usage scenario	The response indicates association of a permission with a specific usage scenario.
	High frequency of use	The response indicates high frequency of use of a permission and/or apps that requires the permission.
	Storage of work-related data	The response indicates that the use of a permission is related to the storage of work-related data.
Infrequent/no use of permission and/or of apps requiring the permission	Sensor data inaccurate or untrustworthy	The response indicates that sensor data is inaccurate or expresses a lack of trust in sensor data.
	Added feature on the smartphone	The response indicates that the feature associated with the permission is a niche and/or non-essential feature.
	Not useful or not used by other users	The response mentions that the permission is not useful for anyone, including other users.
Privacy concerns	Specific data access	The response indicates concerns about access to specific data.
	Privacy of others	The response indicates concerns about the privacy of others.
	Intentional turning off of permissions	The response indicates intent or actions involving turning permissions off because of privacy concerns.
	Control over data	The response indicates a need to control the data accessed through permissions.
No privacy concerns	—	The response indicates *not* being concerned about compromising privacy through the permission.
Used via means other than the smartphone	—	The response indicates the data and/or apps connected to the permission are used via means other than mobile devices or technology.
Functionality	—	The response explains the functionality associated with the permission.
Misunderstanding	—	The response reflects a misunderstanding of the permission.
Unfamiliarity	—	The response reflects unfamiliarity with the permission.
Unrelated	—	The response is unrelated to what the permission controls.

When explaining why a permission is highly important in relation to others, more than half of the responses (n = 225; 51%) referred to the relevance or importance of the *functionality* enabled by the permission. As Table 3 shows, a large number of responses referring to functionality were connected to permissions, such as `Camera`, `Contacts`, and `Files and Folders`, that control access to data requested by features in a variety of apps. While some participants explicitly mentioned the data, others elaborated on how they associated the permission with various types of data and app features. Moreover, the responses revealed that the participants considered that some types of data, such as photos and videos, may overlap with other permissions:

Table 3. Results of coding the 358 open-ended responses of the participants providing their reasons for ranking a permission as important to them, along with illustrative examples. The themes are not mutually exclusive. The table excludes the 39 responses that we deemed unrelated to the importance of the permission and the 43 responses reflecting a misunderstanding of the permission that we analyzed separately.

Themes and Counts	**Top permissions and Counts**	**Subthemes and Counts**	**Example responses**
Functionality $n = 225$	Camera: n= 44 Contacts: $n = 37$ Files and Folders: $n = 36$	Not applicable	"Contacts setting helps store and organize phone numbers and save our time by retrieving them easily." — (Contacts) [P097, Android, Woman, 24] "It is important to save some documents as files and folders helps sort documents, photos and videos, or audio files. ..." — (Files and Folders) [P090, Android, Man, 24]
Personal use of a permission and/or of apps requiring the permission $n = 101$	Camera: $n = 23$ Contacts: $n = 16$ Call Logs: $n = 11$	Specific usage scenario $n = 38$	"So I'm able to use Maps, Weather, Uber." — (Location) [P052, Android, Man, 69] "...it is a much needed thing while making video calls over the Internet..." — (Camera) [P109, Android, Man, 30]
		Storage of work-related data $n = 12$	"During my work time, the camera is very useful to collect work-related data by scanning and digitizing documents." — (Camera) [P008, Android, Man, 35]
		High frequency of use $n = 11$	"...it affects my privacy, safety, and it is relevant for location-based services I use daily." — (Location) [P099, iOS, Woman, 34]
		Other $n = 40$	"...Calendar is very important because it helps in event management..." — (Calendar) [P032, Android, Woman, 40]
Privacy concerns $n = 81$	Camera: $n = 15$ Location: $n = 9$ Call Logs: $n = 8$ Photos and Videos: $n = 8$	Specific data access $n = 42$	"Because I don't want others to access my voice, which is one of my biometrics." — (Speech Recognition) [P002, Android, Woman, 56]
		Privacy of others $n = 11$	"...it could reveal all the [phone] numbers of my friends and family who would be exposed to all the threats." — (Phone) [P111, Android, Woman, 29]
		Control over data $n = 14$	"Because I want control over who and what has access to my call logs. It's not anyone's business whom I call or who calls me." — (Call Logs) [P096, Android, Man, 50]
		Intentional turning off of permissions $n = 8$	"...and to stop the data stealing, I need to turn off my microphone setting for particular apps." — (Microphone) [P117, Android, Woman, 34]
		Other $n = 6$	"It is my local files and folders which contain private information." — (Files and Folders) [P024, Android, Man, 37]

> "This permission accesses and manages our files like photos, videos, or documents. This is needed for things like storing photos with the camera app or downloading files from the web." — (Files and Folders) [P062, Android, Man, 24]

Nearly a quarter of the responses ($n = 101$, 23%) mentioned that the judgment of importance was based on relatively frequent use of the permission and/or of the apps requiring the permission.

At a more granular level, the reasons were connected to specific usage scenarios, frequency of use, or work-related tasks (see Table 3).

Eighty-one responses (18%) cited concerns about privacy as the reason behind considering a permission as highly important. More than half of these 81 responses (n = 42; 52%) mentioned the privacy-sensitivity of the associated data types (e.g., voice recordings, location) or data categories (e.g., work-related information):

> "Because my cell phone is a backup for some of my work and gig documents, and some of this information is sensitive. I am careful about who has access to this, especially when it comes to apps and sharing these docs across different networks and OSes." — (`Files and Folders`) [P096, Android, Man, 50]

In a few instances, the responses linked multiple permissions, such as `Camera` and `Location`, as being connected to the same data type:

> "This would literally show all that one has to know about me, including my location, etc." — (`Camera`) [P022, Android, Woman, 28]

Interestingly, one participant expressed privacy concerns even without clearly understanding what data the permission accessed, indicating a general sense of distrust:

> "Honestly, this is ambiguous enough to draw concern. Anything on the device could fall under this category of use." — (`Research Sensor & Usage Data`) [P120, Android, Man, 47]

In addition to their privacy, the participants expressed concerns about the privacy of *others* as well. Such responses mentioned worries regarding a permission exposing the information of others, such as friends and family, that was stored on the participant's smartphone. Such worries were particularly evident for permissions such as `Contacts`, `Call Logs`, `Photos and Videos`, and `Phone`, all of which potentially control access to data containing information about others.

4.2.2 Bottom-Ranked Permissions. Of the 391 responses explaining the reasons for ranking a permission among the top three least important, 323 included a proper explanation, with the remaining 68 being unrelated (n = 44; 11%) or marked as a misunderstanding (n = 24; 6%). Table 4 presents the results of coding the 361 relevant answers according to the themes and subthemes described in Table 2.

Like in the case of the permissions ranked high in importance, one of the main reasons (n = 202; 52%) for assigning the lowest importance to permissions was based on personal use, but in the opposite way. The participants considered a permission unimportant based on *infrequent or no* use of the permission and/or of the apps that required the permission. For instance, 48 of the 202 such responses were about `HomeKit`, which is typically irrelevant for those who do not own smart home devices controlled via the permission. However, many participants did acknowledge that such permissions could be considered as an *extra* feature that is beneficial only to specific user groups rather than being relevant to all users:

> "It is mostly not needed to know our heart rate or steps. It may help patients or the elderly. Some sportspeople may need it for their fitness [monitoring] purposes. But it is not essential for all." — (`Body Sensors`) [P062, Android, Man, 24]

In contrast, a notable number of responses (n = 59; 15%) explicitly stated that there was no use for the given permission or mentioned that the functionality associated with the permission was not a core feature of a smartphone. For example, a quarter (n = 15; 25%) of these 59 responses were about the `Health` permission, with participants stating that they do not use their smartphones to monitor their health. Some participants reported accessing the functionality connected to such permissions via alternative means:

Table 4. Results of coding the 391 open-ended responses of the participants providing their reasons for ranking a permission as unimportant to them, along with illustrative examples. The themes were not mutually exclusive. The table excludes the 44 responses that we deemed unrelated to the unimportance of the permission and the 24 responses reflecting a misunderstanding of the permission that we analyzed separately.

Themes and Counts	**Top permissions and Counts**	**Subthemes and Counts**	**Example responses**
Infrequent/no use of the permission and/or of apps requiring the permission $n = 205$	`HomeKit`: $n = 48$ `Body Sensors`: $n = 25$ `Health`: $n = 20$ `Nearby Devices`: $n = 14$ `Nearby Interactions`: $n = 14$	Not useful or not used by other users $n = 16$	"Because not everyone uses their phone to connect with nearby devices. . . " — (`Nearby Interactions`) [P004, Android, Woman, 64]
		Added feature on the smartphone $n = 14$	"It is just an added feature. Compared to the other features, the wallet setting has less importance." — (`Wallet`) [P131, Android, Man, 33]
		Sensor data inaccurate or untrustworthy $n = 8$	"I don't trust the sensors in the smartphone for physical activity. I think it can't give a proper reading. So I don't use it." — (`Physical Activity / Motion & Fitness`) [P117, Android, Woman, 34]
		Other $n = 165$	"I may not frequently engage in activities or use apps that rely on nearby device interactions or proximity-based services." — (`Nearby Interactions`) [P099, iOS, Woman, 34]
Used via means other than the smartphone $n = 59$	`Health`: $n = 15$ `Calendar`: $n = 9$ `Body Sensors`: $n = 8$	Not applicable	". . . may prefer using dedicated wearable devices (e.g., fitness trackers, smartwatches) for such purposes." — (`Health`) [P025, Android, Woman, 26] ". . . because it is not widely used by people on their phone, and there are some specific devices present in the market which are made only to run these apps. I feel that body sensors are helpful only for health and security professionals." — (`Body Sensors`) [P109, Android, Man, 30]
Functionality $n = 34$	`Bluetooth`: $n = 5$	Not applicable	"It is used to connect with the locally available network." — (`Local Network`) [P019, Android, Woman, 27]
Privacy concerns $n = 27$	`Body Sensors`: $n = 4$	Not applicable	"I have my own fitness plan, and I am wary of having that information on my phone." — (`Physical Activity / Motion & Fitness`) [P052, Android, Man, 69]
No privacy concerns $n = 11$	`Music`: $n = 2$ `Wallet`: $n = 2$	Not applicable	". . . I'm not as concerned about apps listening in on conversations as I am with other types of permissions. I generally trust that apps requesting microphone access are doing so for legitimate purposes." — (`Microphone`) [P093, Android, Man, 33]
Unfamiliarity $n = 25$	`HomeKit`: $n = 14$	Not applicable	"Because I have no idea what this setting means, and I have never used this setting." — (`Local Network`) [P002, Android, Woman, 56]

> "I primarily use messaging apps or email for communication rather than traditional text messages." — (`SMS`) [P093, Android, Man, 33]

A more detailed look revealed that several participants viewed certain permissions as unnecessary, not just for themselves but also for others (see Table 4). Some participants questioned the reliability and accuracy of the data connected to sensor-related permissions, such as `Body Sensors` and `Health`, expressing doubts about the meaningfulness and utility of such data (see the example comment in Table 4) Some even mentioned disabling unneeded permissions entirely:

> "I always turn these off, which makes it a pointless feature." — (`Reminders`) [P120, Android, Man, 47]

As with the top-ranked permissions, privacy concerns were a factor that influenced bottom rankings as well, with 38 (10%) of the responses citing it as a reason for assigning a permission the lowest importance. Nearly three-fourths of the 38 (n = 27; 71%) responses mentioned having privacy concerns related to the permission in question. In contrast, 11 explicitly stated that the permission was unimportant to them because they had *no* privacy concerns about its operation. Notably, one response expressed concern not just about the specific permission but about the overall burden of managing multiple permissions, highlighting privacy concerns about data access enabled by default settings:

> "My Android phone comes with numerous settings that are enabled by default, many of which may compromise our privacy, drain battery power, or slow down the device. So nearby device is less important to me." — (`Nearby Devices`) [P101, Android, Woman, 33]

Even though the participants themselves chose the permissions they ranked as highly unimportant, some responses (n = 25, 6%) nevertheless expressed unfamiliarity with the permission when asked for the reasons behind the ranking. More than half of these (n = 14; 56%) were about the `HomeKit` permission, which was also among the permissions receiving the highest proportion of low ratings for importance (see Figure 1). We noted unfamiliarity as a reason for the relatively low importance assigned to other permissions such as `Body Sensors` and `Research Sensor & Usage Data`, which similarly received high proportions of low importance ratings (see Figure 1). Overall, the above findings suggest that unfamiliarity itself is one of the factors that leads users to assign the lowest importance to a permission.

4.3 Comprehension of Permission Operation *(RQ3)*

By asking the participants to describe their operational understanding of three randomly selected permissions, we obtained a total of 453 responses across the 26 permissions included in the study, with each permission receiving explanations from 15 participants on average. Of these, we deemed 65 (14%) as unrelated to describing how the permission operates. Table 5 presents the results of categorizing the remaining 388 responses according to the level of operational understanding of the permission reflected in them.

We categorized a response as demonstrating correct understanding if the participant accurately described the data accessed via the permission. More than half (n = 207; 53%) of the responses showed that the participant correctly understood what the permission controls. If the response explained the operation of the permission based on specific apps or referenced only a portion of the data accessed via the permission, we considered it as reflecting partial functional understanding. More than a quarter of the responses (n = 105; 27%) indicated that the participant understood the operation of the permission only partially. In such cases, we typically found that the participant's understanding of the operation of the function was shaped by familiarity with specific apps or functionalities rather than by a nuanced understanding of what the permission specifically controls. The participants with partial understanding often failed to account for all the data that could be accessed via the given permission. For instance, as illustrated in one of the example responses in

Table 5. Results of categorizing the level of understanding in the 453 open-ended responses of the participants regarding their comprehension of what a given permission controls, along with illustrative examples. The themes are not mutually exclusive. The table excludes the 65 responses that we deemed unrelated to operational comprehension of the permission.

Level of Understanding and Counts	**Top Permissions and Counts**	**Example responses**
Fully correct understanding $n = 207$	`Calendar`: $n = 16$ `Contacts`: $n = 16$ `Location`: $n = 13$	"It will show the devices which are nearby and ready to pair with my device." — (`Nearby Devices`) [P021, Android, Woman, 27] "It controls notifications and interruptions on a device." — (`Focus / Do Not Disturb`) [P125, iOS, Woman, 57] "This setting controls which apps can access my contacts." — (`Contacts`) [P080, iOS, Man, 35] "The Calendar setting controls access to calendar events and schedules stored on the smartphone, limiting which apps can view or modify this information when requested." — (`Calendar`) [P099, iOS, Woman, 34]
Partially correct understanding $n = 105$	`Wallet`: $n = 8$ `Reminders`: $n = 7$	"Phone controls the contact details." — (`Phone`) [P053, Android, Woman, 29] "This is to extract the speech to text if we get a call from an unknown language and also very helpful for calls from foreign countries with unknown numbers." — (`Speech Recognition`) [P094, Android, Woman, 40] "It has all contacts of my friends and family." — (`Call logs`) [P110, Android, Woman, 25] "It helps to set important appointments." — (`Reminders`) [P081, Android, Woman, 27]
Misunderstanding $n = 73$	`Music`: $n = 9$ `Tracking`: $n = 7$ `Research Sensor & Usage Data`: $n = 6$	"Access to my money and transaction data." — (`Wallet`) [P024, Android, Man, 37] "Usage data warns me if I use more of my data." — (`Research Sensor & Usage Data`) [P006, iOS, Woman, 25]
Unfamiliarity $n = 8$	`Research Sensor & Usage Data`: $n = 1$ `Reminders`: $n = 1$	"I have no knowledge about this." — (`Reminders`) [P042, Android, Woman, 42] "I'm not entirely sure about this one. It's broad enough to possibly include any number of tracking metrics. . . " — (`Tracking`) [P120, Android, Man, 47]

Table 5, participant P110 failed to note that the `Call Logs` permission allows access to *all* incoming and outgoing calls, not just those to/from friends and family. Such partial understanding can lead to believing that the scope of a permission is more limited than is the case. In particular, we found that permissions that controlled similar or related data types could lead to confusion, resulting in partial understanding. For instance, we found that some of the responses conflated `Reminders` with `Calendar` (as seen in one of the example responses in Table 5), `Health` with `Body Sensors` and `Physical Activity / Motion & Fitness`, and `Phone` with `Call logs` and `Contacts`:

> "Phone is majorly important because it contains all required features like contacts, files and folders, etc." — (`Phone`) [P085, Android, Woman, 42]

We coded a response as reflecting a misunderstanding of how a permission operates if it mischaracterized the functionality of the permission, incorrectly identified the data controlled by the permission, or exhibited misconceptions about usage scenarios and/or apps associated with the permission. We found that 19% ($n = 73$) of the 388 responses indicated that the participant misunderstood what the permission controls. As mentioned above, for a deeper analysis of misunderstandings, we combined these responses with the 39 and 24 responses we flagged as reflecting a misunderstanding of the permission when coding the reasons the participants provided for ranking a permission as important or unimportant, respectively.

Table 6 presents the results of coding 77 of the 136 responses with misunderstandings into five subthemes. The largest proportion of misunderstandings among the 136 responses ($n = 32$; 24%) resulted from vague or confusing labeling of the permission. For instance, as one of the example responses in Table 6 shows, participant P060 misinterpreted the label `Tracking` as being about location tracking. Nearly a similar proportion ($n = 28$; 21%) of misunderstandings resulted from the participant associating the wrong type of data with the permission, such as participant P012 associating fingerprints with `Body Sensors` (see the example response Table 6). In a few cases ($n = 6$; 4%), the misunderstanding led the participants to unwarranted privacy concerns. In contrast, some misunderstandings created a false sense of security that the permission could be used to seek help in emergencies ($n = 7$; 5%) or to find lost devices or persons ($n = 4$; 3%) The remaining 59 responses did not fit any of the five subthemes, and we did not identify additional coherent subthemes that could be used to categorize these responses.

In general, we found that the participants tended to infer what a permission controls based on the label used for the permission and/or their experience of using apps that ask for the permission. However, in many cases, the label for the permission was not sufficiently precise, thus making it difficult to infer what exactly it controlled (see examples in Table 6). In some cases, the label could be misinterpreted for a different concept with similar terminology, such as 'Usage Data' in `Research Sensor & Usage Data` being mistaken for the amount of data accessed over the network when using the smartphone:

> "This setting is useful for my network speed and monthly usage of my data, like as sensor enable mode." — (`Research Sensor & Usage Data`) [P104, Android, Woman, 27]

In addition, we noted that misunderstandings occurred when a permission could potentially be connected to data that could be obtained from a variety of sources, such as audio data that can be obtained from music services, audio and video files, microphones, etc.:

> "Anything in the Music app. May also include voice memos and possibly even audio taken from the videos in your photo album." — (`Music and Audio / Media`) [P054, iOS, Woman, 39]

Even though we explicitly avoided asking about permissions for which the participant answered 'I do not know this setting' when rating permissions, eight participants (2%) indicated unfamiliarity with the permission for which we asked them to explain operational understanding. As the example responses in Table 5 suggest, the unfamiliarity may have resulted from vague, broad, or confusing labeling, such as 'Tracking,' or from thinking more deeply about operational detail when explaining than when providing a numeric rating for importance.

Table 7 provides the distribution of the levels of operational understanding across each of the 26 permissions included in the study. Since we asked each participant about only three of the permissions, the total number of responses per permission is about 15 on average. While the participants fully or partially understood the operation of most of the permissions, there were a few notable exceptions. The `Music and Audio / Media`, `Phone`, and `Tracking` permissions were misunderstood to a much greater extent compared to others, while `Body Sensors`, `Nearby Interactions`, and `Wallet` tended to be understood partially, rather than fully. Notably, there was at least one response with a misunderstanding for 23 out of the 26 permissions, with no misunderstanding noted only for `Bluetooth`, `Files and Folders`, and `Location`.

Table 6. Results of coding the 136 responses we categorized under 'Misunderstanding' when coding the reasons provided by the participants for ranking a permission as important or unimportant or the explanations given by the participants regarding what a permission controls, along with illustrative examples. We have labeled the subthemes so that they are self-explanatory. The table excludes the 59 responses we did not classify under any subtheme.

Subthemes and Counts	**Top Permissions and Counts**	**Example responses**
Terminology misunderstanding $n = 32$	`Tracking`: $n = 12$ `Phone`: $n = 6$ `Research Sensor & Usage Data`: $n = 5$	"Tracking is used to track our location to where we live." — (`Tracking`) [P060, Android, Woman, 25] "It controls the settings for setting up and using my phone." — (`Phone`) [P036, Android, Woman, 36] "Usage data warns me if I use more of my data." — (`Research Sensor & Usage Data`) [P006, iOS, Woman, 25]
Incorrect association between data and permission $n = 28$	`Music and Audio / Media`: $n = 4$ `Phone`: $n = 4$	"I believe [it controls] security features like passcodes, biometrics, and app permissions." — (`Phone`) [P135, Android, Man, 45] "It controls stuff such as fingerprint sensors." — (`Body Sensors`) [P012, Android, Man, 30] "Phone health setting typically controls features and optimizations aimed at prolonging battery life, etc." — (`Health`) [P125, iOS, Woman, 57]
Permissions help in emergencies $n = 7$	`Body Sensors`: $n = 2$ `Call Logs`: $n = 1$ `Local Network`: $n = 1$ `Nearby Interactions`: $n = 1$ `Phone`: $n = 1$ `Tracking`: $n = 1$	"These sensors can trigger alerts to emergency contacts or services, potentially saving lives in critical situations." — (`Body Sensors`) [P025, Android, Woman, 26] "Local network is very useful to connect in emergencies to contact others in critical times." — (`Local Network`) [P103, Android, Man, 30]
Misunderstanding leading to privacy concerns $n = 6$	`Bluetooth`: $n = 1$ `Calendar`: $n = 1$ `HomeKit`: $n = 1$ `Local Network`: $n = 1$ `Nearby Interactions`: $n = 1$ `Tracking`: $n = 1$	"Sharing data via nearby interactions might raise privacy concerns for us to control the information, and sometimes, it asks for app installation..." — (`Nearby Interactions`) [P097, Android, Woman, 24] "This would reveal all devices and their files, which can be a highly risky vulnerability." — (`Local Network`) [P111, Android, Woman, 29]
Permissions help find lost devices or persons $n = 4$	`Nearby Devices`: $n = 2$ `Tracking`: $n = 2$	"Tracking system helps track stolen vehicles or mobile devices. It can be tracked around the country and therefore ensure that it is returned in the quickest amount of time." — (`Tracking`) [P086, Android, Man, 62] "Nearby Devices helps control the location of the mobile phone when it is lost." — (`Nearby Devices`) [P071, Android, Woman, 29]

4.4 Permissions-related Interactive Practices

For a more refined understanding of interactions with permissions, we examined the responses of the participants regarding specific interactive practices related to permission settings, including the latest Android feature of automatically removing permissions from unused apps and the iOS feature that reports the use of permissions by apps.

Figure 3 provides a stacked bar chart of the distributions of the responses of the participants regarding how frequently they engage in specific practices. As Figure 3 shows, 58% of the participants reported often or always reading about app permissions (if available in the app description) when installing an app, and 44% indicated that they frequently change app permissions via the permissions manager under smartphone settings. We found that 36% of the participants frequently

Table 7. Distribution of the 393 open-ended responses of the participants across the four levels of understanding of what a given permission controls.

Permission	Fully Correct Understanding	Partially Correct Understanding	Misunderstanding	Unfamiliarity
Bluetooth	9	5	0	0
Body Sensors	4	6	5	1
Calendar	16	3	2	0
Call Logs	11	5	2	0
Camera	3	2	3	0
Contacts	16	3	2	0
Files and Folders	11	1	0	0
Focus / Do Not Disturb	11	3	2	1
Health	9	6	4	1
HomeKit	5	1	2	1
Local Network	9	6	3	0
Location	13	4	0	0
Microphone	6	3	2	0
Music and Audio / Media	4	5	9	0
Nearby Devices	11	6	5	0
Nearby Interactions	4	6	3	0
Notifications	10	5	1	0
Phone	1	4	5	0
Photos and Videos	7	1	3	0
Physical Activity / Motion & Fitness	6	3	1	0
Reminders	7	7	2	1
Research Sensor & Usage Data	5	3	6	1
SMS	10	6	1	0
Speech Recognition	11	1	2	1
Tracking	2	2	7	0
Wallet	6	8	1	1

install apps from a source other than the official app store. The relatively high proportion of participants who install such apps could be because most of our participants used Android, which lets users install apps from external sources.

If an app asks for a permission that is deemed unjustified, a majority of the participants (n = 89; 59%) stated that they would grant such a permission only if they believed that denying the permission would hamper the app's functionality or features, while a quarter of the participants (n = 36; 24%) said that they would deny such a permission request. However, nearly a fifth of the participants (n = 26, 17%) indicated that they would allow the permission request despite finding it unjustified.

Auto-removal of permissions in Android. Of the 120 participants who primarily used Android, only 46 (38%) were aware of the newer feature that automatically removes permissions when apps are unused for some time. The others were either unaware (n = 59; 49%) or unsure (n = 15; 12.5%). We asked those who were aware of the feature about its usefulness. Table 8 presents the results of coding the open-ended text responses of the participants regarding the utility of the feature. Most of the 46 participants (n = 33; 71%) found the feature to be useful for various purposes, with 21 (46%) indicating that the feature enhances their privacy and security. However, nearly a fifth of the 46 participants (n = 7; 17%) reported that not finding the feature useful.

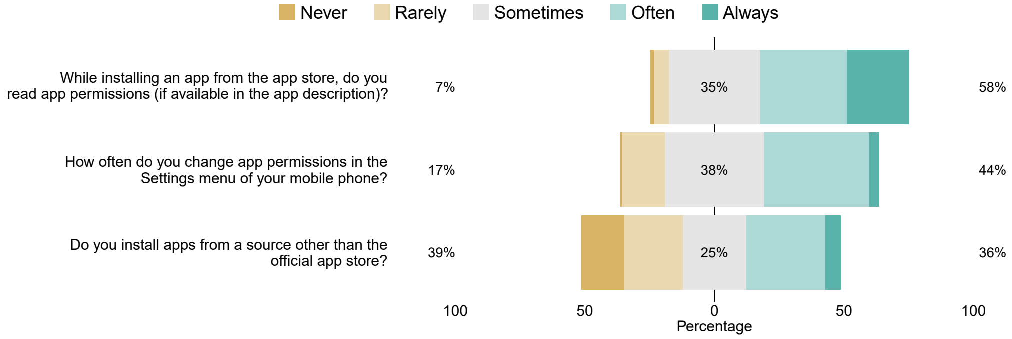


Fig. 3. A stacked bar chart showing the distribution of participant responses regarding their practices related to interacting with smartphone permissions, indicating the percentages of participants who engage in the practice never or rarely (left), sometimes (middle), or often or always (right).

Table 8. Results of coding the 46 responses regarding the usefulness of the Android feature that automatically removes permissions from unused apps. We have labeled the themes so that they are self-explanatory. The table excludes the 6 responses that we deemed unrelated to the feature.

Themes	n	Example responses
Useful: Enhanced privacy/security	21	"It's a great feature. It's a simple way to protect your privacy without having to manually manage apps." — [P093, Android, Man, 33]
Useful: Battery life	4	"I think unwanted permissions to unwanted apps can consume battery, so this feature can help maintain phone charge." — [P149, Android, Woman, 31]
Useful: Convenience	4	"This is a highly useful feature as it would stop unwanted permissions from persisting." — [P022, Android, 28, Woman]
Useful: Other	4	"It can help save storage space by removing unused apps and reduces the risk of malicious apps accessing my data in the background without permission." — [P062, Android, Man, 24]
Not useful	7	"I'm not crazy about it, but it also asks when I use it again, so it hasn't been an issue for me yet. I just wish the phone people would stop trying to direct me on how to use my own devices. I'm perfectly capable." — [P096, Android, Man, 50]

App Privacy Report in iOS. We found that all except one of the participants who primarily used iOS were aware of the App Privacy Report feature but used it relatively infrequently. Of the 31 participants who primarily used iOS, the 13 (42%) who reported using the App Privacy Report most frequently still used it only once a week. Another 11 (36%) used it less frequently. About a fifth of the participants who primarily used iOS (n = 6; 19%) had heard of the App Privacy Report but never used it.

4.5 Demographic Influences

We performed the statistical analyses mentioned in Section 3.4 to check whether the ratings for the importance of a permission were associated with personal characteristics and demographics of the participants. Unsurprisingly, there were statistically significant differences between Android and iOS users regarding the two iOS-specific permissions of `HomeKit` (W = 1027.5, Bonferroni-corrected

$p = 0.044$) and `Wallet` ($W = 1130.5$, Bonferroni-corrected $p = 0.030$). As expected, those who primarily used iOS rated these two permissions as more important than those who primarily used Android (`HomeKit` means: iOS = 3.63, Android = 2.83; `Wallet` means: iOS = 4.55, Android = 3.86). Interestingly, parents and non-parents differed in their ratings of the `Microphone` permission ($W = 2849.5$; means: parents = 4.81, non-parents = 4.41; Bonferroni-corrected $p = 0.028$). The higher importance given to the `Microphone` permission by parents might be because of they prefer for using voice-based smart assistants provided by smartphones [19]. The only statistically significant difference between the ratings of men (mean = 4.08) and women (mean = 4.53) was regarding the `Music and Audio / Media` permission ($W = 1876$, Bonferroni-corrected $p = 0.047$). The age of the participants was positively correlated with the ratings of importance of only the `Tracking` permission (Spearman's $\rho = 0.28$, Bonferroni-corrected $p = 0.015$). We found no other statistically significant associations between the ratings and privacy concerns, technical efficacy, device OS, age, gender, and parenthood.

5 Discussion

Our findings regarding user prioritization and comprehension of the complete set of permissions available in the permissions manager provide a more unified view that complements and extends the literature on smartphone permissions. Below, we connect the insight from our findings to those derived from the studies of individual permissions or runtime permission dialogs. We additionally place the findings within the larger context of the UX of the permissions manager.

5.1 User Prioritization of Smartphone Permissions

Our findings highlight that users do not consider all permissions in the permissions manager equally important. Note that we did not define the term 'importance' for the participants. Instead, we sought to uncover the factors that the participants consider when ascribing importance to a permission. We found that the participants assigned absolute and relative importance to permissions based on personal use and privacy concerns.

5.1.1 Personal Use. The explanations of the participants regarding their judgments of importance often mentioned personal usage scenarios, indicating that individual usage patterns can shape perceptions regarding the necessity and utility of granting a permission. Our findings add to the collection of studies that point out the need to assess the relevance of permissions in relation to the user's intended purpose for using the app [20, 61].

The participants tended to deem a permission as more important if it was necessary for the apps and functionalities they frequently used and less important if they had never used apps, features, or data associated with the permission. Several participants explicitly turned off the permissions they deemed highly unimportant in line with the findings of Prange et al. [61] showing that users prefer not to grant permissions for infrequently used apps or features and revoke permissions for apps or features they deem unneeded. In fact, some participants in our study felt that certain permissions were tied to niche features of the smartphone that seemed unnecessary not only for themselves but for most users. Such views show that many users may wish to use only a subset of the features offered by smartphones. However, current permissions managers do not support subsetting the permissions list to include only those associated with the subset of apps and features to which users wish to limit their use.

Asking participants to rate and rank permissions according to importance helped us understand the full context of how users prioritize permissions in comparison to asking them to consider only the perceived sensitivity and potential risk associated with each permission [16]. For example, the participants who did not use digital wallets rated the `Wallet` permission as less important, even though they recognized that it controlled sensitive financial data. Similarly, the `HomeKit` permission that controls relatively sensitive data from smart home devices [16] was almost universally deemed to be of the lowest importance because of unfamiliarity or a perceived lack of utility.

Interestingly, we found that the `Files and Folders` permission was one of the topmost important permissions for the participants (see Figures 1 and 2). The high importance ascribed to the permission could lead users to overlook the security risks of granting access to device storage [3] because of being habituated to granting the permission when asked [68] or because of the immediate need to use the app that requests the permission at runtime [46]. Indeed, Andriotis et al. [4] found that users often permit popular social media apps to access device storage but forget ever granting the permission. By surfacing its high importance for users, our findings motivate the need for more research on the use of the `Files and Folders` permission, which has so far received limited research attention in human-centered research.

5.1.2 Privacy Concerns. Interestingly, the participants mentioned privacy concerns as a reason for considering a permission as highly important or highly unimportant, but in different ways. When privacy concerns were associated with highly important permissions, the participants referred to the privacy sensitivity of the type of data associated with those permissions. In addition to the sensitive permissions of `Camera`, `Location`, and `Microphone` that enable capturing and sharing real-time data through smartphone sensors [15, 27, 29, 32, 61], the participants in our study were concerned about potential exposure of the data *stored* on the device through permissions such as `Files and Folders`, `Photos and Videos`, `Wallet`, etc. In fact, access to specific data or types of data stored on the device was the top privacy concern expressed in the responses of the participants (see Table 3). As Figures 1 and 2 show, the participants rated and ranked many of these permissions as more important to them than the `Location` and `Microphone` permissions.

In contrast to the specific privacy concerns regarding highly important permissions, expressions of privacy concerns in the case of highly unimportant permissions were typically general. In many of the cases in which the responses expressed privacy concerns about the permission, the participants indicated that ranking the permission as highly unimportant may have been driven by avoiding the use of apps and functionality tied to that permission to mitigate the underlying privacy concerns. In other cases, the participants explained that they considered the permission to be highly important because they did not have any privacy concerns related to it.

Several participants expressed concerns about a permission enabling access to the data of *others* stored on their devices. Prior research has explored such interdependent privacy concerns [18] related to the `Photos`, `Contacts`, and `Calendar` permissions on the smartphone, finding that users make interdependent privacy decisions that typically prioritize their own privacy over that of others [57] Although we do not know whether the participants in our study cared less about the privacy of others than their own, it is noteworthy that they explicitly recognized the potential impact of their permission settings on the privacy of others. We found that interdependent privacy concerns were the most prominent for the `Photos and Videos` and `Contacts` permissions, consistent with the findings of Marsch et al. [57]. We additionally noted interdependent privacy concerns regarding the `Call Logs` and `Phone` permissions. Unlike those who participated in the study of Marsch et al. [57], who employed visual cues to prime users about the data of others, the participants in our study raised these concerns spontaneously without any prompting. Our findings make the case for future research to explore user awareness of interdependent privacy issues across all available permissions.

The participants in our study expressed a desire for greater control regarding adjusting permission settings, especially for permissions that controlled the data they considered sensitive. For instance, the participants wished to disable certain permissions altogether. Our findings highlight that the

UI/UX of current permissions managers fails to provide users with adequate control, even though researchers have been highlighting the need for greater user control over smartphone permissions for a number of years [36, 63].

5.2 User Comprehension of Smartphone Permissions

Although the participants seemed to have a reasonable functional understanding of the operation of many of the permissions, we discovered a substantial number of cases that reflected partial or complete misunderstanding of what a permission controls. Partial understanding typically resulted from not recognizing the full scope of the data access possible through the permission. Our findings provide additional nuance by categorizing the misunderstandings into various types (see Table 6).

A large proportion of the misunderstandings were caused by being confused about the functionality because of the permission label. Prior studies have similarly found that users find it difficult to comprehend overly complex or vague terminology [2] and are confused when there are discrepancies between the label and the description of a permission [63]. For instance, some participants interpreted the labels of some permissions, such as `Body Sensors`, `Health`,`Tracking`, and `Nearby Devices`, as connected to seeking assistance in emergencies or locating lost devices or people.

The second main driver of misunderstandings was associating a permission with data different from what it actually controls. Such misunderstandings occurred when a permission controlled access to multiple types of data, when multiple permissions controlled access to the same data, or when closely related functionalities were associated with separate permissions. For example, the `Contacts` and `Call Logs` permissions are both connected to the phone numbers of one's contacts. Some participants of our study conflated the functionality of one such permission with the other, while others lumped together the data controlled by these permissions. These misunderstandings highlight that the UI of the permissions manager does not always accurately portray the backend operation of the permission. Our findings echo those of Shen et al. [63] who studied runtime permission dialogs and discovered that users misunderstand permissions that control access to closely related data because they find it challenging to comprehend precisely which data is controlled by which permission.

Incomplete or inaccurate comprehension of how a permission operates obviously makes it challenging for users to make *informed* choices about data sharing. Moreover, misunderstandings can lead users to develop a false sense of protection. For example, some participants falsely assumed that the permissions apply only to data stored locally on the device and not to that stored externally in the cloud. Current permission settings do not typically permit users to manage access to the data stored in the cloud differently from that stored on the device.

It should be noted, however, that we evaluated basic comprehension based on the descriptions of the permissions provided to users in the UI or the help pages. Therefore, our findings cannot account for discrepancies between the description and the backend operation and data flows. Given that many apps share data with third parties [28], there is a need for further research to examine the match between user-facing information about the operation of a permission with the actual data collection and sharing practices enabled via the permission and to investigate user comprehension of real-world data flows.

6 Design Implications

The insight from our findings can be applied to overcome various shortcomings of current permissions managers that the findings surfaced. To that end, we propose several design suggestions to enhance the UX of the permissions manager.

Personalize the order of permissions. Current interfaces that list permissions with an arbitrary or alphabetical static order for every user fail to account for the variations in perceptions of importance *across permissions and users* that we uncovered in our study. Our findings make the case for personalizing the order in which permissions are listed by sorting them according to the importance of each permission for the user. Since we found that the importance users place on permissions is shaped by their personal use, the personalization could be achieved by applying machine learning approaches to the analytics of user interactions. For instance, individual and collective patterns in granting and denying permissions could be used to infer the importance of a given permission for a given user. Such approaches have been shown to be promising for developing adaptive privacy interfaces that are more suited to a user's preferences and practices, especially if the user is included in the feedback loop [14, 66]. Alternatively, or in addition, the interface can be designed to support manual reordering of permissions as needed. Such user-tailored mechanisms can improve the UX by aligning privacy controls with real-world usage practices [48]. Moreover, a personalized order could streamline privacy management by helping users quickly find and adjust the permissions they deem the most important.

Hide irrelevant permissions. We found that many users consider only a small subset of permissions to be relevant and useful. Inclusion of personally irrelevant and unimportant permissions in the permissions manager can overwhelm users and increase the cognitive burden of finding the desired permissions in the full list of permissions [42, 66]. Our findings make the case for providing users with the ability to declutter the interface by manually hiding the permissions they deem unimportant, as suggested in prior research as well [66]. We found that users interact with such permissions rarely, if ever. Similar to the use of smart defaults in IoT privacy management [14], permissions managers could be set to turn off and automatically hide the permissions from the main list of permissions if they are rarely or never used. Users could reactivate a deactivated permission by explicitly granting it when requested by an app or enabling it via a separate UI screen that lists the deactivated permissions. Automatically disabling and hiding such permissions could substantially reduce the cognitive burden of interacting with the permissions manager by helping users focus on a limited set of frequently used permissions.

Use more meaningful terms for permission labels. We found that user comprehension of the operation of a permission is influenced by its label. In particular, we noted that overly broad or ambiguous terms in permission labels can create misunderstandings about what a permission controls. As Schmidt et al. [62] found, vague permissions labels can lead to users granting data access without fully understanding the implications of the action. Labeling permissions with more meaningful terms that lay users can be clearly understand can help avoid misunderstanding or partial understanding. Methods such as cognitive walkthrough could be leveraged to understand how users interpret various terms.

Provide granular access control for all permissions. Current permissions managers on smartphones permit users to go beyond a binary grant or deny decision by providing more granular options, such as choosing to grant access 'While using the app' [6] or providing access only to selected pieces of data, such as specific photos [39]. However, such options are available for only a few permissions deemed sensitive by the OS and are not consistent across permissions. For example, the `Files and Folders` permission on Android enables apps to "Access all files on your device" [8] without providing them the ability to limit access to specific files or folders. However, our findings indicate that users may wish to separate access to files based on context, such as separating personal files from work-related documents. Our findings suggest that the UX of permissions managers could be enhanced by extending the availability of granular access control to *all* permissions. Moreover, the granular options should be designed so that users can limit access based on time as well as specific pieces of data to avoid enabling persistent access to a limited subset of data or temporary access to all data controlled by the permission. Implementation of granular access control may need to be accompanied by corresponding regulations or policies requiring developers to support the granular options in their apps.

Include visuals to facilitate more accurate comprehension. Our findings show that users are unfamiliar with many of the available permissions and may harbor misunderstandings about how a permission operates. The unfamiliarity and misunderstandings suggest that the minimal, single-line descriptions included in permissions managers to explain the type of data controlled via a permission are inadequate to ensure accurate comprehension of the operation. A more accurate understanding of the operation of a permission can help users make informed decisions and deny unwarranted data access [25, 63]. However, designing privacy UIs that effectively educate users about their privacy and helping them make informed choices is challenging [37]. A potential approach to address the challenges could be to augment the text descriptions with visual depictions that explain the data accessed via each permission [65, 73]. Research indicates that user trust and confidence can be boosted by clarifying the purpose of a permission [53, 55] and visually depicting the underlying data flows [67].

Support batch revocations. Our findings reveal that users prefer fully disabling permissions they consider irrelevant, unfamiliar, or privacy-sensitive. Fully disabling a permission involves revoking access to the data controlled by that permission in bulk for all apps currently granted the permission [61]. Currently, users must revoke a permission separately for each app, making it cumbersome and slow to revoke a permission from multiple apps simultaneously. The UX could be enhanced by supporting batch revocations via one or more convenient interactive mechanisms, such as a 'Deny all' button, voice command for a voice assistant, etc.

Flag permissions that may impact the privacy of others. Our findings show that many users take into account the potential for affecting the privacy of others through permissions that control access to data containing information about other people. However, current permissions managers do not explicitly flag permissions that can potentially expose information about others. It could be helpful to flag such permissions by augmenting the corresponding explanatory text and/or contextually alerting users with a message such as "This permission may reveal personal information about other people." Such alerts could facilitate greater consideration of interdependent privacy and help users protect not just their own privacy but also that of others they care about.

7 Conclusion

Permission settings remain the primary means for users to express and enact their privacy preferences on their mobile devices. Permissions managers, typically embedded in the Settings menu of the device, provide a central hub for users to manage access to the data that can be collected via the devices. With increasing types and amounts of personal data that can be collected via modern devices, coupled with growing user awareness of its sensitivity and the need to comply with applicable privacy laws and regulations, the number of permissions in the permissions manager continues to proliferate. Current permissions manager UIs present all users with the entire list of permissions in a fixed order set by the OS. However, as our findings highlight, users do not consider all permissions equally important and prioritize them according to their utility and privacy sensitivity for their usage contexts. We further found that the absolute and relative judgments of importance for most of the permissions vary across users. Importantly, we surface unclear permission labels and mismatches in the mapping between a permission and the data it controls as the two leading causes of misunderstandings regarding how a permission operates. Our findings complement the findings from studies of user interaction with runtime permission requests for individual permissions and provide a unifying view across all permissions available to users. Our insight could be applied broadly to enhance the design of permissions managers in interactive devices and platforms by creating interactive experiences that are more efficient and personally relevant.

Author Contributions

CRediT:
Manila Devaraja: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Resources, Visualization, Writing – original draft, Writing – review & editing;
Sameer Patil: Conceptualization, Data curation, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing

Acknowledgments

We thank the participants of the study for their time and effort. Thanks are due to Ellery Gresham and Annabelle Warner for their help in coding the open-ended responses. We are grateful to those who piloted the study and suggested improvements. We acknowledge the anonymous reviewers and the participants of the Human-Centered Computing seminar at the University of Utah for their feedback and comments. We wish to thank Khawar Murad Ahmed, Sara Nurollahian, Hrishikesh Pachlag, and Brandt Redd for their extensive feedback on paper drafts and Farhana Khan for helping refine the presentation of the figures. The research reported in this paper was supported by the National Science Foundation award #2219354. The contents of the paper are the work of the authors and do not necessarily reflect the views of the sponsors.

References

[1] Paarijaat Aditya, Bobby Bhattacharjee, Peter Druschel, Viktor Erdélyi, and Matthew Lentz. 2014. Brave new world: Privacy risks for mobile users. In *Proceedings of the ACM MobiCom Workshop on Security and Privacy in Mobile Environments* (Maui, HI, USA) *(SPME '14)*. Association for Computing Machinery, New York, NY, USA, 7–12. doi:10.1145/2646584.2646585

[2] Nourah Alshomrani, Steven Furnell, and Ying He. 2023. Assessing User Understanding, Perception and Behaviour with Privacy and Permission Settings, In HCI for Cybersecurity, Privacy and Trust, Held as Part of the 25th HCI International Conference, HCII 2023, Abbas Moallem (Ed.). *Lecture Notes in Computer Science* 14045, 557–575. doi:10.1007/978-3-031-35822-7_36

[3] Haya Altuwaijri and Sanaa Ghouzali. 2020. Android data storage security: A review. *Journal of King Saud University - Computer and Information Sciences* 32, 5 (2020), 543–552. doi:10.1016/j.jksuci.2018.07.004

[4] Panagiotis Andriotis, Martina Angela Sasse, and Gianluca Stringhini. 2016. Permissions snapshots: Assessing users' adaptation to the Android runtime permission model. In *2016 IEEE International Workshop on Information Forensics and Security* (Abu Dhabi, UAE) *(WIFS 2016)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 1–6. doi:10.1109/WIFS.2016.7823922

[5] Android. 2020. App privacy labels now live on the App Store. https://developer.apple.com/news/?id=3wann9gh Accessed: 2025-06-23.

[6] Android. 2025. Android privacy settings and permissions. https://www.android.com/intl/en_us/safety/privacy/ Accessed: 2025-06-23.

[7] Android Developer Documentation. 2025. Auto-reset permissions from unused apps. https://developer.android.com/about/versions/11/privacy/permissions#auto-reset Accessed: 2025-06-23.

[8] Android Help. 2025. Change app permissions on your Android phone. https://support.google.com/android/answer/9431959 Accessed: 2025-06-23.

[9] Sarah Anrijs, Koen Ponnet, and Lieven De Marez. 2020. Development and psychometric properties of the Digital Difficulties Scale (DDS): An instrument to measure who is disadvantaged to fulfill basic needs by experiencing

difficulties in using a smartphone or computer. *PLOS ONE* 15, 5, Article e0233891 (May 2020), 15 pages. doi:10.1371/journal.pone.0233891

[10] Apple Developer Documentation. 2025. Requesting access to protected resources. https://developer.apple.com/documentation/uikit/requesting-access-to-protected-resources Accessed: 2025-06-23.

[11] Apple Support. 2025. About App Privacy Report. https://support.apple.com/en-us/102188 Accessed: 2025-06-23.

[12] Apple Support. 2025. About privacy and Location Services in iOS, iPadOS, and watchOS. https://support.apple.com/en-us/102515 Accessed 2025-06-23.

[13] Mehrnaz Ataei, Auriol Degbelo, and Christian Kray. 2018. Privacy theory in practice: Designing a user interface for managing location privacy on mobile devices. *Journal of Location Based Services* 12, 3–4 (2018), 141–178. doi:10.1080/17489725.2018.1511839

[14] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. 2018. A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces* (Tokyo, Japan) *(IUI '18)*. Association for Computing Machinery, New York, NY, USA, 165–176. doi:10.1145/3172944.3172982

[15] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little brothers watching you": Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, UK) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. doi:10.1145/2501604.2501616

[16] Florian Bemmann and Sven Mayer. 2024. The Impact of Data Privacy on Users' Smartphone App Adoption Decisions. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 278 (Sept. 2024), 23 pages. doi:10.1145/3676525

[17] Florian Bemmann, Helena Stoll, and Sven Mayer. 2024. Privacy Slider: Fine-Grain Privacy Control for Smartphones. *Proc. ACM Hum.-Comput. Interact.* 8, MHCI, Article 272 (Sept. 2024), 31 pages. doi:10.1145/3676519

[18] Gergely Biczók and Pern Hui Chia. 2013. Interdependent Privacy: Let Me Share Your Data, In Financial Cryptography and Data Security (FC 2013) (Okinawa, Japan), Ahmad-Reza Sadeghi (Ed.). *Lecture Notes in Computer Science* 7859, 338–353. doi:10.1007/978-3-642-39884-1_29

[19] Patrick Bombik, Tom Wenzel, Jens Grossklags, and Sameer Patil. 2022. A multi-region investigation of the perceptions and use of smart home devices. *Proceedings on Privacy Enhancing Technologies* 2022, 3 (2022), 6–32. doi:10.56553/popets-2022-0060

[20] Kerstin Bongard-Blanchy, Jean-Louis Sterckx, Arianna Rossi, Verena Distler, Salvador Rivas, and Vincent Koenig. 2022. An (Un)Necessary Evil - Users' (Un)Certainty about Smartphone App Permissions and Implications for Privacy Engineering. In *2022 IEEE European Symposium on Security and Privacy Workshops* (Genoa, Italy) *(EuroS&PW 2022)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 1–8. doi:10.1109/EuroSPW55150.2022.00023

[21] Jan Lauren Boyles, Aaron Smith, and Mary Madden. 2012. Privacy and Data Management on Mobile Devices. (Sep 2012). https://www.pewresearch.org/internet/2012/09/05/privacy-and-data-management-on-mobile-devices/

[22] Virginia Braun and Victoria Clarke and. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. doi:10.1191/1478088706qp063oa

[23] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2019. Thematic Analysis. In *Handbook of Research Methods in Health Social Sciences*, Pranee Liamputtong (Ed.). Springer Singapore, Singapore, 843–860. doi:10.1007/978-981-10-5251-4_103

[24] Christoph Buck and Simone Burster. 2017. App Information Privacy Concerns. In *2017 Americas Conference on Information Systems* (Boston, MA, USA) *(AMCIS 2017)*. Association for Information Systems, Atlanta, GA, USA. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/17

[25] Weicheng Cao, Chunqiu Xia, Sai Teja Peddinti, David Lie, Nina Taft, and Lisa M. Austin. 2021. A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. In *30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association, 803–820. https://www.usenix.org/conference/usenixsecurity21/presentation/cao-weicheng

[26] Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. 2012. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 1, 16 pages. doi:10.1145/2335356.2335358

[27] Robert E. Crossler and France Bélanger. 2019. Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. *Information Systems Research* 30, 3 (2019), 995–1006. doi:10.1287/isre.2019.0846

[28] Michalis Diamantaris, Elias P. Papadopoulos, Evangelos P. Markatos, Sotiris Ioannidis, and Jason Polakis. 2019. REAPER: Real-time App Analysis for Augmenting the Android Permission System. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy* (Richardson, TX, USA) *(CODASPY '19)*. Association for Computing Machinery, New York, NY, USA, 37–48. doi:10.1145/3292006.3300027

[29] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice Architecture and Smartphone Privacy: There's a Price for That. In *The Economics of Information Security and Privacy*, Rainer Böhme (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 211–236. doi:10.1007/978-3-642-39498-0_10

[30] Yusra Elbitar, Alexander Hart, and Sven Bugiel. 2025. The Power of Words: A Comprehensive Analysis of Rationales and Their Effects on Users' Permission Decisions. In *The Network and Distributed System Security Symposium* (San Diego, CA, USA) *(NDSS 2025)*. 18 pages. doi:10.14722/ndss.2025.230544

[31] Yusra Elbitar, Michael Schilling, Trung Tin Nguyen, Michael Backes, and Sven Bugiel. 2021. Explanation Beats Context: The Effect of Timing & Rationales on Users' Runtime Permission Decisions. In *30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association, 785–802. https://www.usenix.org/conference/usenixsecurity21/presentation/elbitar

[32] Kassem Fawaz and Kang G. Shin. 2014. Location Privacy Protection for Smartphone Users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, AZ, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 239–250. doi:10.1145/2660267.2660270

[33] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. doi:10.1145/2335356.2335360

[34] Suzanne Frey. 2022. Get more information about your apps in Google Play. https://blog.google/products/google-play/data-safety/ Accessed: 2025-06-23.

[35] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 407, 24 pages. doi:10.1145/3491102.3517504

[36] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2019. Privacy perception and user behavior in the mobile ecosystem. In *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good* (Valencia, Spain) *(GoodTechs '19)*. Association for Computing Machinery, New York, NY, USA, 177–182. doi:10.1145/3342428.3342690

[37] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. Privacy Perception when Using Smartphone Applications. *Mobile Networks and Applications* 25, 3 (2020), 1055–1061. doi:10.1007/s11036-020-01529-z

[38] Jason I. Hong, Yuvraj Agarwal, Matt Fredrikson, Mike Czapik, Shawn Hanna, Swarup Sahoo, Judy Chun, Won-Woo Chung, Aniruddh Iyer, Ally Liu, Shen Lu, Rituparna Roychoudhury, Qian Wang, Shan Wang, Siqi Wang, Vida Zhang, Jessica Zhao, Yuan Jiang, Haojian Jin, Sam Kim, Evelyn Kuo, Tianshi Li, Jinping Liu, Yile Liu, and Robert Zhang. 2021. The Design of the User Interfaces for Privacy Enhancements for Android. arXiv:2104.12032 [cs.CR] doi:10.48550/arXiv.2104.12032

[39] iPhone User Guide. 2025. Control access to your contacts on iPhone. https://support.apple.com/en-gb/guide/iphone/iph9536aa9a5/ios#:~:text=On%20iPhone%2C%20you%20control%20which,individual%20contacts%2C%20then%20tap%20Done. Accessed: 2025-06-23.

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

[41] Manoel Pereira Junior, Simone Isabela de Rezende Xavier, and Raquel Oliveira Prates. 2014. Investigating the Use of a Simulator to Support Users in Anticipating Impact of Privacy Settings in Facebook. In *Proceedings of the 2014 ACM International Conference on Supporting Group Work* (Sanibel Island, Florida, USA) *(GROUP '14)*. Association for Computing Machinery, New York, NY, USA, 63–72. doi:10.1145/2660398.2660419

[42] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone, In Financial Cryptography and Data Security (FC 2012) (Bonaire), Jim Blyth, Sven Dietrich, and L. Jean Camp (Eds.). *Lecture Notes in Computer Science* 7398, 68–79. doi:10.1007/978-3-642-34638-5_6

[43] Rehana Masrur Khan and Masrur Alam Khan. 2007. Academic Sojourners, Culture Shock and Intercultural Adaptation: A Trend Analysis. *Studies About Languages* (2007), 38–46. Issue 10.

[44] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2023. Comparing Privacy Labels of Applications in Android and iOS. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society* (Copenhagen, Denmark) *(WPES '23)*. Association for Computing Machinery, New York, NY, USA, 61–73. doi:10.1145/3603216.3624967

[45] Asma Khatoon and Peter Corcoran. 2017. Android permission system and user privacy — A review of concept and approaches. In *2017 IEEE 7th International Conference on Consumer Electronics - Berlin* (Berlin, Germany) *(ICCE-Berlin 2017)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 153–158. doi:10.1109/ICCE-Berlin.2017.8210616

[46] Jennifer King. 2013. “How Come I’m Allowing Strangers To Go Through My Phone?”—Smartphones and Privacy Expectations. In *Eighth Symposium on Usable Privacy and Security (SOUPS ’12) Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM)* (Washington, D.C., USA). 14 pages. doi:10.2139/ssrn.2493412

[47] Bart P. Knijnenburg. 2017. Privacy? I Can’t Even! Making a Case for User-Tailored Privacy. *IEEE Security & Privacy* 15, 4 (2017), 62–67. doi:10.1109/MSP.2017.3151331

[48] Bart P. Knijnenburg, Reza Ghaiumy Anaraky, Daricia Wilkinson, Moses Namara, Yangyang He, David Cherry, and Erin Ash. 2022. User-Tailored Privacy. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing, Cham, 367–393. doi:10.1007/978-3-030-82786-1_16

[49] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Preference-based location sharing: Are more privacy options really better?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI ’13)*. Association for Computing Machinery, New York, NY, USA, 2667–2676. doi:10.1145/2470654.2481369

[50] Sylvia Kowalewski, Martina Ziefle, Henrik Ziegeldorf, and Klaus Wehrle. 2015. Like us on Facebook! – Analyzing User Preferences Regarding Privacy Settings in Germany. *Procedia Manufacturing* 3 (2015), 815–822. doi:10.1016/j.promfg.2015.07.336 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015.

[51] Rena Lavranou, Stylianos Karagiannis, Aggeliki Tsohou, and Emmanouil Magkos. 2023. Unraveling the Complexity of Mobile Application Permissions: Strategies to Enhance Users’ Privacy Education. *European Journal of Engineering and Technology Research* 1, CIE (Dec 2023), 87–95. doi:10.24018/ejeng.2023.1.CIE.3141

[52] Yuanchun Li, Yao Guo, and Xiangqun Chen. 2016. PERUIM: Understanding mobile application privacy with permission-UI mapping. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Heidelberg, Germany) *(UbiComp ’16)*. Association for Computing Machinery, New York, NY, USA, 682–693. doi:10.1145/2971648.2971693

[53] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy 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* (Pittsburgh, PA, USA) *(UbiComp ’12)*. Association for Computing Machinery, New York, NY, USA, 501–510. doi:10.1145/2370216.2370290

[54] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. 2014. Modeling Users’ Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *10th Symposium On Usable Privacy and Security* (Menlo Park, CA, USA) *(SOUPS 2014)*. USENIX Association, 199–212. https://www.usenix.org/conference/soups2014/proceedings/presentation/lin

[55] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. 2024. Data Safety vs. App Privacy: Comparing the Usability of Android and iOS Privacy Labels. *Proceedings on Privacy Enhancing Technologies* 2024 (2024), 182–210. Issue 2. doi:10.56553/popets-2024-0047

[56] David Machin, Michael J. Campbell, Say Beng Tan, and Sze Huey Tan. 2018. *Sample Sizes for Clinical, Laboratory and Epidemiology Studies*. John Wiley & Sons Ltd., Hoboken, NJ, USA. doi:10.1002/9781118874905

[57] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won’t You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 437 (oct 2021), 35 pages. doi:10.1145/3479581

[58] Nurul Momen, Sven Bock, and Lothar Fritsch. 2020. Accept - Maybe - Decline: Introducing Partial Consent for the Permission-based Access Control Model of Android. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies* (Barcelona, Spain) *(SACMAT ’20)*. Association for Computing Machinery, New York, NY, USA, 71–80. doi:10.1145/3381991.3395603

[59] Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux. 2017. SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices. In *2017 IEEE Symposium on Security and Privacy* (San Jose, CA, USA) *(IEEE S&P 2017)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 1058–1076. doi:10.1109/SP.2017.25

[60] Aswati Panicker, Novia Nurain, Zaidat Ibrahim, Chun-Han (Ariel) Wang, Seung Wan Ha, Elizabeth Kaziunas, Maria K. Wolters, and Chia-Fang Chung. 2024. Forms of Fraudulence in Human-Centered Design: Collective Strategies and Future Agenda for Qualitative HCI Research. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA ’24)*. Association for Computing Machinery, New York, NY, USA, Article 469, 5 pages. doi:10.1145/3613905.3636309

[61] Sarah Prange, Pascal Knierim, Gabriel Knoll, Felix Dietz, Alexander De Luca, and Florian Alt. 2024. “I do (not) need that Feature!” – Understanding Users’ Awareness and Control of Privacy Permissions on Android Smartphones. In *Twentieth Symposium on Usable Privacy and Security* (Philadelphia, PA, USA) *(SOUPS 2024)*. USENIX Association, 453–472. https://www.usenix.org/conference/soups2024/presentation/prange

[62] David Schmidt, Alexander Ponticello, Magdalena Steinböck, Katharina Krombholz, and Martina Lindorfer. 2025. Analyzing the iOS Local Network Permission from a Technical and User Perspective. In *2025 IEEE Symposium on Security and Privacy* (San Francisco, CA, USA) *(IEEE S&P 2025)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 4229–4247. doi:10.1109/SP61157.2025.00045

[63] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can Systems Explain Permissions Better? Understanding Users' Misperceptions under Smartphone Runtime Permission Model. In *30th USENIX Security Symposium (USENIX Security '21)*. USENIX Association, 751–768. https://www.usenix.org/conference/usenixsecurity21/presentation/shen-bingyu

[64] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy Tipping Points in Smartphones Privacy Preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 807–816. doi:10.1145/2702123.2702404

[65] Miriam Sturdee, Lauren Thornton, Bhagya Wimalasiri, and Sameer Patil. 2021. A Visual Exploration of Cybersecurity Concepts. In *Proceedings of the 13th Conference on Creativity and Cognition* (Virtual Event, Italy) *(C&C '21)*. Association for Computing Machinery, New York, NY, USA, Article 46, 10 pages. doi:10.1145/3450741.3465252

[66] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. 2017. Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences. In *Thirteenth Symposium on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS 2017)*. USENIX Association, 145–162. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/tsai

[67] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, and Nigel Shadbolt. 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, CO, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5208–5220. doi:10.1145/3025453.3025556

[68] Anthony Vance, Jeffrey L. Jenkins, Bonnie Brinton Anderson, Daniel K. Bjornn, and C. Brock Kirwan. 2018. Tuning out security warnings: a longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Q.* 42, 2 (June 2018), 355–380. doi:10.25300/MISQ/2018/14124

[69] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In *2017 IEEE Symposium on Security and Privacy* (San Jose, CA, USA) *(IEEE S&P 2017)*. Institute for Electrical and Electronics Engineers, Los Alamitos, CA, USA, 1077–1093. doi:10.1109/SP.2017.51

[70] Yun Zhou, Alexander Raake, Tao Xu, and Xuyun Zhang. 2017. Users' Perceived Control, Trust and Expectation on Privacy Settings of Smartphone, In Cyberspace Safety and Security (CSS 2017), Sheng Wen, Wei Wu, and Aniello Castiglione (Eds.). *Lecture Notes in Computer Science* 10581, 427–441. doi:10.1007/978-3-319-69471-9_31

[71] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W. Freeh. 2011. Taming information-stealing smartphone applications (on Android), In Proceedings of the 4th International Conference on Trust and Trustworthy Computing (Trust 2011) (Pittsburgh, PA, USA), Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres (Eds.). *Lecture Notes in Computer Science* 6740, 93–107. doi:10.1007/978-3-642-21599-5_7

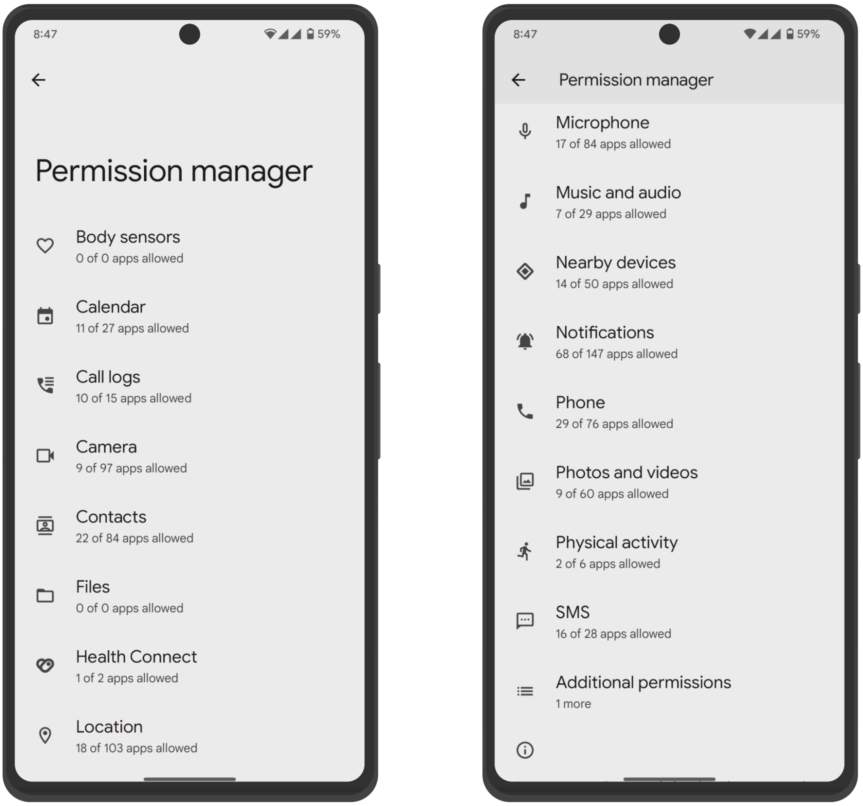
[72] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2023. "Revoked just now!" Users' Behaviors Toward Fitness-Data Sharing with Third-Party Applications. *Proceedings on Privacy Enhancing Technologies* 2023 (2023), 47–67. Issue 1. doi:10.56553/popets-2023-0004

[73] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2024. Our Data, Our Solutions: A Participatory Approach for Enhancing Privacy in Wearable Activity Tracker Third-Party Apps. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024), 734–754. doi:10.56553/popets-2024-0139

A Permissions Manager UIs

As a reference, we provide screenshots of the UIs of the permissions managers in Android 13.0 and iOS 17.4.1, respectively. Android uses the term ‘Permission manager’ to refer to the UI for adjusting permissions, while iOS labels it as ‘Privacy & Security.’

A.1 Android



8:47 59%

Permission manager

Body sensors
0 of 0 apps allowed

Calendar
11 of 27 apps allowed

Call logs
10 of 15 apps allowed

Camera
9 of 97 apps allowed

Contacts
22 of 84 apps allowed

Files
0 of 0 apps allowed

Health Connect
1 of 2 apps allowed

Location
18 of 103 apps allowed

8:47 59%

Permission manager

Microphone
17 of 84 apps allowed

Music and audio
7 of 29 apps allowed

Nearby devices
14 of 50 apps allowed

Notifications
68 of 147 apps allowed

Phone
29 of 76 apps allowed

Photos and videos
9 of 60 apps allowed

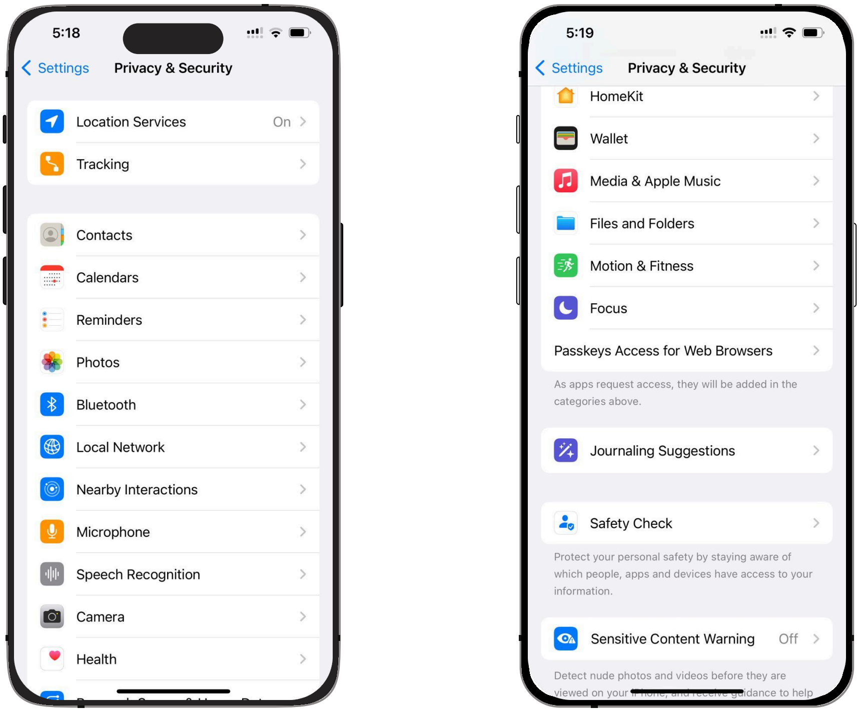
Physical activity
2 of 6 apps allowed

SMS
16 of 28 apps allowed

Additional permissions
1 more

Fig. A.1. Screenshots showing the list of all permissions available to users in the permissions manager UI of Android 13.0.

A.2 iOS



5:18

< Settings Privacy & Security

Location Services On >

Tracking >

Contacts >

Calendars >

Reminders >

Photos >

Bluetooth >

Local Network >

Nearby Interactions >

Microphone >

Speech Recognition >

Camera >

Health >

5:19

< Settings Privacy & Security

HomeKit >

Wallet >

Media & Apple Music >

Files and Folders >

Motion & Fitness >

Focus >

Passkeys Access for Web Browsers >

As apps request access, they will be added in the categories above.

Journaling Suggestions >

Safety Check >

Protect your personal safety by staying aware of which people, apps and devices have access to your information.

Sensitive Content Warning Off >

Detect nude photos and videos before they are viewed on your iPhone, and receive guidance to help

Fig. A.2. Screenshots showing the list of all permissions available to users in the permissions manager UI of iOS 17.4.1.

B Descriptions of Permission Settings

Android and iOS provide additional information about each permission. In the case of Android, the information is provided via the Android Help webpage at: https://support.google.com/android/answer/9431959. In iOS, information about each permission is provided on the screen users see when they invoke the screen for that permission from the permissions manager.

B.1 Android

Table B.1 provides the explanatory information about permissions as presented on the Android Help webpage at the time we conducted the research.

Table B.1. Descriptive information about each permission in Android 13.0 obtained from the Android Help webpage. The permissions are listed in the order in which they appear in the UI.

Permission	Description
Body sensors	Access sensor info about your vital signs.
Calendar	Access your calendar.
Call logs	Read and write your phone call log.
Camera	Take pictures and record videos.
Contacts	Access your contacts.
Files	Access all files on your device.
Health Connect	With this permission, applications can read and write your health and fitness data.
Location	Access your device’s location.
Microphone	Record audio.
Music and audio	Access music and other audio files on your device.
Nearby devices	Find, connect to, and determine the relative position of nearby devices.
Notifications	Send notifications.
Phone	Make and manage phone calls.
Photos and videos	Access photos and videos on your device.
Physical activity	Access your physical activity, like walking, biking, driving, step count, and more.
SMS	Send and check SMS messages.

B.2 iOS

Table B.2 provides the explanatory information about permissions that we gathered via the iOS UI screens at the time we conducted the research.

Table B.2. Descriptive information about each permission in iOS 17.4.1 obtained via the iOS UI screens. The permissions are listed in the order in which they appear in the UI.

Permission	**Description**
Location Services	Allows access to your location.
Tracking	Allow apps to track your activity across other companies' apps and websites.
Contacts	Access contacts on the phone.
Calendars	Access to Calendar events on the iPhone. Calendar events may include additional data such as locations, email addresses, or notes.
Reminders	Access to reminders on the phone.
Photos	Access to photos on the phone. Photos may contain data associated with location, depth information, captions, and audio.
Bluetooth	Access to the Bluetooth sensor to use third-party devices, such as wireless keyboards, headphones, speakers, car kits, game controllers, and more, with the phone.
Local Network	Allows apps to find and communicate with devices on your local network.
Nearby Interactions	Allows apps to measure the precise distance between your phone and other objects.
Microphone	Allows access to the microphone of the phone.
Speech Recognition	Allows apps to send voice data to Apple's servers to process what you said.
Camera	Access to the phone camera(s).
Health	Access to health data on the phone. Health data on the phone automatically records your step counts and walking and running distances.
Research Sensor & Usage Data	Enables the collection of data concerning how you interact with your device to later share with research studies.
HomeKit	HomeKit lets people securely control connected accessories in their homes using Siri or the Home app on the iPhone, iPad, Apple Watch, and Mac.
Wallet	Access to your Wallet, which allows you to securely store credit/debit cards, digital tickets, boarding passes, digital keys, and more in one place for easy access.
Media & Apple Music	Permission to access to your Apple Music subscription, your music and video activity, and your media library.
Files and Folders	Access to files and folders on the phone.
Motion & Fitness	Motion & Fitness tracking stores data on your device which can be used to estimate your body motion, mobility, step counts, stairs climbed, and more.
Focus	Tells apps that you have silenced notifications using Focus on the phone.

C Questionnaire

The complete questionnaire we used to gather the data for our research is included in the subsections below. The subsection titles are purely explanatory and were not shown to the participants.

Prior to answering the questionnaire, we provided participants with detailed information about the study to seek their informed consent for participation. Only those who consented to participate proceeded to answer the questionnaire.

C.1 Commitment

- We care about the quality of our data. In order for us to get the most accurate measures of your knowledge and opinions, it is important that you thoughtfully provide your best answers to each question in this study.
  Will you provide your best answers to each question in this study?
  ○ I will provide my best answers.
  ○ I will not provide my best answers.
  ○ I cannot promise either way.

C.2 Screening

- What is your worker ID for Amazon Mechanical Turk? [text box]

- What is your year of birth?
  [Dropdown of years from 1900 to 2023]

- How long have you lived in the United States?
  ○ Less than 1 year
  ○ Between 1 year and 2 years
  ○ Between 2 years and 3 years
  ○ Between 3 years and 4 years
  ○ Between 4 years and 5 years
  ○ Between 5 years and 6 years
  ○ Between 6 years and 7 years
  ○ Between 7 years and 8 years
  ○ Between 8 years and 9 years
  ○ Between 9 years and 10 years
  ○ More than 10 years but NOT all of my life
  ○ All my life
  ○ I do not live in the United States

- What is the operating system of your primary mobile phone?
  ○ Android (Google)
  ○ iOS (Apple)
  ○ Windows
  ○ I do not know
  ○ Something else (Please specify:) [text box]

C.3 Rating the Importance of Permissions

Following is a list of smartphone permission settings that allow or restrict apps from using specific information. For example, the location setting will allow or restrict access to information about the location of the phone when apps request location information.

Below is a list of permission settings available on typical smartphones, although not all of them may be present on your own device. Based on your best understanding of each permission setting, **please rate the following smartphone permission settings in terms of how important it is for you to control the information connected to the setting**, with 1 being the least important and 5 being the most important.

	Least important				Most important	
	1	2	3	4	5	I do not know this setting.
Bluetooth	○	○	○	○	○	○
Body Sensors	○	○	○	○	○	○
Calendar	○	○	○	○	○	○
Call Logs	○	○	○	○	○	○
Camera	○	○	○	○	○	○
Contacts	○	○	○	○	○	○
Files and Folders	○	○	○	○	○	○
Focus / Do Not Disturb	○	○	○	○	○	○
Health	○	○	○	○	○	○
HomeKit	○	○	○	○	○	○
Local Network	○	○	○	○	○	○
Location	○	○	○	○	○	○
Microphone	○	○	○	○	○	○
Music and Audio / Media	○	○	○	○	○	○
Nearby Devices	○	○	○	○	○	○
Nearby Interactions	○	○	○	○	○	○
Notifications	○	○	○	○	○	○
Phone	○	○	○	○	○	○
Photos and Videos	○	○	○	○	○	○
Physical Activity / Motion & Fitness	○	○	○	○	○	○
Reminders	○	○	○	○	○	○
Research Sensor & Usage Data	○	○	○	○	○	○
SMS	○	○	○	○	○	○
Speech Recognition	○	○	○	○	○	○
Tracking	○	○	○	○	○	○
Wallet	○	○	○	○	○	○

C.4 Ranking Most Important Permissions

Smartphone permission settings allow or restrict apps from using specific information. For example, the location setting will allow or restrict access to information about the location of the phone when apps request location information.

The dropdowns below list the permission settings available on typical smartphones, although not all of them may be present on your own device. Based on your best understanding of each permission setting, please specify the **top five most important** smartphone permission settings ranked based on their importance to you, with 1 being the most important, 2 being the next most important, and so on.

Please select a setting **only once** across the five dropdowns.

- 1 [Dropdown listing the 26 permissions included in Section C.3]
- 2 [Dropdown listing the 26 permissions included in Section C.3]
- 3 [Dropdown listing the 26 permissions included in Section C.3]
- 4 [Dropdown listing the 26 permissions included in Section C.3]
- 5 [Dropdown listing the 26 permissions included in Section C.3]

C.5 Ranking Least Important Permissions

Smartphone permission settings allow or restrict apps from using specific information. For example, the location setting will allow or restrict access to information about the location of the phone when apps request location information.

The dropdowns below list the permission settings available on typical smartphones, although not all of them may be present on your own device. Based on your best understanding of each permission setting, please specify the **top five least important** smartphone permission settings ranked based on their importance to you, with 1 being the least important, 2 being the next least important, and so on.

Please select a setting **only once** across the five dropdowns.

- 1 [Dropdown listing the 26 permissions included in Section C.3]
- 2 [Dropdown listing the 26 permissions included in Section C.3]
- 3 [Dropdown listing the 26 permissions included in Section C.3]
- 4 [Dropdown listing the 26 permissions included in Section C.3]
- 5 [Dropdown listing the 26 permissions included in Section C.3]

C.6 Reasons for Top-Ranked Permissions

We would like to know a bit more about the smartphone permission settings that are the **most** important to you.
[NOTE: We asked participants three of the questions below that corresponded to their top three choices in Section C.4: Ranking Most Important Permissions.]

- Why is **Bluetooth** an important setting for you? [Essay text box]
- Why is **Body Sensors** an important setting for you? [Essay text box]
- Why is **Calendar** an important setting for you? [Essay text box]
- Why is **Call Logs** an important setting for you? [Essay text box]
- Why is **Camera** an important setting for you? [Essay text box]
- Why is **Contacts** an important setting for you? [Essay text box]
- Why is **Files and Folders** an important setting for you? [Essay text box]
- Why is **Focus / Do Not Disturb** an important setting for you? [Essay text box]
- Why is **Health** an important setting for you? [Essay text box]
- Why is **HomeKit** an important setting for you? [Essay text box]
- Why is **Local Network** an important setting for you? [Essay text box]
- Why is **Location** an important setting for you? [Essay text box]
- Why is **Microphone** an important setting for you? [Essay text box]
- Why is **Music and Audio / Media** an important setting for you? [Essay text box]
- Why is **Nearby Devices** an important setting for you? [Essay text box]
- Why is **Nearby Interactions** an important setting for you? [Essay text box]
- Why is **Notifications** an important setting for you? [Essay text box]
- Why is **Phone** an important setting for you? [Essay text box]
- Why is **Photos and Videos** an important setting for you? [Essay text box]

- Why is **Physical Activity / Motion & Fitness** an important setting for you? [Essay text box]
- Why is **Reminders** an important setting for you? [Essay text box]
- Why is **Research Sensor & Usage Data** an important setting for you? [Essay text box]
- Why is **SMS** an important setting for you? [Essay text box]
- Why is **Speech Recognition** an important setting for you? [Essay text box]
- Why is **Tracking** an important setting for you? [Essay text box]
- Why is **Wallet** an important setting for you? [Essay text box]

C.7 Reasons for Bottom-Ranked Permissions

We would like to know a bit more about the smartphone permission settings that are the **least** important to you.
[NOTE: We asked participants three of the questions below that corresponded to their top three choices in Section C.5: Ranking Least Important Permissions.]

- Why is **Bluetooth** a less important setting for you? [Essay text box]
- Why is **Body Sensors** a less important setting for you? [Essay text box]
- Why is **Calendar** a less important setting for you? [Essay text box]
- Why is **Call Logs** a less important setting for you? [Essay text box]
- Why is **Camera** a less important setting for you? [Essay text box]
- Why is **Contacts** a less important setting for you? [Essay text box]
- Why is **Files and Folders** a less important setting for you? [Essay text box]
- Why is **Focus / Do Not Disturb** a less important setting for you? [Essay text box]
- Why is **Health** a less important setting for you? [Essay text box]
- Why is **HomeKit** a less important setting for you? [Essay text box]
- Why is **Local Network** a less important setting for you? [Essay text box]
- Why is **Location** a less important setting for you? [Essay text box]
- Why is **Microphone** a less important setting for you? [Essay text box]
- Why is **Music and Audio / Media** a less important setting for you? [Essay text box]
- Why is **Nearby Devices** a less important setting for you? [Essay text box]
- Why is **Nearby Interactions** a less important setting for you? [Essay text box]
- Why is **Notifications** a less important setting for you? [Essay text box]
- Why is **Phone** a less important setting for you? [Essay text box]
- Why is **Photos and Videos** a less important setting for you? [Essay text box]
- Why is **Physical Activity / Motion & Fitness** a less important setting for you? [Essay text box]
- Why is **Reminders** a less important setting for you? [Essay text box]
- Why is **Research Sensor & Usage Data** a less important setting for you? [Essay text box]
- Why is **SMS** a less important setting for you? [Essay text box]
- Why is **Speech Recognition** a less important setting for you? [Essay text box]
- Why is **Tracking** a less important setting for you? [Essay text box]
- Why is **Wallet** a less important setting for you? [Essay text box]

C.8 Comprehension of Permission Operation

The following questions pertain to your **expectations** regarding **three** of the permission settings available on typical smartphones, although not all of them may be present on your own device. [NOTE: We asked participants three of the questions below chosen at random from the set of 26 questions covering the 26 permission settings included in Section C.3. Prior to choosing the questions, we excluded the questions corresponding to the permissions for which participants chose the 'I do not know this setting' option when rating the permissions (see Section C.3: Rating the Importance of Permissions).]

- What do you believe the **Bluetooth** setting controls? [Essay text box]
- What do you believe the **Body Sensors** setting controls? [Essay text box]
- What do you believe the **Calendar** setting controls? [Essay text box]
- What do you believe the **Call Logs** setting controls? [Essay text box]
- What do you believe the **Camera** setting controls? [Essay text box]
- What do you believe the **Contacts** setting controls? [Essay text box]
- What do you believe the **Files and Folders** setting controls? [Essay text box]
- What do you believe the **Focus / Do Not Disturb** setting controls? [Essay text box]
- What do you believe the **Health** setting controls? [Essay text box]
- What do you believe the **HomeKit** setting controls? [Essay text box]
- What do you believe the **Local Network** setting controls? [Essay text box]
- What do you believe the **Location** setting controls? [Essay text box]
- What do you believe the **Microphone** setting controls? [Essay text box]
- What do you believe the **Music and Audio / Media** setting controls? [Essay text box]
- What do you believe the **Nearby Devices** setting controls? [Essay text box]
- What do you believe the **Nearby Interactions** setting controls? [Essay text box]
- What do you believe the **Notifications** setting controls? [Essay text box]
- What do you believe the **Phone** setting controls? [Essay text box]
- What do you believe the **Photos and Videos** setting controls? [Essay text box]
- What do you believe the **Physical Activity / Motion & Fitness** setting controls? [Essay text box]
- What do you believe the **Reminders** setting controls? [Essay text box]
- What do you believe the **Research Sensor & Usage Data** setting controls? [Essay text box]
- What do you believe the **SMS** setting controls? [Essay text box]
- What do you believe the **Speech Recognition** setting controls? [Essay text box]
- What do you believe the **Tracking** setting controls? [Essay text box]
- What do you believe the **Wallet** setting controls? [Essay text box]

C.9 Permissions-related Practices

- What kind of lock do you have on your mobile phone? (*Select all that apply.*)
  □ Fingerprint
  □ Face recognition
  □ Password (Alphanumeric)
  □ Pattern
  □ PIN (Numbers only)
  □ No lock
  □ Something else (Please specify:) [text box]

- Do you install apps from a source other than the official app store?
  ○ Never ○ Rarely ○ Sometimes ○ Often ○ Always

- While installing an app from the app store, do you read app permissions (if available in the app description)?
  ○ Never ○ Rarely ○ Sometimes ○ Often ○ Always

- How often do you change app permissions in the Settings menu of your mobile phone?
  ○ Never ○ Rarely ○ Sometimes ○ Often ○ Always

- If an app asks for a permission (e.g., location, contacts, etc.) that you think is not justified, what is your approach?
  ○ Allow the permission anyway
  ○ Allow the permission only if not allowing it makes the app dysfunctional or hampers some feature I want to use.
  ○ Deny the permission
  ○ Something else (Please specify:) [text box]

- Recent versions of Android can automatically remove permissions from unused apps.
  Have you encountered this feature?
  [NOTE: The question was asked only to participants who primarily used Android.]
  ○ Yes
  ○ No
  ○ I'm not sure
  ○ Something else (Please specify:) [text box]

- [If the participant selected 'Yes' for the question 'Recent versions of Android can automatically remove permissions from unused apps. Have you encountered this feature?,' then ask:]
  What are your thoughts on the feature that automatically removes permissions from unused apps? [text box]

- Recent versions of iOS provide an App Privacy Report that details how often apps access your data.
  How often have you used this feature?
  [NOTE: The question was asked only to participants who primarily used iOS.]
  ○ Once a day
  ○ Once a week
  ○ Once a month
  ○ A few times a year
  ○ Once a year
  ○ Heard of this feature but never used it
  ○ Never heard of this feature
  ○ Something else (Please specify:) [text box]

C.10 Technical Efficacy

[NOTE: The following items were taken from the *General Digital Difficulties (GDD)* subscale of the Digital Difficulties Scale [9]. We randomized the order in which the items were presented to the participants.]

To what extent do you agree with the following statements?
[Options: *Disagree*, *Rather Disagree*, *Neither Disagree nor Agree*, *Rather Agree*, *Agree*]

- In general, I often have difficulty when using my smartphone, apps, websites, or computer programs.

- In general, I am not able to solve questions or problems on my own when using my smartphone, apps, websites, or computer programs.
- In general, I need support when trying out something new on my smartphone or computer.
- In general, I find it hard to adjust settings of my smartphone, apps, websites, or computer programs (for example, privacy or safety settings).
- In general, I often have questions or problems when using my smartphone, apps, websites, or computer programs after an update has been done.

[NOTE: The following items were taken from the *Worries about Future Digital Difficulties (WFDD)* subscale of the Digital Difficulties Scale [9]. We randomized the order in which the items were presented to the participants.]

Please answer the following questions based on the past six months.
[Options: *(Almost) Never*, *Rarely*, *Sometimes*, *Often*, *Very Often*]

- How often do you worry that you will be unable to keep up with ongoing changes in smartphones, apps, websites, or computer programs in the future?
- How often do you worry that future developed smartphones, apps, websites, or computer programs will be too difficult for you to use?
- How often do you worry that you will find it hard to keep up with the use of smartphones, apps, websites, or computer programs in the future?

C.11 Privacy Concerns

[NOTE: The following items were taken from the App Information Privacy Concerns (AIPC) scale [24]. We randomized the order in which the items were presented to the participants.]

Please indicate the extent to which you agree with each of the following statements:
[Options: Strongly Agree, Agree, Somewhat Agree, Neither Agree nor Disagree, Somewhat Disagree, Disagree, Strongly Disagree]

- Mobile app privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. [NOTE: *Requirements* subscale]
- Control of personal information lies at the heart of mobile app users' privacy. [NOTE: *Requirements* subscale]
- I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want. [NOTE: *Anxiety* subscale]
- I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy. [NOTE: *Anxiety* subscale]
- Mobile app providers seeking information online should disclose the way the data are collected, processed, and used. [NOTE: *Requirements* subscale]
- A good privacy policy for mobile app users should have a clear and conspicuous disclosure. [NOTE: *Requirements* subscale]
- It is very important to me that I am aware and knowledgeable about how my personal information will be used. [NOTE: *Personal attitude* subscale]
- It usually bothers me when mobile apps ask me for personal information. [NOTE: *Requirements* subscale]

- When mobile apps ask me for personal information, I sometimes think twice before providing it. [NOTE: *Personal attitude* subscale]
- I am concerned that mobile apps may monitor my activities on my mobile device. [NOTE: *Anxiety* subscale]
- I am concerned that mobile apps are collecting too much information about me. [NOTE: *Anxiety* subscale]
- I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization. [NOTE: *Anxiety* subscale]
- When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes. [NOTE: *Anxiety* subscale]
- I am concerned that mobile apps may share my personal information with other entities without getting my authorization. [NOTE: *Anxiety* subscale]
- Compared to others, I am more sensitive about the way mobile app providers handle my personal information. [NOTE: *Personal attitude* subscale]
- To me, it is the most important thing to keep my privacy intact from app providers. [NOTE: *Personal attitude* subscale]
- I am concerned about threats to my personal privacy today. [NOTE: *Anxiety* subscale]

[NOTE: The following item was embedded within the above items as an attention check:
'Please select disagree in response to this item to show that you are reading carefully.']

C.12 Demographics

- What is your age (in years)?
  [Dropdown of ages from 1 to 120]

- What is your gender?
  ○ Man
  ○ Woman
  ○ Non-binary
  ○ Prefer to self-describe: [text box]
  ○ Something else (Please specify:) [text box]

- What is your ethnicity? (*Select all the apply.*)
  □ American Indian or Native American
  □ Asian
  □ Black or African American
  □ Hispanic
  □ Native Hawaiian or Other Pacific Islander
  □ White / Caucasian
  □ Something else (Please specify:) [text box]
  □ Do not wish to specify

- Are you a student?
  ○ Yes
  ○ No

- What is the highest level of education you have completed? (*If currently enrolled, highest degree received.*)
  ○ Less than high school
  ○ Some high school

- ○ High school diploma
- ○ Vocational training
- ○ Some college but no degree
- ○ College graduate (B.S., B.A., or other 4 year degree)
- ○ Master's degree or Professional degree (e.g., Law, Medicine, Business, etc.)
- ○ Doctoral degree
- ○ Something else (Please specify:) [text box]

- Which one of the following companies does not make mobile phones?
  [NOTE: This question was an attention check.]
  - ○ Apple
  - ○ Google
  - ○ Samsung
  - ○ Nokia
  - ○ Whole Foods

- What is/was your major field of study? [text box]

- What is your current employment status? (*Select all that apply.*)
  - □ Employed full-time
  - □ Employed part-time
  - □ Unemployed looking for work
  - □ Unemployed not looking for work
  - □ Homemaker
  - □ Retired
  - □ Disabled
  - □ Unable to work
  - □ Prefer not to say
  - □ Something else. (Please specify:) [text box]

- [If the participant selected 'Employed full-time,''Employed part-time,' 'Unemployed looking for work,' or 'Retired' as the answer for the question 'What is your current employment status?,' then ask:]
  What is/was your occupation? [text box]

- What is your current annual household income?
  - ○ Less than $10,000
  - ○ $10,000 - $19,999
  - ○ $20,000 - $29,999
  - ○ $30,000 - $39,999
  - ○ $40,000 - $49,999
  - ○ $50,000 - $59,999
  - ○ $60,000 - $69,999
  - ○ $70,000 - $79,999
  - ○ $80,000 - $89,999
  - ○ $90,000 - $99,999
  - ○ $100,000 - $149,999
  - ○ More than $150,000
  - ○ Do not wish to specify

- Which of the following best describes the locality where you live?
  - ○ Urban
  - ○ Suburban
  - ○ Rural
- What is your current relationship status?
  - ○ Single, never married
  - ○ Married
  - ○ Widowed
  - ○ Divorced
  - ○ Separated
  - ○ Something else (Please specify:) [text box]
- How many children do you have?
  - ○ 0
  - ○ 1
  - ○ 2
  - ○ 3
  - ○ 4
  - ○ More than 4
  - ○ Do not wish to specify

C.13 Commitment Verification

- Did you answer all questions in the study according to the provided instructions?
  Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.
  - ○ I answered all questions according to the provided instructions.
  - ○ I sometimes chose random answer options because I was not motivated to answer the question or did not know how to answer it.
  - ○ I often chose random answer options because I wanted to finish as quickly as possible.
- Did you complete the questionnaire without distractions?
  Please answer honestly. Your answer has NO consequences for you or the compensation you will receive.
  - ○ I completed the study with full attention.
  - ○ I was sometimes distracted (by people, noises, etc.).
  - ○ I was often distracted (by people, noises, etc.).

C.14 Feedback

Finally, we would appreciate your feedback on the questionnaire.

- Do you have any suggestions for improving the questionnaire? [Essay text box]
- Is there anything else you would like to tell us? [Essay text box]

C.15 Conclusion

Thank you for participating in the study. We appreciate your time and effort.
Your study completion code is: [randomly generated 8-digit number].
Please copy the above code and enter it on Amazon Mechanical Turk.
Note that you need to enter the code correctly to receive credit for participating in the study.