"I do (not) need that Feature!" – Understanding Users' Awareness and Control of Privacy Permissions on Android Smartphones

Sarah Prange[1], Pascal Knierim[2], Gabriel Knoll[3], Felix Dietz[1], Alexander De Luca[4], Florian Alt[1]

[1]*University of the Bundeswehr Munich, Germany, {firstname.lastname}@unibw.de*
[2]*University of Innsbruck, Austria {firstname.lastname}@uibk.ac.at*
[3]*LMU Munich, Germany, {firstname.lastname}@campus.lmu.de*
[4]*Google Munich, Germany*

Abstract

We present the results of the first field study ($N = 132$) investigating users' (1) *awareness* of Android privacy permissions granted to installed apps and (2) *control behavior* over these permissions. Our research is motivated by many smartphone features and apps requiring access to personal data. While Android provides privacy permission management mechanisms to control access to this data, its usage is not yet well understood. To this end, we built and deployed an Android application on participants' smartphones, acquiring data on actual privacy permission states of installed apps, monitoring permission changes, and assessing reasons for changes using experience sampling. The results of our study show that users often conduct multiple revocations in short time frames, and revocations primarily affect rarely used apps or permissions non-essential for apps' core functionality. Our findings can inform future (proactive) privacy control mechanisms and help target opportune moments for supporting privacy control.

1 Introduction

For many years, the decision of what data is collected, processed, and potentially shared with third parties had been the sole decision of the app or service provider, with many Android apps requesting more permissions than necessary in the past [38]. Users unwilling to share the requested data could only make a simple choice – installing or not installing the app or service. More recently, a trend can be observed towards designing apps and services in a more privacy-preserving way. An example is providing users more control by allowing one or multiple permission(s) to be modified (granted/revoked) during use. Additionally, *runtime permissions*, introduced in Android 6.0, allow apps to request permissions when needed.

Empowering users to manage privacy permissions creates several challenges, most importantly scalability. The number of apps/services and diverse data sources make it hard for users to stay aware of which data is collected by whom and make permission settings suit their needs and purposes.

Researchers tried to tackle this challenge by a) making privacy information more easily accessible to inform decisions (e.g., [54, 56]) and b) providing users support to take control over privacy choices. For instance, the concept of *privacy assistants* helps users make privacy choices based on their preferences [30, 48]. Another example is the *Privacy Dashboard* introduced in Android 12, which provides users a quick overview of which permissions are granted to which service or application and the auto-revoke feature that removes access to unused permissions. At the same time, there is currently little knowledge of the degree to which people are aware of such privacy permission management mechanisms; if so, how they use them; and how effective these mechanisms are in terms of supporting users in making informed privacy choices, in particular as they change permissions of apps after installation. However, such knowledge is valuable to enhance existing or design novel privacy permission management approaches that better support this post-installation or post-first use update of permissions. We address this through the first in-situ field study, gathering users' privacy permission behavior in an uncontrolled environment over a two-week period.

The following two questions drive our research:

RQ1 – Awareness. Are users aware of a) privacy permissions granted to installed apps and b) current interfaces to manage (and revoke) permissions?

RQ2 – Control. How often, when, and why do users grant, deny, and revoke privacy permissions?

To answer these questions, we conducted a study with Android smartphone users ($N =132$), primarily young Europeans, consisting of two parts: first, our study app acquired current apps and permission settings of participants' phones, allowing us to analyze which privacy permissions they had *initially granted* or *initially denied* for their installed apps; second, our app monitored participants' devices for two weeks for

permission updates to investigate if, for example, participants *revoked* or *later granted* a particular permission. We complemented this data using the Experience Sampling Method [83]: permission updates triggered notifications redirecting users to in-app questionnaires, asking for reasons for their decision.

We found that revocations affect privacy permissions that users consider sensitive (e.g., access to stored files or the camera), but only if this does not affect an app's core functionality or intended use case. Moreover, several updates were often conducted in short time frames, indicating opportune moments exist when users are willing to work on their privacy choices. Our findings provide a better understanding of users' current privacy control and can help to design future mechanisms to support users (proactively) in doing so.

Contribution Statement. Our contribution is twofold. Firstly, we contribute an in-depth investigation of privacy permission awareness and control (i.e., grant/revoke actions) in the real world among 132 Android users. In particular, we collected (1) data on actual privacy permission states at the beginning of the study as well as (2) data on permission changes, along with experience sampling data over the course of two weeks. Secondly, we discuss how our findings can inform future user interfaces supporting privacy permission management.

2 Related Work

We draw from several strands of related work. We illustrate users' privacy awareness and perceptions towards data available on mobile devices and highlight the usefulness of mobile privacy control interfaces. We focus on Android permissions as iOS apps are generally encrypted, and no publicly available analysis tools exist [58]. Hence, an in-situ exploration of users' permission behavior is impossible on iOS.

2.1 Users' Privacy Awareness & Perceptions

Privacy preferences and concerns about sharing data are highly individual [29, 36, 81] and based on contextual factors. For instance, the type and purpose of a specific device as well as the frequency of data being collected [28,29,60,61,89], along with who collects the data [39, 59] and how long it is stored [36], impact users' willingness to share personal data.

Users are particularly concerned about cameras and microphones, as these can capture sensitive data [18, 27, 29, 57, 60, 69]. However, current mobile phones provide an increasing number of sensors that can likewise capture sensitive data. Examples include but are not limited to, GPS sensors allowing users' location to be inferred or gyroscopes allowing users' physical activity to be derived. Other examples of data available on mobile devices include users' personal files, location, and communication data, all of which are considered sensitive data [49]. Users are also specifically concerned about access to their text messages, e-mails, photos, and contacts [39].

At the same time, users are often unaware of which sensors are active on their mobile devices [49] and which data

is collected by apps running on their devices [21]. Moreover, textual descriptions of permissions can be misleading in terms of actual permissions being required [33], and permissions are often requested for third-party libraries rather than apps' core functionality [37]. Specific privacy implications of certain personal data being exposed thus remain unclear to users [23]. Consequently, it is challenging for users to adequately assess which service or functionality currently has access to a specific sensor, let alone the concrete privacy implications of sharing this data. Modern smartphones offer visual cues through hardware and software, such as the microphone and camera indicators, to address this. However, users struggle to understand how much personal information can be gained from smartphone data. In particular, while access to e-mails discloses sensitive information, users underestimate this as a threat [34]. Lastly, users also tend to sacrifice privacy preferences for personal needs [19,44,68] (e.g., if access to a certain sensor would enable a certain feature) or are unaware of the extent to which their personal data is being collected [19].

Increasing privacy awareness, for example, through simple means like microphone indicators, is a prerequisite for users to be able to take control over their personal data and ultimately act according to their privacy needs [29,65,66].

2.2 Mobile Privacy Control Mechanisms

Users mostly wish to stay in control over their data [20, 27, 66, 81]. Current privacy interfaces aim to support this.

2.2.1 Designing for Mobile Privacy Control

The default approach to gathering users' consent before data collection is notice and choice [32, 41, 75, 78]. However, privacy notices are often of poor usability [74], and, thus, insufficient [32]. To address this, researchers proposed privacy notices to be visually appealing [56] and privacy choices to be designed meaningfully and accessible [41].

Current privacy control is oftentimes non-accessible [29, 47], either overly reduced [41] or too complex [20, 43, 47], or overwhelming [79]. Moreover, the number of permission requests is rising: more permissions are requested than necessary [38], and requests are made for third-party libraries rather than core functionality of apps [33]. Tahaei et al. shed light on the developers' perspective: developers are oftentimes unsure about the scope of permissions and, thus, tend to request multiple permissions for smooth functionality of apps [82].

Researchers tried to support users in re-gaining control over their personal data while at the same time reducing the number of decisions to be made [76]. Personalized privacy assistants, for instance, assess users' privacy preferences automatically to make personalized recommendations on privacy settings [30,48]. Considering contextual factors, e.g., the purpose of a specific permission request can improve such recommendations [79]. SmarPer learns from users' decision patterns to automate runtime permissions [71]. Also, repetitive privacy decisions could be automized [80] to reduce users'

decision burden. For mobile applications, the "Privacy Facts" display can help users better understand to-be requested privacy permissions and thus make more informed decisions for apps requiring less privacy intrusive permissions [54].

Prior research also showed that more restrictive privacy policies can increase users' willingness to share data [62]. Possible decision and control support could thus include which data is collected, where and for how long it is stored, and with whom it is shared [62]. Moreover, information on data accessed without actively using the app, data transmission, and app ratings can help users make informed decisions about privacy permissions [77]. Also, as users tend to base their privacy concerns on previous (potentially bad) experiences, privacy choices might be designed to be personal and concrete [55]. Other approaches include the automated analysis of requested permissions [33], respective textual descriptions [37], or users' comments [50] to help assess the actual need for requested permissions and identify undesired app behaviors. Lastly, privacy permission could be requested *proactivly* when access is actually necessary, for example, contextually choosing permissions relevant enough to prompt users directly, similar to Android's runtime permissions. Other permissions could be defined once during setup [64].

Android Privacy Permissions   Android implements privacy control via *permissions* [8]: app developers have to gather users' consent before accessing specific sensors or data (for example, location or stored files). This is typically done by a request prompt: users can choose to *accept* or *deny* access. For Android apps, privacy notices and permission requests typically appeared *upon app installation*. While being recognized by users, these install-time permissions were rarely understood, thus limiting users in making informed privacy decisions regarding whether to install a certain app [40, 53]. With the shift to *runtime permissions* [13] from Android 6.0, permissions are only requested when needed first, providing users with additional contextual information. This allows users to decide whether specific permission is necessary and to revoke decisions later [25]. This contextual approach also benefits developers as grant rates increase [35]. In addition, from Android 11 on, users have more control over the location, microphone, and camera permissions. Moreover, permissions can be granted for *one time* only, and permissions are *auto-revoked* for unused apps [9]. Other permission models have also changed significantly. For instance, access to users' photo library is now limited through the *Photo Picker* [11], meaning apps only have access to specific photos the user selects.

Android Privacy Interfaces   To summarize current permission states, Android's *Permission Manager* lists permission types along with apps that currently do or do not have access to these. With Android 12.0, the *Privacy Dashboard* (see Appendix B) was introduced to provide users with a detailed overview of which applications currently have access to which sensors, along with means to grant or revoke this access [1].

2.2.2   Understanding Users' Mobile Privacy Choices

To design privacy interfaces, understanding users' current use of privacy control is crucial to support them in future choices. In an online survey, Frik et al. found that many users are unaware of privacy permission settings available on their smartphones and have not actively changed them due to a perceived lack of expertise or low self-efficacy [42]. Once granted, users rarely revoke third-party access to personal data (e.g., fitness data) – either because they are unaware of the permission previously granted or they are unaware of the option to revoke access post-hoc [90]. At the same time, strict privacy settings might negatively affect apps' usability [51]. Looking into Google's single sign-on system, Balash et al. showed that users are concerned about giving third-party apps access to personal information but less concerned about access to calendars, emails, or cloud storage [24].

While Android's *runtime permissions* allow users to assess whether or not an application needs specific access by putting them in context, most such permission requests are still accepted, with exceptions mainly for microphone and calendar access. When denying permissions, users mainly believe an app should not need certain permissions or would work without them. In contrast, for granting permissions, access to features and trust are dominant reasons [25]. Bakopoulou et al. found that users oftentimes cannot adequately assess the implications of their private information being exposed to mobile applications [23]. More recently, Cao et al. identified factors impacting privacy decision-making among 1,719 users of Android versions 6.0 to 10. Users were likelier to deny permissions requests they did not expect and less likely to deny permissions that came with explanations [26]. Tahaei et al. found that end-users grant permissions as they desire a certain functionality or trust a certain app [82]. To minimize the number of user decisions, Liu et al. [63] suggest a privacy assistant that automatically configures app permissions based on an initial privacy assessment.

2.3   Summary

The number of apps on users' smartphones makes it challenging for them to be aware of and control their personal data being collected and shared. This challenge is exacerbated as many apps request more permissions than necessary for the core functionality it provides [33, 38, 82]. At the same time, users' awareness and comprehension of, as well as the possibility to revoke a decision previously made, are essential components for the usability of privacy choice mechanisms [46]. Newer Android versions tackle this challenge by providing users with a) *runtime permissions* (since Android 6.0), which gives users more context to form a privacy decision [25]; b) an overview of current permission states per app and control options (*Permission Manager*, followed by the *Privacy Dashboard* on Android 12); and c) privacy indicators visualizing current access to sensors (since Android 12).

Prior work investigated users' general privacy perceptions towards mobile apps [19, 21, 49], privacy permission behavior resulting from the runtime permission dialogs [25], and recently, users' privacy control behavior using surveys [23, 42, 90] or one-time collection of permission states [22]. We add to this knowledge by contributing an in-situ investigation of users' a) *awareness* of built-in privacy control interfaces and permission states and b) *permission control* (e.g., revoking permission that was initially granted or later granting permission that was initially denied) on current Android versions by collecting in-the-wild data over a period of *two weeks*. We gather those *in-situ* insights by implementing an Android app that collected information on installed apps and permission states, as well as on updates to these. We complement our data using Experience Sampling (ESM) [83].

Our approach is in line with prior research on privacy permissions. Field studies have generally been used to understand the contextual nature of permission granting decisions [85, 88], and for automating permission management [86, 87]. ESM as data collection method was effectively applied in prior privacy studies among Android users [22, 25] to capture their privacy behaviors [26], yet did not focus on post-hoc privacy management, including revoking permissions.

3 Research Approach

Using the Experience Sampling Method (ESM) [83] and automated data logging using an Android application, we collected data on users' *awareness* of current privacy permissions states (RQ1) and updates of privacy permissions (*control*, RQ2) among 132 participants. Following van Berkel's suggestion for ESM-based studies using smartphones [83], we decided on a two-week period. This also provided enough time to observe a substantial number of permission updates. Note that with this approach, we aimed to identify general permission management behavior rather than generalizing our findings to the broader population.

3.1 Apparatus

We built an Android app for version 8.0 to 12.0 (the latest version at the time of the study) in Kotlin 1.6.20 [15], thus covering 86.7% of Android users. The app comprises two major components: the *Permission Scanner* and the *In-App Experience Sampling (ESM) Questionnaire Interface* (see Figure 1, right). The Permission Scanner regularly monitored participants' devices for permission states of all installed apps (every two hours, excluding system services and apps with zero usage time). For this, our application requested access to Android's Package Manager [16] and Usage Stats Manager [17]. In case at least one permission *update* (i.e., change in permission compared to the last scan) was detected, an ESM questionnaire was triggered, asking for reasons for up to five permissions updates, depending on the number of updates. The In-App Experience Sampling Questionnaires were implemented using *SurveyKit* [14].
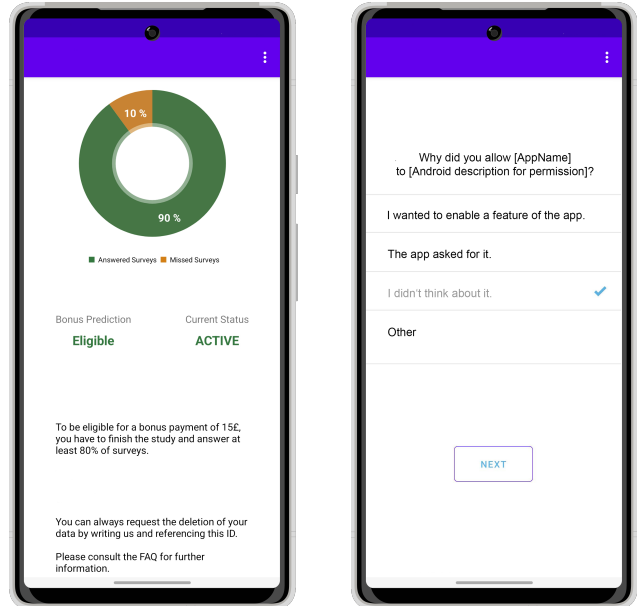
Figure 1: Study App Screenshots. Left: The home screen provides participants with an overview of answered/missed experience sampling questionnaires, eligibility for the bonus payment, and access to contact information. Right: A sample screen with an experience sampling questionnaire.

The app's home screen provided participants with an overview of answer statistics using MPAndroidChart [7] and access to contact information and frequently asked questions (see Figure 1, left). Data was stored in a Firebase Realtime Database [5]. We also used Firebase Crashlytics [4] to analyze and account for any errors during the study. The app was made available to participants using Firebase App Distribution [3].

3.2 Collected Data

Our application collected data through automated logging and questionnaires. Participants were asked to answer a questionnaire at the beginning (*initial questionnaire*), after one week (*mid-term questionnaire*), and at the end (*final questionnaire*) of the study. In addition, participants were asked to answer two types of experience sampling questionnaires: a questionnaire on control (*ESM control questionnare*) and one on awareness (*ESM awareness questionnaire*).

3.2.1 Automated Data Logging

Our application automatically collected the following data: information on the device (device name, brand, and Android version); an initial list of all installed applications along with usage duration; state of privacy permissions upon installation; and privacy permission updates during the study.

Permission States & Updates For privacy permissions of apps, we logged their state at the beginning of the study (i.e., *initially granted* or *initially denied*), and every two hours over two weeks. If a permission state changed during the study (i.e., a different state than the previous scan), we recognized

this as a *permission update*. We consider updates from previously granted permissions to denied access (i.e., *revoked*) and updates from initially denied permissions to granted permissions (i.e., *granted later*). Update data includes app names, requested permissions with the current state, and app usage time. Our data might include permission changes resulting from a) newly installed apps or b) Android's auto-revoke or one-time permission features (from Android 11 on [9]). Note that for a), users' (active) privacy decisions, as made when first using a new app, are included in our data. For b), we acknowledge that some updates might have been initiated by Android rather than consciously by users (see Section 4.4.4).

3.2.2 Experience Sampling (ESM)

We utilized ESM, prompting participants with in-situ questionnaires via notifications [83]. Our app administered two types: (1) upon detected permission *updates* asking for reasons (ESM control questionnaire) and (2) asking about permission states of certain apps *daily* (ESM awareness questionnaire). We covered all permissions updated within the respective time frame for the ESM control questionnaires. Answer options included sample reasons (see Appendix C.3.1) and an option for free text. These options resulted from discussions among the authors to reflect the research questions. We always presented them in the same order to ensure consistency.

For the ESM awareness questionnaire (see Appendix C.3.2), we randomly chose up to five installed apps that operated in the foreground at least once since installation and required access to at least one permission. We did not give participants the correct answers (i.e., permission states). We included attention checks such as "If you read this, please select 'No'". To increase motivation, participants received clear information on the study goal and additional compensation for active engagement with the ESM questions [84]. Moreover, participants were asked to use their personal devices and could set a custom time span per day in which ESM questionnaires were sent [83]. All ESM questionnaires were withdrawn after a certain timespan (control: after 2 hours, awareness: after 12 hours) to ensure in-situ answers [83].

3.2.3 Questionnaires

We complemented our data collection with an initial and final questionnaire on users' perception of privacy permissions and a midterm questionnaire on using Android's privacy management tools (see Appendix C). Participants were to choose permissions for which they wanted to be particularly alert (*awareness*). The midterm questionnaire covered prior usage of Android's Privacy Dashboard and Permission Manager, depending on participants' Android version (*control*). This questionnaire was designed to hint users to these interfaces and see if their behavior would change in the second week of the study. We validated the clarity of all questionnaires in a pilot run, where all co-authors and research group members tested the app for two weeks, giving continuous feedback.

3.3 Procedure

Participants used our Android application over two weeks. The detailed procedure was as follows (see Figure 2):

1) **Installation & Setup.** Participants who agreed to participate first downloaded our application. Participants were prompted to consent to the study's procedure and privacy policy upon installation. After consent, the app collected information on the device, installed apps, and current permissions of apps along with usage duration.
2) **Initial Questionnaire.** Participants then answered an initial questionnaire covering their privacy preferences before the study (see Appendix C.1 for a full list of questions). After this questionnaire, our app started the automated data logging (permission updates) and experience sampling.
3) **Experience Sampling Phase.** For two weeks, the app scanned participants' devices for permission updates. Upon change, the app would trigger a questionnaire (via a notification), asking for the reasons for later granting or revoking that specific permission (ESM control questionnaire, see Appendix C.3.1). In addition, the app asked daily about permission states of a random selection of apps (ESM awareness questionnaire, see Appendix C.3.2).
4) **Mid-Term Questionnaire.** After a week, participants filled in a mid-term questionnaire on using Android's current privacy interfaces, asking them to visit the *Permission Manager* and/or *Dashboard* afterwards (Appendix C.2).
5) **Final Questionnaire.** The final questionnaire repeated the initial questions on privacy perceptions (Appendix C.1).

3.4 Recruitment & Requirements

We recruited our sample via Prolific, an online subject pool [12, 72]. We enforced several requirements through pre-screening: (1) Participants must be fluent in English. (2) The sample should be equally balanced in terms of gender and only include users aged 18 or above based on their demographic characteristics (see [6] for details on balanced samples). (3) We sampled participants residing in Europe, Canada, the USA, and Australia. We did so to reduce effects from, e.g., smartphones being shared among family members, people tending to use multi-purpose apps (WeChat in China), or cases in which vendors pre-install apps (many countries in Africa.).

Participants were required to use the app on their personal smartphones with Android versions 8 to 12.0. Through Prolific, participants installed and set up the app. Upon setup completion ($N = 300$, 14 minutes on average, according to Prolific), participants were reimbursed with 1.9 GBP on average[1]. For participants following the study over two weeks and answering at least 80% of the ESM questionnaires, we paid a bonus of 15 GBP (average time commitment 56 minutes, based on the total usage time of the study app). The study was conducted between April and May 2022.

---

[1]The average hourly wage was 7.62 GBP as suggested by Prolific.
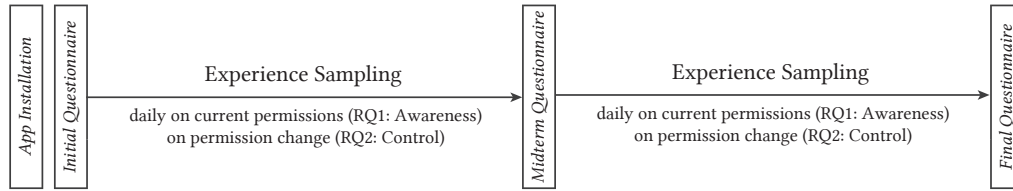
Figure 2: Study Procedure: Participants first installed the application and filled out an initial questionnaire. In the following experience sampling phase, participants were asked about active permission revocations (control) and awareness of current permissions. They filled out a midterm questionnaire after one week and a final questionnaire after two weeks.

3.5 Ethical Considerations

In the country where this research was conducted, formal IRB approval is not required for this type of human subject research [70]. However, we comply with all university ethics regulations and national data protection regulations. Consent was gathered as follows. First, participants read the study description and then accessed the study through Prolific [12]. Second, they were directed to Firebase App Distribution [3], where they consented to downloading and installing the app[2]. Third, we gathered participants' informed consent through our app before collecting data. We stopped data collection automatically after two weeks and suggested uninstalling our app. Collected data comprises an app list, permission settings changes, and questionnaire answers. All data was collected anonymously using randomly generated identifiers. As such, we are unable to identify individual participants or devices. Through Prolific, we only recruited participants with a minimum age of 18. We followed Prolific's suggestion for reimbursing the *study's initial setup procedure*, which took 14 minutes on average. For participating over 14 days with a daily effort of around 4 minutes, we paid a bonus of 15 GBP.

3.6 Limitations

Android Versions Our study is limited to participants running Android version 8 and above. This excludes older versions but ensures compatibility and access to the *Permission Manager*. In a few cases, the app showed unforeseen behavior, leading to the exclusion of some participants (see Section 3.7).

Sample Our participant sample is biased towards young users (mean age 26.45) from European countries with Android versions below 12.0. Thus, our results might not apply to the general population or future Android versions.

Selection Bias The initial and midterm questionnaires and participation in our study, in general, might have influenced permission control behavior. Still, we a) wanted to be transparent about the study goal, not using any deception, and b) see if knowledge about Android's privacy tools (midterm questionnaire) influences users' behavior. The study advertisement and task did not explicitly require participants to engage with permission management actively but only to answer ESM questionnaires. The initial questionnaire deliberately did not

hint at privacy management but focused on permissions' general importance. We did not find significant differences in the number of permission updates in the study's first vs. second week (before/after the midterm questionnaire).

We acknowledge that, due to self-selection, participants may have had fewer privacy concerns than the average population. Generally, self-stated privacy preferences (as in our questionnaires) tend to differ from actual behavior (cf. the "privacy paradox" [44]). Our results include logging data on actual privacy permission states to account for this.

User vs. System-initiated Updates Sixty-six participants (on Android 11 or 12) could grant permissions for camera, microphone, and location for *one time* [10] only, and permissions might have been revoked automatically for unused apps (cf. auto-revoke [9]). We could not actively capture these cases (see Section 3.2.1), but found the number of such possible cases through post-hoc analysis (see Section 4.4.4).

App (Un)Installs Our analysis considers permissions granted to newly installed apps during the study as these result from conscious user decisions. We did not consider uninstalls as permission changes because we do not know the reasons. We acknowledge privacy concerns, similar to those leading to permission revocation, might have been the reason.

3.7 Data Cleaning

The setup and app installation were completed by 300 participants. Of these, 179 completed the full study, with 158 participants answering at least 80% of the ESM questionnaires and, thus, receiving the bonus. Of these, we excluded 13 participants based on corrupt or missing data, and 13 participants based on app crashes, failed attention checks, or unknown Android versions. Ultimately 132 samples were analyted.

During the study, we collected answers for a total of 366 ESM control questionnaires (2.77 on average per participant), 885 ESM awareness questionnaires (6.7 on average per participant)[3], and initial, midterm, and final questionnaires. Note that from a few participants, we received more than one answer set for the same questionnaire. In these cases, we considered the first complete set of answers for analysis.

---

[2]Note that participants opted out during the first or second step.

[3]Notifications for all ESM questionnaires were withdrawn after a certain time. Hence, questionnaires may have remained unanswered. We did not enforce receiving one ESM awareness questionnaire per day from every participant. This practice follows Berkel et al. to ensure in-situ answers [83].

3.8 Participants

Participants were 18 to 54 years old ($Mean = 26.45$, $SD = 6.95$). 65 participants identified as women, 63 as men, and four as non-binary. Participants' nationality was mostly Polish ($N = 40$), Portuguese ($N = 26$), Italian ($N = 22$), or Greek ($N = 14$). Others were Spanish ($N = 6$), Czech ($N = 4$), British ($N = 3$), and of other mostly European nationalities (see Appendix D.1). All participants were fluent in English.

Most participants were employed full-time ($N = 38$), unemployed (and job seeking, $N = 32$), employed part-time ($N = 26$), not in paid work ($N = 5$), starting a new job within the next month ($N = 3$), or other ($N = 27$). One participant's employment data expired. Most participants completed a high school diploma ($N = 52$) or undergraduate degree ($N = 43$). 23 received a graduate degree, and few other educational levels were mentioned. Regarding their technical background, the fact that they were active on prolific and 126 participants (70.4%) were aware of the possibility of revoking permissions hints at solid technical knowledge.

4 Results

Overall, participants had 15 to 202 installed applications ($Mean = 99.42$, $SD = 34.43$) with 36,904 granted permissions and 40,175 denied permissions in total (see Table 1). Throughout our study, we acquired *permission updates* among 128 participants (2,866 updates in total, thereof grants: 1,064, revokes: 1,802, see Tables 5 and 4 for reasons). In addition, participants answered a total of 885 ESM awareness questionnaires (RQ1, 6.70 on average per participant) and 366 ESM control questionnaires (RQ2, 2.77 on average per participant).[4] Participants were somewhat aware of current permission states with 49% correct answers for granted permissions, and 34% correct answers for denied permissions (see Table 3). In the following, we present detailed results of our automated data logging and experience sampling.

4.1 App Usage

Upon installation, our study application acquired initial information on participants' Android devices and installed applications, along with initial permission states.

Android Devices & Versions   Most participants used Android 11 ($N = 46$) or 10 ($N = 43$), some used Android 12.0 ($N = 20$) or 9 ($N = 18$), and a few participants used Android 8.0.0 or 8.1.0 ($N = 5$). Hence, all participants had access to the *Permission Manager* and 20 to *Privacy Dashboard*. Device brands mainly included Xiaomi/Redmi ($N = 53$), Huawei ($N = 25$), and Samsung ($N = 20$).

Installed Apps & Permissions   Participants initially had 15 to 202 apps installed ($Mean = 99.42$, $SD = 34.43$, see Table 6 for most used apps). One app requested 0 to 22 permissions ($Mean = 5.87$, $SD = 4.41$, total number of all

---

[4]Note that questionnaires may have remained unanswered (Section 3.7).

Table 1: Overview of Initial Permission States: List of all permissions available for users to choose on Android, along with their state (i.e., denied vs granted) at the beginning of our study. Values shown represent the ratio of the permission being denied/granted in relation to the total number this specific permission was requested among all applications all participants had initially installed (total number of permission requests: 77,079, granted: 36,904, denied: 40,175).

Permission Name	#req.	Denied (%)		Granted (%)
read phone numbers	731	83.99		16.01
get accounts	4139	64.89		35.11
access background location	1771	63.13		36.87
Bluetooth scan	1490	62.55		37.45
camera	6342	58.33		41.67
read calendar	1534	57.24		42.76
record audio	4557	55.63		44.37
read phone state	4909	54.94		45.06
access fine location	5905	51.96		48.04
write calendar	1228	51.95		48.05
access coarse location	6445	51.34		48.66
read contacts	5120	51.07		48.93
write external storage	8575	50.24		49.76
read external storage	9792	48.72		51.28
access media location	1384	47.47		52.53
write contacts	2077	33.37		66.63
activity recognition	657	32.27		67.73
query all packages	2891	31.75		68.25
read SMS	1237	21.18		78.82
read call log	1327	19.67		80.33
body sensors	176	18.75		81.25

permissions: 77,079, thereof initially granted: 36,904, initially denied: 40,175). Of these, *read phone numbers* was mostly denied (83.99%), followed by access to *accounts* (64.89%), *background location* (63.12%), and Bluetooth scan (62.55%). Participants were also somewhat strict about *camera* (58.36% denied), *calendar* (57.24% denied), and *audio* access (55.63% denied). In contrast, access to *body sensors* (81.25%) was granted most, followed by reading the *call log* (80.33%), and *SMS* (78.82%). A reason for access to body sensors being often granted is that apps likely required those permissions to enable their main functionality; for example, smartwatches running WearOS require access to body sensors. Overall, participants had 47 to 540 *initially granted* permissions ($Mean = 304.37$, $SD = 91.71$) and 37 to 543 *initially denied* permissions ($Mean = 279.58$, $SD = 95.78$). Table 1 summarizes permission states when the study started.

4.2 Android Usage

The following results describe users' awareness of Android privacy permissions and their knowledge and use of Android's privacy interfaces (control).

4.2.1 Awareness of Privacy Permissions

We captured users' wishes for awareness of specific permission types at the beginning and end of our study. Looking at the data collected at the beginning, participants wished to be particularly informed about the following permissions: camera ($N = 121$), location ($N = 118$), and microphone ($N = 116$,

Table 2: Awareness of Privacy Permissions: Number of participants who particularly wished to be informed of the following privacy permissions (assessment in initial vs final questionnaire, respectively). Change is normalized by participants ($N = 132$). Participants could choose multiple permissions.

Permission Name	Initial	Final	Change
camera	121	124	+2.3%
location	118	125	+5.3%
microphone	116	120	+3.0%
phone numbers	114	114	0.0%
contacts	111	117	+4.5%
SMS	104	107	+2.7%
external file storage	100	100	0.0%
call history	99	112	+9.8%
installed apps	88	86	-1.5%
other users on the smartphone	77	75	-1.5%
Bluetooth	74	71	-2.3%
physical activity	71	69	-1.5%
body sensors	69	72	+2.3%
calendar	56	54	-1.5%
none of these	21	5	-12.1%

see Table 2 for details)[5]. After the study, the picture is similar, with a slight increase in numbers, which can probably be attributed to raised awareness due to the increased exposure to permissions during the study: location ($N = 125$), camera ($N = 124$), and microphone ($N = 120$, see Table 2 for details).

4.2.2 Knowledge of Android Privacy Interfaces

The *midterm questionnaire* revealed that the majority of participants ($N = 125$) were aware of the fact that they can post-hoc revoke permissions ($N = 7$ stated "No"). Many participants stated to have revoked a permission before ("Yes": 92, "No": 33), mainly due to privacy concerns ($N = 59$), a feature not being used anymore ($N = 51$), or security concerns ($N = 32$). Only one participant did not think about it, and one stated "other". Most participants ($N = 108$) mentioned to have engaged with the *Permission Manager* before. However, they typically used it less than once a month ($N = 84$, "At least once a month": 21, "At least once a week": 3). 15 participants had not used the *Permission Manager* before, and 9 did not know about it. Of Android 12 users ($N = 20$), only a few ($N = 7$) had used the *Privacy Dashboard* before. Most of them stated they used it less than once a month ($N = 5$), and a few used it at least once a month ($N = 2$). Two participants stated that they had not used the Dashboard before, while 11 were unaware of the Dashboard at all. Note that these low numbers need to be treated with care and are expected, as the goal of the Dashboard is to provide an overview when the need arises. Thus, low usage counts are expected.

4.3 RQ1: Awareness of Permission States

In daily ESM awareness questionnaires, we asked participants if they were aware of the current privacy permissions of certain apps (up to five apps per questionnaire, randomly chosen). Questions were in the form of "Does app x cur-

---

[5]Note that this is in line with the importance of how Android 11+ treats these permissions, e.g. by allowing one-time permissions [10].

rently have access to permission y?". Overall, 885 daily ESM awareness questionnaires were answered by participants (6.70 on average per participant), covering 4,395 questions (i.e., permission-app tuples): 2,153 (49%) questions targeted permissions currently granted and 2,242 (51%) currently denied.

For permissions that were currently granted, this was assessed correctly almost half of the time ($N = 1,052$, 49%), 455 times (21%) it was falsely believed the permission was currently not granted, and 646 times (30%) participants indicated they do not know. For permissions that were currently not granted, 760 questions were correctly answered with "No" (34%). In contrast, 685 were falsely answered with "Yes" (i.e., granted, 31%) and 797 times participants indicated they do not know (36%)[6]. Table 3 provides an overview. Cases where specific permissions were granted, but participants believed they were denied (i.e., they answered with "No"), are particularly privacy-critical. Looking at the specific permissions that we (randomly) asked for in the ESM awareness questionnaires, the following permissions were often falsely assessed: read (70 of 325) and write (51 of 223) access to the external storage; read phone state (33 of 167); and camera access (31 of 129). Table 8 in Appendix D.2 provides details on correct and false answers per permission.

4.4 RQ2: Controlling Permissions

We collected data of 2,866 updates on privacy permissions, including revoking permissions previously granted and vice versa. Data was collected automatically through scans of our study app and manually using experience sampling (ESM control questionnaire), asking participants for reasons for their permission updates (see Tables 5 and 4 for an overview). Participants mainly chose among the given answer options, while "Other" was chosen only 40 times (1122 ESM questions in total, with 1289 reasons given). Given the low number, we report these examples directly where appropriate.

4.4.1 Revoked Permissions

Of 2,866 permission updates, 1,802 were revocations (62.88%). Participants mostly revoked read ($N = 276$) and write ($N = 242$) access to their external storage, camera access ($N = 192$), location access (coarse $N = 155$, fine $N = 142$, and background $N = 56$), and permissions to record audio ($N = 136$), read phone state ($N = 125$) or contacts ($N = 90$), get accounts ($N = 83$), Bluetooth scans ($N = 74$), and query all packages ($N = 71$). Table 9 in Appendix D.3 provides an overview of the apps most affected by revokes. Interestingly, revokes also affected apps heavily used, including Instagram ($N = 11$), TikTok ($N = 27$), YouTube ($N = 18$), or Messenger ($N = 13$, Table 6). Revoked permissions (e.g., location for Instagram or TikTok) are not essential for *consuming* content.

---

[6]Note that some of these "Yes" answers may stem from the auto-reset feature of Android 11/12 having revoked permissions automatically. Hence, some "Yes" answers might have been correct from the participants' point-of-view. Nonetheless, we did not observe differences between users with Android 11/12 and those with older versions (see Table 3).

Table 3: Awareness of Current Privacy Permissions: Participants' answers to daily ESM awareness questionnaires. For "granted" permissions, the correct answer is "yes", while for "denied" permissions, the correct answer is "no" (marked in bold/green). The table shows the total distribution of answers and for older (8-10) vs newer (11-12) Android versions.

Permission State	Yes		No		I don't know
Granted	**1052 (49%)** old: 54%, new: 44%		455 (21%) old: 22%, new: 21%		646 (30%) old: 24%, new: 35%
Denied	685 (31%) old: 31%, new: 30%		**760 (34%)** old: 22%, new: 32%		797 (36%) old: 24%, new: 38%

Table 4: Reasons for *Revoking* Permissions: Using Experience Sampling, we gathered the reasons for a total of 682 revokes that were conducted during the study (multiple select).

Reason for *Granting* Permissions	
I didn't need the feature.	357
I was concerned about my privacy.	212
I didn't think about it.	135
I was concerned about the security of my device.	88
Other	22

Table 5: Reasons for *Granting* Permissions: Using Experience Sampling, we gathered the reasons for a total of 440 grants that were conducted during the study (multiple select).

Reason for *Granting* Permissions	
I wanted to enable a feature of the app.	227
The app asked for it.	117
I didn't think about it.	106
Other	18

Using the ESM control questionnaires, we acquired additional data on 682 revocation events. The ESM mainly covered events related to revoking read ($N = 120$) and write ($N = 103$) access to external storage, access to the camera ($N = 98$) and location (coarse $N = 62$ and fine $N = 47$), reading phone states ($N = 44$), recording audio ($N = 42$), or reading contacts ($N = 31$). Apps that were covered mostly include TikTok ($N = 17$), ZAFUL ($N = 12$), Twitter ($N = 12$), PayPal ($N = 12$), Pikmin Bloom ($N = 9$), and others. As reasons for their decision, participants mostly mentioned not needing the respective feature (mentioned for 352 revokes by 75 participants), privacy (212 revokes, 58 participants), and security (88 revokes, 36 participants) concerns, not having thought about it (133 revokes, 43 participants), and other (22 revokes, 11 participants) such as they did not actively choose or the app did not ask for it, or "it must have happened automatically" (one participant each, see Table 4). Participants could choose several reasons when asked for a specific app and permission.

4.4.2 Permissions Granted Later

Updates during the study included 1,064 'granted later' permissions (37.12%). Participants mostly granted permission to read ($N = 121$) or write ($N = 101$) external storage, access location (coarse $N = 101$; fine $N = 91$), record audio ($N = 136$), query all packages ($N = 74$), read phone state ($N = 59$), and camera ($N = 54$). Regarding highly used apps, grants affected,

e.g., Instagram ($N = 3$) or TikTok ($N = 21$), but also apps of the category *Tools* such as Google ($N = 25$) or the Phone ($N = 31$, see Table 6). Table 10 in Appendix D.3 provides an overview of apps with most grants.

From the ESM control questionnaires, we acquired data on 440 permission grants, mainly affecting permission to read ($N = 81$) and write ($N = 63$) external storage, access to Bluetooth ($N = 54$), camera ($N = 42$), or location (coarse $N = 38$ and fine $N = 29$), or to query all packages ($N = 30$). Apps affected included Instagram ($N = 9$), Ferrarm SIM ($N = 9$), and others. Participants mostly wanted to enable a feature of an app (mentioned for 223 grants by 70 participants), and the affected app asked for certain permission (117 grants, 50 participants), or they did not think about it (105 grants, 38 participants). For 18 grants, other reasons were mentioned (11 participants), including they did not remember giving permission, were unsure about consequences, or the app was pre-installed (one participant each, see Table 5). Note that participants could choose several reasons again.

4.4.3 Bulk Permission Updates

A total of 702 apps were affected by permission updates throughout the study (692 unique on a per-user basis, 493 unique apps overall), with updates of 2,866 permissions in total (22.39 on average across 128 participants who conducted such updates). Many scans by our study app (every two hours) comprised updates of more than one app and/or more than one permission, indicating that participants ($N = 128$) conducted updates in "bulks", that is, in short time frames. Such scans included one to 27 apps ($Mean = 1.43$, $SD = 1.57$), with 106 updates including more than one app (384 updates included only one). Per app, more than one permission was updated in most cases ($N = 487$ vs. 215 cases with single permissions updated for an app), with 1 to 19 permissions updated at once ($Mean = 4.08$, $SD = 3.44$). In total, 383 scans included updates of multiple permissions (107 scans only one).

4.4.4 User vs. System-initiated Permission Updates

A total of 66 participants (50%) were using Android 11 or above. For these, Android might have initiated some permission updates. In particular, the *auto revoke* [9] feature automatically withdraws permissions for apps that have not been used for several months. However, among the 1392 permission updates (808 revokes) we collected from participants with newer Android versions, only 32 revokes (4%) affected apps not used at all during the two weeks of study. More-

Table 6: Most Used Apps and Permission Updates: This table presents the most used apps in our dataset (left) along with corresponding permission updates (right). We sorted all *apps* based on the total overall *usage time* (sum in hours) as acquired from the initial scan. We list the first 25 apps below (*N*: number of installations). The *Category* is based on the Google Playstore [2], except for two side-loaded apps that we categorized accordingly. Permission updates include *revokes* and *grants*.

App	N	Category	Total Usage Time (hours)	Permission Updates: **Revokes**		Permission Updates: **Grants**	
Instagram	94	Social	1980.9	11	coarse loc (1), fine loc (1), access media location (1), camera (1), get accounts (1), read contacts (1), read external storage (1), read phone numbers (1), read phone state (1), record audio (1), write external storage (1)	3	coarse loc (1), Bluetooth (1), Bluetooth scan (1)
Chrome	131	Communications	1581.1	1	Bluetooth scan (1)	0	
TikTok	62	Social	1494.1	27	query all packages (11), coarse loc (2), camera (2), read calendar (2), read contacts (2), read external storage (2), record audio (2), write calendar (2), write external storage (2)	21	query all packages (18), Bluetooth (2), Bluetooth scan (1)
Facebook	93	Social	1345.1	1	read phone numbers (1)	1	Bluetooth scan (1)
Messenger	100	Communications	1003.6	13	coarse loc (1), fine loc (1), camera (1), get accounts (1), read calendar (1), read contacts (1), read external storage (1), read phone numbers (1), read phone state (1), read SMS (1), record audio (1), write contacts (1), write external storage (1)	2	Bluetooth (1), Bluetooth scan (1)
YouTube	121	Video Players & Editors	888.2	18	coarse loc (2), fine loc (2), camera (2), get accounts (2), read contacts (2), read external storage (2), read phone state (2), record audio (2), write external storage (2)	0	
WhatsApp	87	Communications	684.1	0		1	Bluetooth scan (1)
Reddit	51	Social	467.0	17	coarse loc (4), camera (4), read external storage (4), record audio (4), write external storage (1)	5	Bluetooth (4), Bluetooth scan (1)
YouTube Vanced	20	Video Players & Editors	427.2	11	background loc (1), coarse loc (1), fine loc (1), access media location (1), camera (1), get accounts (1), read contacts (1), read external storage (1), read phone state (1), record audio (1), write external storage (1)	0	
Huawei Home	14	Tools	411.5	2	read calendar (2)	2	Bluetooth (2)
Telegram	50	Communications	304.0	21	background loc (2), coarse loc (2), fine loc (2), camera (2), get accounts (2), read contacts (2), read external storage (2), record audio (2), write contacts (2), write external storage (2), read call log (1)	8	Bluetooth scan (1), Bluetooth (2), read call log (1), read phone numbers (2), read phone state (2)
Twitter	48	Social	280.8	18	coarse loc (2), fine loc (2), camera (2), get accounts (2), read contacts (2), read external storage (2), read phone state (2), record audio (2), write external storage (2)	3	Bluetooth (3)
Netflix	68	Entertainment	273.2	0		0	
Discord	63	Communications	262.3	1	read contacts (1)	5	Bluetooth (1), camera (1), read external storage (1), record audio (1), Bluetooth scan (1)
Google	123	Tools	208.0	13	background loc (2), activity recognition (2), Bluetooth scan (2), query all packages (2), read external storage (2), write external storage (2), camera (1)	25	coarse loc (2), fine loc (2), Bluetooth (2), camera (1), get accounts (2), read calendar (2), read call log (2), read contacts (2), read phone state (2), read SMS (2), record audio (2), write calendar (2), write contacts (2)
Phone	105	Tools	150.5	0		31	coarse loc (3), Bluetooth (3), get accounts (3), read call log (3), read contacts (3), read external storage (2), read phone state (2), read SMS (3), record audio (3), write contacts (3), write external storage (2), fine loc (1)
Snapchat	35	Communications	116.4	28	read phone numbers (4), background loc (3), coarse loc (2), fine loc (2), camera (1), get accounts (3), read call log (3), read contacts (2), read external storage (1), read phone state (2), record audio (1), write contacts (3), write external storage (1)	17	Bluetooth (3), Bluetooth scan (1), coarse loc (1), fine loc (1), camera (2), read contacts (1), read external storage (2), read phone numbers (1), read phone state (1), record audio (2), write external storage (2)
Spotify	89	Music & Audio	112.0	3	Bluetooth scan (3)	1	Bluetooth (1)
Clock	87	Tools	102.1	1	read phone state (1)	0	
Maps	78	Travel & Local	96.7	9	background loc (1), access media location (1), activity recognition (1), Bluetooth scan (1), camera (1), read contacts (1), read external storage (1), record audio (1), write external storage (1)	3	coarse loc (1), fine loc (1), Bluetooth (1)
Gallery	82	Photography	96.0	11	coarse loc (3), fine loc (3), query all packages (2), get accounts (1), read contacts (1), read phone state (1)	5	access media location (2), query all packages (1), read external storage (1), write external storage (1)
Zoom	18	Business	73.7	0		0	
Gmail	127	Communications	73.6	1	read phone state (1)	0	

access fine location; access coarse location; access background location; read calendar; write calendar; access media location; camera; Bluetooth; Bluetooth scan; read external storage; write external storage; query all packages; record audio; read contacts; write contacts; read phone numbers; get accounts; read phone state; activity recognition; read SMS; read call log;

over, we collected permission revocations among users in both groups ($N = 61$ users with permission revokes on new Android, $N = 64$ users with revokes on old Android). The total number of permissions updated is very similar: $N = 1,474$ for older Android versions and $N = 1,392$ for newer Android versions[7]. In addition, many permission updates (including revokes) were conducted for heavily used apps (see Table 6). Thus, the majority of revoked permissions do not fall under the auto-revoke feature. Still, there might be cases in which users chose to grant camera, location, or microphone permissions for *one time* [10] only. These permissions are revoked automatically as soon as the requesting app moves into the background. Hence, such one-time permissions would only

---

[7]Note that we did not find any statistically significant differences in the number of updates (neither for total number nor number of grants or revokes) for users with older vs newer Android versions.

occur in our dataset if users used an app during the end of/the beginning of a new two-hour timeslot. To identify such cases, we looked at permissions per user and app that were granted and revoked multiple times but found no such cases.

5 Discussion

5.1 Awareness of Privacy Permission States

Our study results indicate that people have an alarmingly low level of awareness regarding what permissions specific apps have. In particular, only 49% of granted permissions and 34% of denied permissions were assessed correctly. Past studies have shown that privacy awareness is a prerequisite for users to make meaningful decisions [29, 65, 66], for example, about whether or not an app should retain certain permission at a given point in time. Moreover, Frik et al. identified a lack of awareness regarding the availability of privacy settings, leading users to not take action according to their privacy needs [42]. The permission model of modern smartphone operating systems seems to address this already: asking for permissions in context, that is, right at the time when they are needed (cf. *runtime permissions* on newer Android versions). This helps users build better mental models of the permission space and also enables them to select only permissions that make sense to them for a particular application or feature.

We found that in many cases users think that permissions they gave are not actually given and vice versa. In 455 cases, granted permissions were falsely assessed as denied (21%), which is critical from a privacy point-of-view as apps might access personal data without users being aware of it. Moreover, there were many cases where users indicated they did not know (granted: 30%, denied: 36%). This is likely related to the sheer number of (partially unused or rarely used) installed applications on users' phones (99.42 on average for this study). Also, prior work found that it is oftentimes not clear to users which permissions are requested for the actual application vs. third-party services [33], and textual descriptions of applications oftentimes lack detailed information on permission requests [37]. Permission reminders, as standard in current OS versions and other proactive features, can mitigate this to some extent but come with the risk of overburdening users with recurring warnings. However, as shown in previous work, increasing awareness can help to motivate them and take action about their privacy [34, 45, 73], and information prompts might thus be acceptable. Information that could be relevant in such interfaces includes, but is not limited to, the type of data that is collected and stored, for how long, and with whom it is shared [62]. Other relevant information includes whether an app can access private data in the background; or how an app is rated by others [77]. Another opportunity could be to convey information on the risks rather than the resources or sensors being assessed [40].

5.2 Types of Permission Revocations

Participants changed permission states for installed apps in 2,866 cases, including 1,802 *revocations*. Reasons include a lack of need for (or lost benefit of) the respective feature, privacy, and security, in that order (see Table 4). This indicates that, while privacy and security play a major role in the process (mentioned by 94 participants, 71%), other factors do as well in a significant way. This indicates that messaging around revocation support should cater to these needs to help users make informed decisions. Looking at the details of permission revocations, three trends become apparent:

1) **Privacy-Relevance of Revoked Permissions.** Most revocations recorded in the study fall into the bucket of the top three permissions that participants want to have an eye on: location, camera, and microphone access. The sensitivity of this data was shown in previous work [18, 22, 27, 29, 57, 60, 69].
2) **Affected Apps.** Participants rarely revoked permissions for frequently used apps. This indicates that the benefit of allowing an app access to a certain permission increases through usage frequency. While YouTube and TikTok are among the most installed apps with high usage time showing relevant revocation activity, their revocations fall into what will be listed in point 3 below.
3) **Functionality-Relevance of Revoked Permissions.** Revocations are mostly related to permissions not essential for the app's core functionality. In particular, looking at the apps with the highest usage times (see Table 6), permissions might be necessary for *producing* content but not for *consumption*. For instance, access to the camera, external storage, media, or location was revoked for apps such as Instagram, TikTok, and Youtube, which still allows using these apps to *consume* content. This indicates that users consider the use case and functionality they intend to use an app for when deciding on permissions and use the opportunity to restrict permissions necessary for *producing* content if they do not intend to do so. Thus, future approaches could consider effects on core functionality [51]. This is in line with prior work indicating that end-users and developers alike consider app functionality and features when it comes to permission management [82].

Researchers have suggested a number of innovative privacy designs. The above-mentioned trends and the insights from our real-world study build a solid foundation to review existing privacy designs and assess their ability to address important aspects we identified (see below). Furthermore, they can inform future designs of mobile privacy control.

5.3 (Proactive) Mobile Privacy Control

Prior work showed users want to protect personally identifiable information on their smartphones and, thus, are open to supportive tools [23]. Privacy protection mechanisms follow different approaches in terms of proactivity, from low to

high [52] or from simple notifications (or recommendations) to full automation, where systems act on users' behalf [30]. Users prefer simple and proactive mechanisms while still staying in control as opposed to full automation [30, 52]. Moreover, permission prompts should provide explanations to increase users' confidence in their decisions [35].

Finding the right balance for proactive privacy support features on mobile devices seems, thus, essential. For instance, proactive privacy permissions (as an extension to the current runtime permission model) could a) learn over time or b) be based on rules (for example, context-based) [64]. Proactive privacy controls could also guide users through available settings [42] or notify them when in privacy-critical contexts [30] to, for example, avoid microphone access in private spaces or at custom timings [41,67]. Alternatively, privacy controls could adapt to users' profiles and, e.g., suggest revoking certain permissions vs. entirely uninstalling certain apps [22].

Our study data shows that before and after the study, participants were interested in getting proactive support, such as being notified, especially regarding permissions related to location, camera, and microphone use. While these permissions are essential for using some applications (e.g., a microphone for using the phone), in many cases, permissions are secondary (e.g., microphone access for a messenger application supporting text-based communication). As discussed above, other examples include revoking permissions for non-active apps, as implemented since Android 11, and for non-essential vs. essential permissions for a certain app. A proactive privacy control mechanism could focus on permissions users care about from a privacy perspective but still consider functionalities essential to users based on the intended use of a certain app (e.g., consuming vs. producing content). Considering contextual information can improve recommendations for privacy settings [71,79]. Also, permissions non-essential for the core functionality could be detected automatically (cf. the Reaper approach [33]). Communicating to users which permissions are a pre-condition for using a certain functionality can additionally help them make a decision [76]. As such, the overall decision load could still be kept rather low.

Moreover, information on permissions that are (un)desired could be crowd-sourced based on users' comments, as suggested in prior work: CHAMP analyzes users' comments to point to undesired and/or privacy-intrusive app behaviors [50]. However, the capabilities and opportunities of novel smartphones and apps keep changing, as do users' preferences. This indicates user preferences should be assessed repeatedly.

5.4 Bulk Revocations & Opportune Moments

When participants updated permissions for a specific app, independent of the (external) trigger, they often seemed to engage in updating more permissions for the given app (4.08 permissions per application on average) as well as permissions for other apps (in 106 cases) in short time frames. This is interesting for two reasons: First, current privacy interfaces

on mobile devices such as Android's *Permission Manager* and *Privacy Dashboard* already foster bulk permission updates by displaying other apps with the same permission or other permissions for the same app. With knowledge of applications for which users jointly change permissions, permission management interfaces could proactively suggest groups of apps for which a particular permission could be changed. Second, this point in time represents an opportune moment in which users are willing and motivated to engage in a privacy/security activity. Due to the two-hour time window of our study, we were not able to explore those opportune moments in more detail, but future work could look at phone usage patterns, users' current mood or necessity of the current privacy decision [31]. Leveraging this information could further support users in maintaining correct permission states for them.

6 Conclusion

We presented an in-depth investigation of users' awareness of and control over privacy permissions on Android. In a two-week field study with 132 Android users, we collected initial permission states of installed applications as well as updates of permission states throughout the study and experience sampling data. We found that participants mostly revoked access to sensors they consider sensitive (such as microphone or camera), but only if this would not affect an application's core functionality, assuming the app is frequently used. Moreover, participants often conducted such permission updates in bulk. This work provides a better understanding of users' current use of available privacy control mechanisms and serves as a basis to enhance (proactive) mobile privacy control.

References

[1] Android 12. https://www.android.com/android-12/, 2022. last accessed: 2023-02-15.

[2] Choose a category and tags for your app or game. https://support.google.com/googleplay/android-developer/answer/9859673?hl=en, 2022. last accessed: 2023-02-15.

[3] Firebase App Distribution. https://firebase.google.com/docs/app-distribution, 2022. last accessed: 2023-02-15.

[4] Firebase Crashlytics. Track, prioritize, and fix crashes faster. https://firebase.google.com/products/crashlytics, 2022. last accessed: 2023-02-15.

[5] Firebase Realtime Database. Store and sync data in real time. https://firebase.google.com/products/realtime-database, 2022. last accessed: 2023-02-15.

[6] How do I balance my sample within demographics? https://researcher-help.prolific.co/hc/

en-gb/articles/360009221213, 2022. last accessed: 2023-02-15.

[7] MPAndroidChart. https://github.com/PhilJay/MPAndroidChart, 2022. last accessed: 2023-02-15.

[8] Permissions on Android. https://developer.android.com/guide/topics/permissions/overview, 2022. last accessed: 2023-02-15.

[9] Permissions updates in Android 11. https://developer.android.com/about/versions/11/privacy/permissions, 2022. last accessed: 2023-02-15.

[10] Permissions updates in Android 11. One-time permissions. https://developer.android.com/about/versions/11/privacy/permissions#one-time, 2022. last accessed: 2023-02-15.

[11] Photo picker. https://developer.android.com/training/data-storage/shared/photopicker, 2022. last accessed: 2023-02-15.

[12] Prolific. A higher standard of online research. https://prolific.co/, 2022. last accessed: 2023-02-15.

[13] Request app permissions. https://developer.android.com/training/permissions/requesting, 2022. last accessed: 2023-02-15.

[14] SurveyKit: Create beautiful surveys on Android. https://github.com/quickbirdstudios/SurveyKit, 2022. last accessed: 2023-02-15.

[15] What's new in Kotlin 1.6.20. https://kotlinlang.org/docs/whatsnew1620.html, 2022. last accessed: 2023-02-15.

[16] Android Developers - Documentation. PackageManager. https://developer.android.com/reference/android/content/pm/PackageManager, 2023. last accessed: 2023-05-15.

[17] Android Developers - Documentation. UsageStatsManager. https://developer.android.com/reference/android/app/usage/UsageStatsManager, 2023. last accessed: 2023-05-15.

[18] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '19, pages 1–16, Berkeley, CA, USA, 2019. USENIX Association.

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

[20] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020.

[21] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 787–796, New York, NY, USA, 2015. Association for Computing Machinery.

[22] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J. Wisniewski. Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[23] Evita Bakopoulou, Anastasia Shuba, and Athina Markopoulou. Exposures Exposed: A Measurement and User Study to Assess Mobile Data Privacy in Context, 2020.

[24] David G. Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J. Aviv. Security and privacy perceptions of Third-Party application access for google accounts. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 3397–3414, Boston, MA, August 2022. USENIX Association.

[25] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. Exploring decision making with Android's runtime permission dialogs using in-context surveys. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 195–210, Santa Clara, CA, July 2017. USENIX Association.

[26] Weicheng Cao, Chunqiu Xia, Sai Teja Peddinti, David Lie, Nina Taft, and Lisa M. Austin. A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 803–820. USENIX Association, August 2021.

[27] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products.

In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[28] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. HCI in Business: A Collaboration with Academia in IoT Privacy. In Fiona Fui-Hoon Nah and Chuan-Hoo Tan, editors, *HCI in Business*, pages 679–687, Cham, 2015. Springer International Publishing.

[29] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 4:54–75, 2021.

[30] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[31] Jessica Colnago and Hélio Guardia. How to Inform Privacy Agents on Preferred Level of User Control? In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, UbiComp '16, page 1542–1547, New York, NY, USA, 2016. Association for Computing Machinery.

[32] Lorrie Faith Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, 10:273, 2012.

[33] Michalis Diamantaris, Elias P. Papadopoulos, Evangelos P. Markatos, Sotiris Ioannidis, and Jason Polakis. 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*, CODASPY '19, page 37–48, New York, NY, USA, 2019. Association for Computing Machinery.

[34] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. Are You Ready to Lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, page 750–761, New York, NY, USA, 2014. Association for Computing Machinery.

[35] Yusra Elbitar, Michael Schilling, Trung Tin Nguyen, Michael Backes, and Sven Bugiel. Explanation beats context: The effect of timing & rationales on users' runtime permission decisions. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 785–802. USENIX Association, August 2021.

[36] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security*, SOUPS '17, pages 399–412, Berkeley, CA, USA, 2017. USENIX Association.

[37] Johannes Feichtner and Stefan Gruber. Understanding Privacy Awareness in Android App Descriptions Using Deep Learning. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*, CODASPY '20, page 203–214, New York, NY, USA, 2020. Association for Computing Machinery.

[38] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android Permissions Demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, page 627–638, New York, NY, USA, 2011. Association for Computing Machinery.

[39] Adrienne Porter Felt, Serge Egelman, and David Wagner. I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '12, page 33–44, New York, NY, USA, 2012. Association for Computing Machinery.

[40] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. Association for Computing Machinery.

[41] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[42] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[43] Radhika Garg and Christopher Moreno. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 3(2), June 2019.

[44] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77:226–261, 2018.

[45] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Investigating People's Privacy Risk Perception. *Proceedings on privacy enhancing technologies*, 2019(3):267–288, 2019.

[46] Hana Habib and Lorrie Faith Cranor. Evaluating the Usability of Privacy Choice Mechanisms. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 273–289, Boston, MA, August 2022. USENIX Association.

[47] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, Baltimore, MD, August 2018. USENIX Association.

[48] Yangyang He. Recommending Privacy Settings for IoT. In *Proceedings of the 24th International Conference on Intelligent User Interfaces: Companion*, IUI '19, page 157–158, New York, NY, USA, 2019. Association for Computing Machinery.

[49] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. Who Should Get My Private Data in Which Case? Evidence in the Wild. In *Mensch Und Computer 2021*, MuC '21, page 281–293, New York, NY, USA, 2021. Association for Computing Machinery.

[50] Yangyu Hu, Haoyu Wang, Tiantong Ji, Xusheng Xiao, Xiapu Luo, Peng Gao, and Yao Guo. CHAMP: Characterizing Undesired App Behaviors from User Comments Based on Market Policies. In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, pages 933–945, 2021.

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

[52] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[53] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In Jim Blyth, Sven Dietrich, and L. Jean Camp, editors, *Financial Cryptography and Data Security*, pages 68–79, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[54] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, page 3393–3402, New York, NY, USA, 2013. Association for Computing Machinery.

[55] Jennifer King, Airi Lampinen, and Alex Smolen. Privacy: Is There an App for That? In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, New York, NY, USA, 2011. Association for Computing Machinery.

[56] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 437–456, Berkeley, CA, USA, August 2020. USENIX Association.

[57] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. Exploring Privacy Concerns about Personal Sensing. In Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe, editors, *Pervasive Computing*, pages 176–183, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[58] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. Are iphones really better for privacy? a comparative study of ios and android apps. *Proceedings on Privacy Enhancing Technologies*, 2022(2):6–24, March 2022.

[59] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, page 724–725, New York, NY, USA, 2003. Association for Computing Machinery.

[60] H. Lee and A. Kobsa. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, New York, NY, USA, 2016. IEEE.

[61] H. Lee and A. Kobsa. Privacy preference modeling and prediction in a simulated campuswide IoT environment.

In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 276–285, New York, NY, USA, 2017. IEEE.

[62] Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. What Matters to Users? Factors That Affect Users' Willingness to Share Information with Online Advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, New York, NY, USA, 2013. Association for Computing Machinery.

[63] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, SOUPS '16, page 27–41, USA, 2016. USENIX Association.

[64] Nathan Malkin, David Wagner, and Serge Egelman. Runtime Permissions for Privacy in Proactive Intelligent Assistants. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 633–651, Boston, MA, August 2022. USENIX Association.

[65] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*, page 83–95, New York, NY, USA, 2020. Association for Computing Machinery.

[66] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, NordiCHI '20, New York, NY, USA, 2020. Association for Computing Machinery.

[67] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.*, 21(1), February 2021.

[68] Moses Namara, Reza Ghaiumy Anaraky, Pamela Wisniewski, Xinru Page, and Bart P. Knijnenburg. Examining Power Use and the Privacy Paradox between Intention vs. Actual Use of Mobile Applications. In *European Symposium on Usable Security 2021*, EuroUSEC '21, page 223–235, New York, NY, USA, 2021. Association for Computing Machinery.

[69] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. In *Proceedings of the International Conference on Ubiquitous Computing*, UbiComp '08, page 182–191, New York, NY, USA, 2008. Association for Computing Machinery.

[70] Claudia Oellers and Eva Wegner. Does germany need a (new) research ethics for the social sciences? *German Council for Social and Economic Data (RatSWD) Working Paper Series*, 2009.

[71] Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux. Smarper: Context-aware and automatic runtime-permissions for mobile devices. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 1058–1076, 2017.

[72] Stefan Palan and Christian Schitter. Prolific.ac — A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17:22–27, 2018.

[73] Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. "Secure Settings Are Quick and Easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, AVI 2022, New York, NY, USA, 2022. Association for Computing Machinery.

[74] John Rothchild. Against Notice and Choice: the Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else). *Cleveland State Law Review*, 2018.

[75] Paul M Schwartz and Daniel Solove. Notice and choice: Implications for digital marketing to youth. In *The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children*, pages 1–6, 2009.

[76] William Seymour, Mark Cote, and Jose Such. Legal obligation and ethical best practice: Towards meaningful verbal consent for voice assistants. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[77] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. Can systems explain permissions better? understanding users' misperceptions under smartphone runtime permission model. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 751–768. USENIX Association, August 2021.

[78] Robert H Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L.*, 14:370, 2014.

[79] Daniel Smullen and Yuanyuan Feng. The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences. *Proc. Priv. Enhancing Technol.*, 2020(1):195–215, 2020.

[80] Alina Stöver, Sara Hahn, Felix Kretschmer, and Nina Gerber. Investigating how users imagine their personal privacy assistant. *Proc. Priv. Enhancing Technol*, 2:384–402, 2023.

[81] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, page 435–450, Berkeley, CA, USA, 2019. USENIX Association.

[82] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[83] Niels van Berkel, Denzil Ferreira, and Vassilis Kostakos. The Experience Sampling Method on Mobile Devices. *ACM Comput. Surv.*, 50(6), dec 2017.

[84] Niels van Berkel and Vassilis Kostakos. *Recommendations for Conducting Longitudinal Experience Sampling Studies*, pages 59–78. Springer International Publishing, Cham, 2021.

[85] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. Android permissions remystified: A field study on contextual integrity. In *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC'15, page 499–514, USA, 2015. USENIX Association.

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

[87] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. Dynamically regulating mobile application permissions. *IEEE Security & Privacy*, 16(1):64–71, 2018.

[88] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[89] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, November 2019.

[90] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. "revoked just now!" users' behaviors toward fitness-data sharing with third-party applications. *Proceedings on Privacy Enhancing Technologies*, 2023(1):21, 2023.

A Project Material

To access the anonymized dataset and the study application, please contact the authors.

B Android Privacy Interfaces
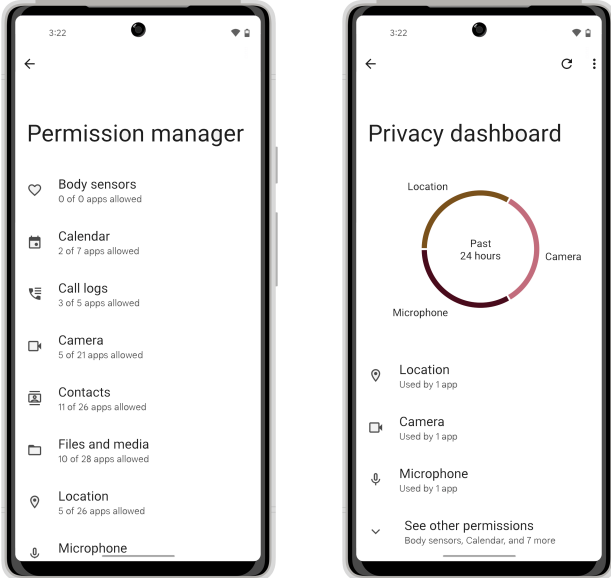
Figure 3: Android Privacy Interfaces: The *Permission Manager* (left) lists permission types along with apps that currently do or do not have access to these. The *Privacy Dashboard* (right, Android 12 and above) provides a more detailed overview of which applications currently have access to which sensors, along with means to grant or revoke this access [1].

C Study Questionnaires

C.1 Privacy Perceptions (Initial & Final)

- For which categories of information do you want to be alerted, if an app requests access. 1/3
  - Location
  - Physical Activity
  - Body Sensors
  - Bluetooth
  - Installed apps
  - None of these

- For which categories of information do you want to be alerted, if an app requests access. 2/3
  - Other users on the smartphone
  - External File Storage
  - Calendar
  - Call history
  - Contacts
  - None of these

- For which categories of information do you want to be alerted, if an app requests access. 3/3
  - Phone Numbers
  - SMS
  - Microphone
  - Camera
  - None of these

C.2 Midterm Questionnaire

- Do you know that you can revoke permissions you previously granted to apps? (yes/no)
  - *if yes* Have you revoked a permission before? (yes/no)
    * *if yes* Why did you revoke that permission? multiple choice
      · I didn't need the feature anymore.
      · I was concerned for my privacy.
      · I was concerned for the security of my device.
      · I didn't think about it.
      · None of these.

- *For Android 12 only:* Have you used the Privacy Dashboard before? (yes/no)
  - *if yes* How often do your use the Privacy Dashboard? single choice
    * At least once a week
    * At least once a month
    * Less than once a month

- *Android versions <12:* Have you looked at the [Permission Manager name of installed Android version] before?
  - *if yes* How often do you look at the [Permission Manager name of installed Android version]? single choice
    * At least once a week
    * At least once a month
    * Less than once a month

- Please look at the [Permission Manager name of installed Android version] after our questions. You can find it under [Path].

C.3 Experience Sampling Questionnaires

C.3.1 Questions Upon Permission Change (ESM control questionnaire)

Granted Permission: Why did you allow [AppName] to [Android description for permission]? multiple choice
- I wanted to enable a feature of the app.
- The app asked for it.
- I didn't think about it.
- Other
  - Please briefly explain your decision for [AppName]. (free text entry)

Revoked Permission: Why did you forbid [AppName] to [Android description for permission]? multiple choice
- I didn't need the feature
- I was concerned for my privacy
- I was concerned for the security of my device
- I didn't think about it
- Other
  - Please briefly explain your decision for [AppName]. (free text entry)

C.3.2 Daily Questions (ESM awareness questionnaire)

- Is [App name] currently allowed to [Android description for permission]? (yes/no/I don't know)

D   Study Results

D.1   Detailed Demographics

Table 7: Demographic Overview of Participant Sample: age, gender, nationality, employment, and educational level. We sampled participants by residency (not nationality), to ensure consistency in app stores. As a result, our sample contains a few participants with Asian and South American nationalities.

Age	18–29	98	*Employment*	Full-Time	38
	30–39	27		Unemployed (and job seeking)	32
	40–49	5		Other	27
	50–54	2		Part-Time	26
				Not in paid work (e.g. homemaker, retired or disabled)	5
Gender	Woman (including Trans Female/Trans Woman)	65		Due to start a new job within the next month	3
	Man (including Trans Male/Trans Man)	63		Data expired	1
	Non-binary (would like to give more detail)	4			
			Education	High school diploma/A-levels	52
Nationality	Poland	40		Undergraduate degree (BA/BSc/other)	43
	Portugal	26		Graduate degree (MA/MSc/MPhil/other	23
	Italy	22		Technical/community college	8
	Greece	14		Secondary education (e.g. GED/GCSE)	4
	Spain	6		Doctorate degree (PhD/other)	2
	Czech Republic	4		Don't know / not applicable	1
	United Kingdom	3			
	other (Europe)	12			
	other (Asia)	2			
	other (South America)	2			
	other (North America)	1			

D.2   RQ1: Awareness of Current Privacy Permission States

Table 8: Participants' answers to daily random questions on current permissions states. Per permission, we list the number of *correct* and incorrect answers and how often this permission and state occurred in daily random questions (in ESM awareness questionnaires) in our dataset.

Permission Name	Permission State: **Granted**			Permission State: **Denied**		
	# questions	**correct** ("yes")	**incorrect** ("no")	# questions	**correct** ("no")	**incorrect** ("yes")
write calendar	27	12	10	12	9	
read call log	46	30		6	5	3
record audio	78	57	10	159	89	28
write contacts	52	27	10	40	21	7
camera	129	75	31	224	113	73
access media location	61	35	16	26	13	8
read contacts	122	73	26	137	63	37
read external storage	325	159	70	448	138	135
access coarse location	146	95	23	162	47	60
access fine location	142	95	21	156	45	52
read phone numbers	7	7		18	5	11
read phone state	167	89	33	182	46	62
Bluetooth scan	15	6	4	38	9	2
read calendar	24	14	3	26	6	15
write external storage	223	89	51	448	100	88
get accounts	97	49	14	138	29	65
access background location	18	14	32	6	12	
query all packages	175	29	18	134	14	25
activity recognition	16	5		1	6	1
read SMS	27	12	8	7	4	3
body sensors	10	8	1	1		1

D.3 RQ2: Controlling Permissions

Table 9: Controlling Permissions: Overview of *revoked* permission updates per app throughout the study, with number of installations and total usage time. Applications that were potentially preinstalled are marked in bold, and applications that are among the most used apps (see Table 6) are marked with *. Note that only apps with at least 16 updates throughout the study are listed.

App	Number of Installs	Total Usage Time (hours)	Permission Updates: Revokes
Mi Video	51	2.35	31 Bluetooth scan (31)
Snapchat*	35	116.41	28 read phone numbers (4), access background location (3), get accounts (3), read call log (3), write contacts (3), access coarse location (2), access fine location (2), read contacts (2), read phone state (2), camera (1), read external storage (1), record audio (1), write external storage (1)
TikTok*	62	1494.08	27 query all packages (11), access coarse location (2), camera (2), read calendar (2), read contacts (2), read external storage (2), record audio (2), write calendar (2), write external storage (2)
HMS Core	18	0.51	26 access background location (2), access coarse location (2), access fine location (2), activity recognition (2), Bluetooth scan (2), camera (2), get accounts (2), query all packages (2), read calendar (2), read external storage (2), write calendar (2), write external storage (2), read contacts (1), read SMS (1)
PayPal	65	6.00	24 access coarse location (3), access fine location (3), camera (3), read contacts (3), read external storage (3), read phone state (3), write contacts (3), write external storage (3)
Teams	49	16.76	21 query all packages (2), access background location (2), access coarse location (2), access fine location (2), camera (2), get accounts (2), read contacts (2), read external storage (2), write contacts (2), write external storage (2), record audio (1)
Telegram*	50	303.96	21 access background location (2), access coarse location (2), access fine location (2), camera (2), get accounts (2), read contacts (2), read external storage (2), record audio (2), write contacts (2), write external storage (2), read call log (1)
Vinted	28	42.22	18 access coarse location (3), access fine location (3), camera (3), read contacts (3), read external storage (3), write external storage (3)
Mi Browser	14	1.36	18 camera (4), record audio (4), access coarse location (3), access fine location (3), read external storage (1), write external storage (1), query all packages (1), read phone state (1)
Twitter*	48	280.76	18 access coarse location (2), access fine location (2), camera (2), get accounts (2), read contacts (2), read external storage (2), read phone state (2), record audio (2), write external storage (2)
Youtube*	121	888.21	18 access coarse location (2), access fine location (2), camera (2), get accounts (2), read contacts (2), read external storage (2), read phone state (2), record audio (2), write external storage (2)
Reddit*	51	467.04	17 access coarse location (4), camera (4), read external storage (4), record audio (4), write external storage (1)
Google Pay	39	0.16	16 access coarse location (2), access fine location (2), camera (2), query all packages (2), read contacts (2), read external storage (2), read phone state (2), write external storage (2)

Table 10: Controlling Permissions: Overview of *granted* permission updates per app throughout the study, with number of installations and average usage time. Applications that were potentially preinstalled are marked in bold, and applications that are among the most used apps (see Table 6) are marked with *. Only apps with at least 16 updates throughout the study are listed.

App	Number of Installs	Total Usage Time (hours)	Permission Updates: Grants
Phone*	105	150.47	31 access coarse location (3), Bluetooth (3), get accounts (3), read call log (3), read contacts (3), read SMS (3), record audio (3), write contacts (3), read external storage (2), read phone state (2), write external storage (2), access fine location (1)
Google*	123	207.93	25 access coarse location (2), access fine location (2), Bluetooth (2), get accounts (2), read calendar (2), read call log (2), read contacts (2), read phone state (2), read SMS (2), record audio (2), write calendar (2), write contacts (2), camera (1)
Bluetooth	37	0.17	25 access coarse location (2), Bluetooth (2), get accounts (2), read call log (2), read contacts (2), read external storage (2), read SMS (2), write contacts (2), write external storage (2), access fine location (1), access media location (1), Bluetooth scan (1), query all packages (1), read phone numbers (1), record audio (1), read phone state (1)
TikTok*	62	1494.08	21 query all packages (18), Bluetooth (2), Bluetooth scan (1)
Galaxy Store	14	1.44	18 Bluetooth (4), read phone state (4), get accounts (3), read external storage (3), write external storage (3), query all packages (1)
Snapchat*	35	116.41	17 Bluetooth (3), camera (2), read external storage (2), record audio (2), write external storage (2), Bluetooth scan (1), access coarse location (1), access fine location (1), read contacts (1), read phone numbers (1), read phone state (1)