Privacy Slider: Fine-Grain Privacy Control for Smartphones

FLORIAN BEMMANN, LMU Munich, Germany
HELENA STOLL, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany

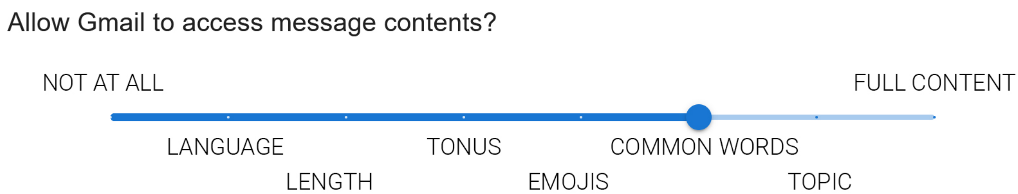


Fig. 1. Privacy Slider enables users to granularity select which data they want to share with smartphone apps.

Today, users are constrained by binary choices when configuring permissions. These binary choices contrast with the complex data collected, limiting user control and transparency. For instance, weather applications do not need exact user locations when merely inquiring about local weather conditions. We envision sliders to empower users to fine-tune permissions. First, we ran two online surveys (N=123 & N=109) and a workshop (N=5) to develop the initial design of *Privacy Slider*. After the implementation phase, we evaluated our functional prototype using a lab study (N=32). The results show that our slider design for permission control outperforms today's system concerning all measures, including control and transparency.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; **Empirical studies in interaction design**; • **Security and privacy** → **Social aspects of security and privacy**.

Additional Key Words and Phrases: privacy, mobile devices, smartphone, permissions

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

1 Introduction

Ubiquitous and mobile devices use various user behavior data, e.g., mobile behavior [55], location [57], and physiological data [52]. These tracking features enable adaptive and intelligent user interfaces, providing the user with information right when needed, e.g., [38]. For this, users enable various permissions [9] with extensive insights into the user's personal profile [40]. However, only around 6% of users understand the scope of the permissions they agree to [60]. Shen et al.

Authors' Contact Information: Florian Bemmann, LMU Munich, Munich, Germany, florian.bemmann@ifi.lmu.de; Helena Stoll, LMU Munich, Munich, Germany, He.Stoll@campus.lmu.de; Sven Mayer, LMU Munich, Munich, Germany, info@sven-mayer.com.

ACM 2573-0142/2024/9-ART272
https://doi.org/10.1145/3676519

[60] argued that current mobile systems hardly convey to users what happens with their data and which specific data is used. Moreover, apps request permission, such as location, to display weather information and full device access to support accessibility. However, the weather could be forecasted by only knowing the current city, and the screen readers only need the screen content – not full access. Current permission systems do not allow fine-grain control but only some toggle switches for groups of data access [40]. In combination, users are often unaware of what they agree to and do not have the necessary control when understanding the specific case. Thus, users need more transparency in the process coupled with better control of their data.

With smartphones becoming more intelligent, apps and services require increasingly more contextual user data to provide high-quality support, e.g., O'Donoghue and Herbert [49]. To reduce potential privacy issues, the researcher has proposed a wide range of mechanisms to preserve the users' privacy. The simplest solution is outsourcing the decision-making process to an algorithm [24, 47, 53]. However, it takes away all control from users. Thus, Gao et al. [29] opposed recommending decisions to the user and not just taking them for them. Moreover, decisions might be context-dependent [69]. This raises the question: Are all-or-nothing decisions, as they are implemented with the current grant or deny toggle switches, a good option in the first place? The current operating system addresses this by adding a frequency component to the permission, which the user can set for how long the permission is valid. However, the underlying decision as to which specific data the app has access remains the same. For this, Olejnik et al. [47] added an option "obfuscate" as an alternative to "deny" and "grant." Here, obfuscate helps to retain privacy which 73% of users found useful. An alternative approach is by Malviya et al. [44], who envisioned that fake data could be used to make a function work while protecting the users' privacy. While these are options to increase the privacy level of the users' data, they lack the ability to allow the users to determine the abstraction level of data to be shared. In other words, the user will still be given full device access and meter-precise location. In summary, the permission interface has to meet the tradeoff of giving users detailed control while sufficiently summarizing and reducing the options so that users are not overwhelmed.

In this work, we aim to address the limitations of today's all-or-nothing permission control systems. As such, we designed and developed a fine-grain permission system. In detail, we envision replacing today's toggle switch with a *Privacy Slider* to hand full data control back to the user. For this, we first conducted an online survey (N=123) to understand what control users envision they need to gain control over their data. In detail, we asked how they could subdivide the all-or-nothing permissions; for instance, the location could be subdivided using the location precision. The results show a total of 135 potential steps for ten data types. Next, we investigated the user's concern concerning the steps using an online study ($N = 109$). This allowed us to rank and potentially group the steps to optimize usability; we supported this step by conducting a workshop ($N = 5$) before starting a multi-stage design and development process of our *Privacy Slider*. In a final evaluation ($N = 32$), we compared *Privacy Slider* to the classical toggle switches in two scenarios: a permission popup and the device permissions screen.

With this paper, we make a set of contributions all leading up to the design and implementation of *Privacy Slider*. Our first two studies show how sliders can support control and transparency based on steps between today's all-or-nothing choices. The subsequent implementation showed that *Privacy Sliders* significantly outperformed toggle switches with respect to privacy, security, control, transparency, and understandability. Thus, *Privacy Sliders* have the potential to support users in making better decisions when controlling their devices' permissions.

2 Related Work

In the following, we review the literature with respect to permission systems on smartphones. We first highlight the limitations and drawbacks of current systems. Next, we look at alternative ideas to the current systems, such as automatic systems and fine-grain permission manipulation.

2.1 Limitations of Smartphone Permission Systems

Mobile devices, such as smartphones, collect various data about their users, context, and usage [39]. All major mobile operating systems implement a permission system, where users must grant data access for specific data types to apps individually [51]. However, the implemented smartphone privacy concepts face limitations and rarely introduce real privacy from a user perspective [23]. Christin et al. [16] found that existing privacy-enhancing systems lack clarifying privacy implications, and users behave inconsistently with their concerns. Balebako et al. [4] found that users are not careless on that topic, but instead have misconceptions about data sharing that happens through smartphone apps and lack sufficient information. On the other hand, users outweigh anticipated costs and potential benefits, referred to as *privacy calculus* [18]. Here, users accept data being collected in exchange for being able to use a service, c.f. *Price of Convenience* [36]. Additionally, today we see *digital resignation* [20, 59] or *privacy fatigue* [15] as an overload or lack of control leads to resignation, i.e., users giving up dealing with privacy decisions. As such, users face a challenge with the fundamental concepts of permissions and the associated privacy.

We also see limitations in the user interface itself. For instance, during permission requests, users show low comprehension [25], leading to a *lack of transparency*. Also, apps often do not convey understandably which information leaves the phone, making it hard for users to understand potential privacy leakages [4]. The wording in the permission UI was also found to be hardly understandable, and it was hard for users to grasp the implications [35]. A general *lack of control* is a crucial cause of privacy concerns [43], which has been shown in the online shopping and social media context [66]. Keusch et al. [37] raised concerns about the lack of control. In some cases, users do not even have privacy in their own hands, e.g., if one user leaks a contact list to a service, the other users (who are contained in that contact list) can not do anything against it [51]. The aforementioned two aspects, transparency and control, are identified as the two main pillars of information privacy [6, 30], also coined as the principles of *notice and choice* [56, 72]. A privacy issue introduced by app developers is *permission overclaiming*, also called *permission overdeclaration* [2]. By setting permissions that are too coarse, developers may claim less data access than they technically have permission-wise. An inappropriately huge amount of permissions also reduces user trust in an application [63]. Fang et al. [23] studied permission overclaiming on the example of the internet permission. This permission poses insufficient expressiveness to enforce control over internet access (i.e., access could be restricted) [5]. They found that many applications would tolerate stricter permission here. 62% request internet permissions, but 36% make requests to specific domains only. Furthermore, third-party libraries that request permission for their purpose lead to that permission being claimed to the full application [50]. Finally, laziness among developers can lead to permission overclaiming due to confusion about the scope of individual permissions [63] and the aim to “just make it work” [5].

2.2 Improving Permission Systems

Fostering **transparency** is one important factor in ensuring users understand the impacts of giving permissions. Thus, a wide range of suggestions to improve transparency has been envisioned, such as adding a purpose to permission toggles Hong et al. [32] (e.g., “file access *for backup*”). Moreover, Cao et al. [12] showed that giving explanations could cut the permission denial rate in their study in half. Mapping permission requests to UI elements helps the understandability [41] about which components of an app actually make use of each permission. Another way to implement transparency in mobile apps is privacy dashboards. They show the users the data they have collected in an aggregating or feed-like view. While this method increases transparency, Bemmann et al. [6] has shown that users are also getting afraid and feel their privacy being more intruded if transparency is realized without accompanying *control* features.

An opposing approach is relieving the user from privacy decisions through **automatic permission** choice prediction systems, e.g., [24, 29, 47, 53], which try to enhance users' privacy. However, their effect on actual privacy is disputed; for instance, Elbitar et al. [21] argue that there are no one-fits-all permission decisions. Thus, automatic approaches could be limited in their usefulness. Furthermore, with changing context, users might want to reevaluate their decision, which Wijesekera et al. [69] investigates by detecting such incidents to trigger the permission request again.

Beyond individualized solutions, many technical solutions have been proposed to serve as a middleware between the app and the user as privacy-enhancing technologies (PETs) for smartphones (e.g., [3, 22, 58]), for an in-depth survey see Shrivastava et al. [61]). Moreover, Pennekamp et al. [51] reviewed privacy enforcement strategies on smartphones. On the level of user manipulation, they structure concepts regarding privacy mechanisms into three categories: 1) **reporting** (e.g., omnipresent install prompts, permission visualization, and ways to allow tracking the flow of private information),2) **fine-grained tuning** (such as user-based configurations), and 3) **fencing** information (e.g., Mockdroid [7], TISSA [73], SHAMDROID [11]).

2.3 Fine-Grain Permission Systems

With the evolution of mobile operating systems, fine-grained control has proliferated in slow steps. Permission popups allowing to choose "only one time" access mitigate the issue of permanent access [45]. Hong et al. [32] already proposed sliders as interface elements as an extension for the one-time-only feature with three options options: allow, ask, and deny. Research proposed various approaches to give users finer control of their data. Jeon et al. [33] categorize permissions into four classes (e.g., outside resources, sensors), each of which common strategies for permission subdivision can be applied. Zhou et al. [73] enables users to bypass the compulsion to grant permission to use an application by giving the option to pass falsified data such as empty data, anonymized data, or bogus. Other approaches involve restrictions on how many times a critical resource may be accessed [46] and context-dependent privacy policy configuration [17].

More drastically, Scoccia et al. [58] restructure the Android permission interface by allowing users to (1) make permissions on a feature level and (2) grant finer-grained permissions by introducing permission levels, i.e., a granularity at which data / a resource can be accessed. They found that users appreciated the greater choice, felt more control, and had higher trust. The traditional Android permissions, in contrast, were described as misleading, and the enforced binary choice was not preferred. However, their study is rather proof of the general concept of more granularity in smartphone permissions, emphasizing the realizability in Android. The major part of their contribution is an implemented app instrumentation and its evaluation. The design process of their so-called permission levels has come up rather short.

3 Research Gap and Derived Concept of a Continuous Permission System

In summary, the presented related work uncovers technical papers in designing and implementing measures to give control to the users. However, only a few studies investigated the user perspective (e.g., Pennekamp et al. [51] rated usability themselves). Only a few studied finer-grained permissions (e.g., Scoccia et al. [58]) and, if so, emphasize technical aspects rather than the user. Moreover,

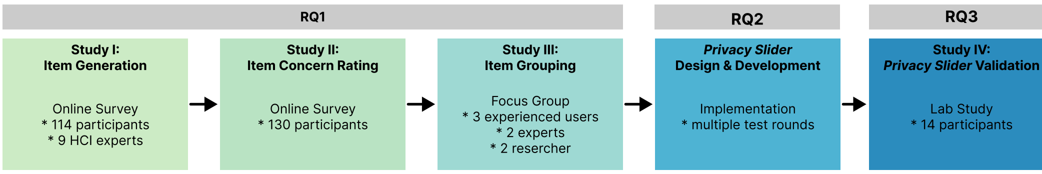


Fig. 2. The development process of *Privacy Slider*.

the review shows that the choices given to the user by today's systems are typically binary, most prominently toggle switches. At the same time, it is clear that choices are often not binary. For instance, to get the weather forecast, apps do not need the user's precise location; the city the user is in would be enough to determine whether an umbrella is necessary today. However, current systems only allow an all-or-nothing choice, which causes many privacy concerns and allows for more potential to infringe on users' privacy than necessary.

As a result, we witness the need for more fine-grained mobile permission systems that enable users to configure their data logging on steps between granting access to all or nothing. For this, we pose three research questions:

RQ1 *What are helpful sub-steps for fine-grained data control?*
RQ2 *How do we deliver the additional control that is usable?*
RQ3 *How does it perform compared to the existing Android permission UI?*

We conducted four studies to address these questions; see Figure 2. In Study I ($N = 123$), we investigated the potential items that are of interest to users to be controllable. In Study II ($N = 109$), we asked users to rate the items concerning their privacy concerns. We used these concerns in Study III ($N = 5$) to rank and group the items into semantically similar groups. Moreover, we investigated possible representation methods, such as how much abstraction and control users want. In combination with multiple rounds of testing and debugging, we developed the final look and feel of *Privacy Slider*. Lastly, we carried out an A/B testing ($N = 32$) to ensure the usability outperforms the industry standard using toggle switches to control users' data. We provide our data evaluation scripts, anonymized study data, and study artifacts; see Section 11.

4 Study I: Item Gathering and Concern Rating (Online Survey - RQ1)

In this study, we investigate what users would like to control beyond current binary options. Here, we intentionally ask users and experts to gain both perspectives: a) What do users understand to be important for them? and b) What could developers see as important to enable certain applications? Therefore, we conducted an online survey ($N = 123$) with smartphone users and HCI experts to reach a sample of diverse experience levels regarding UX and privacy.

We asked participants to envision the use of 10 different data types to explore new avenues for a future permission system. Here, we prompted them with the following ten data types: *app usage*, *camera usage*, *incoming message*, *notification*, *phone calls*, *screen content*, *text input*, *user activity*, *voice input*, and *volume & brightness*. The data types are rooted in a combination of typically tracked and collected data [55] and common activities [8]. Moreover, all of them can be tracked today and are typically controlled via phone permissions.

4.1 Procedure

First, we explained the procedure and content of the study and asked to give informed consent. Next, we asked participants' demographic data such as age, gender, education, and professional field. See the complete question in the supplementary materials. We collected participants' ideas for each

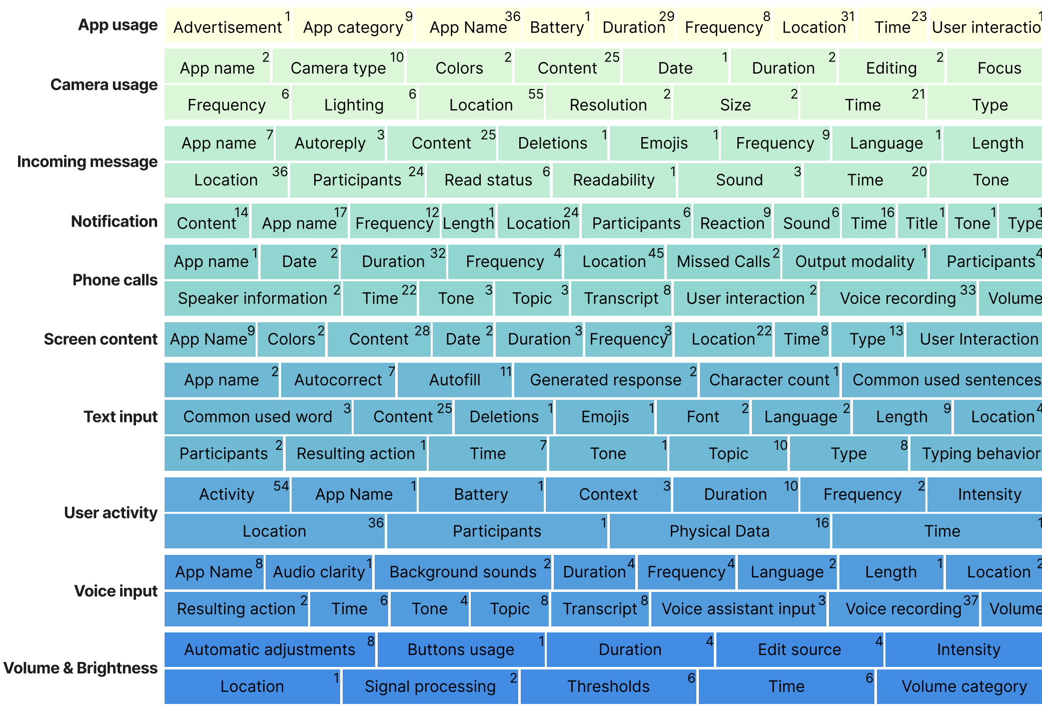


Fig. 3. The 135 codes for the ten data types that emerged from the 1339 participant statements.

datatype using the question: *"Which intermediate stages would you find useful?"*. Participants did this for ten specific data types. Additionally, we asked participants for the logging frequency, which is a property overarching over all data types. At the end of the survey, we rewarded participants with 9 GBP per hour.

4.2 Participants

In total, we recruited 123 participants. We recruited 28 participants from our institution and an additional 86 participants via Prolific to diversify the sample. Additionally, we supplemented the sample with 9 HCI experts whom we personally recruited to reflect expert opinions. We required all participants to use a mobile phone or tablet at last almost daily. Participants were between 19 and 74 years old ($M = 29.1, SD = 9.4$), and 64 identified as female, 58 as male, and one as diverse. The majority reported a university degree as their highest degree of education (85), 19 had a high school degree, 28 had a high school diploma, 5 had a completed apprenticeship, 4 had a secondary school degree, and one participant finished school without graduation. Their top 5 professional fields were IT, electrics and engineering (45), economy and logistics (14), social and pedagogy (12), services and sales (11), and arts and media (8). In total, our sample resided in 19 different countries, most from Germany (37), South Africa (33), Portugal (10), and the United Kingdom (9).

We determined the targeted sample size on the go via thematic saturation, i.e., when the recruitment of further participants did not reveal new steps [42]. We stopped recruitment when the saturation index reached a threshold of 90%, which, through the underlying information weighting model, expresses that the probability of mentions being shared between existing and new participants is 90%.

4.3 Results

We used Python, R, and ATLAS.ti to analyze the data and ensure the validity of the responses. We received 1339 individual feedback statements for the different data types. We analyzed our participants' responses using Affinity Diagramming [31]. We formed code groups per datatype. Through this process, we sorted the 1339 statements into 135 distinct codes. On average, each participant contributed 9.9 codes ($SD = 11.9$). Figure 3 gives a visual overview of the final groups. We retrieved the most distinct codes for the datatype *text input* (21 distinct ideas), *phone calls* (16), and voice inputs (16).

The most common mention across many data types is the location at which a logging event/data item took place, i.e., the location of physical activity, the location the user was at when receiving a text message, etc. It was mentioned as the most frequent step in 6 of 10 data types and was mentioned second frequently for the remaining 4.

For data types where it is appropriate, the name of the respective data item was mentioned often, i.e., for datatype *physical activity*, the activity's name, and for *app usage*, the app's name. The point of time was within the top 5 steps for all data types except *text input* and *voice input*. Also, the duration was mentioned often (e.g., on rank 4 for *activity* and *phone calls*, and rank 3 for *app usage*).

4.4 Summary

With this study, we came up with codes, i.e., characteristics that users deem important for ten data types, whereby many steps are common for multiple data types. However, we do not know whether the frequency of how often a code is mentioned is an indicator of importance, relevance to the user, or privacy concern. It may rather depend on how present an aspect is in the users' minds. Existing research shows that people are initially rather unaware of privacy risks and do hard naming their concerns unless they are confronted with the topic (c.f. Furini et al. [28]). The order of the collected steps is thus neither given by the survey participants nor naturally by the aspects' characteristics. Thus, next, we conducted an additional study to obtain a concern ranking, which is required to place them on a slider scale.

5 Study II: Item Concern Rating (Online Survey - RQ1)

With the results of Study I, we next investigate how the 135 codes (see Figure 3) are rated with respect to their privacy concern. It will inform the design of potential mechanisms to allow users to make fine-grain console adjustments. Thus, we conducted another online survey ($N = 109$) and let users rate their perceived privacy concerns for the codes.

5.1 Procedure

First, we explained the procedure and content of the study. Afterward, we asked them to consent to the data recording and storage. Next, we asked participants' demographic data such as age, gender, education, and professional field. For each step that resulted from the item gathering study (c.f. Figure 3), participants had to rate their agreement with a statement worded "I am very concerned with my smartphone tracking *duration of the activity (e.g., 1h)*" on a continuous (101 point) slider item [27, 54]. We grouped the items on survey pages by datatype, presenting a total of 135 items distributed over 10 pages to the user. Each page started with a short paragraph reminding the participants of their task and context. Steps for the overarching property *frequency* were not ranked, as they are all-time indications that have a natural order. We disclose all study instruments in the supplementary materials of this paper.

5.2 Participants

In total, we recruited 109 participants (42 from our institution and 67 via Prolific). As in the first study, participants had to be fluent in English or German and use a mobile phone or tablet at last "almost daily." Their ages are between 18 and 60 years ($M = 29.7, SD = 9.5$), with 60 identifying as female, 47 as male, one as a diverse participant, and one who preferred not to disclose. The majority reported a university degree as their highest degree of education (65), 34 had a high school degree, 3 had a secondary school diploma, 5 had a completed apprenticeship, and two participants finished school without graduation. Their top 5 professional fields were IT, electrics and engineering (31), economy and logistics (13), health (11), social and pedagogy (9), unemployed (6), service and sale (5), and arts and media (2). 32 did not identify themselves with the given groups and specified other professions. In total, participants reside in 17 distinct countries. The most represented countries of residence were Germany (43), South Africa (21), Portugal (12), and Greece (4).

5.3 Results

The participant's general privacy concern ratings over all items are in the middle of the 1-100 scale ($M = 45.8$, $SD = 33.8$). The concern values are distributed in a rather bimodal distribution, i.e., the fewest values are in the middle range, around 50, and most values are either very low or very high. A slight tendency to the left shows that people were more often rather less concerned than rather high.

Taking a look at the stated concern value grouped by datatype, we see that spoken/written contents were rated most concerning, with phone calls having the highest concern ratings ($Mdn = 59$, $SD = 35.1$) and voice input the second highest ($Mdn = 55$, $SD = 34.8$). Text inputs and screen contents are both on rank three ($Mdn = 46$, $SD = 33.8$). The lowest concern ratings were stated for volume and brightness ($Mdn = 24$, $SD = 31.4$). The values for all ten data types are in Figure 4.

5.4 Summary

As a result of study I and II, we created a collection of steps for a set of common data types. We have not performed any reduction or grouping of steps yet. However, to avoid overloading the UI, a reduction of a reasonable number of steps has to be considered. To group steps, we see two general options: (1) Numerically, i.e., merging steps with close-by concern rating into a group, or (2) semantically. To make this and other design decisions, we will conduct a focus group in the following.

6 Study III: Focused Exploration (Focus Group - RQ1)

In the previous two studies, we have collected steps that represent subaspects of logged data, accompanied by privacy concern ratings. The results of both studies suggest that it is possible to subdivide today's toggle switches to set up permissions. Study I gave a wide range of steps between all or nothing, and Study II ordered them according to the users' concern level. While this allows us to put all steps on a slider, ensuring full transparency and control; to the users; however, with so many steps, the usability might suffer. Thus, next, we investigate potential user-facing presentations of a novel permission system using a focus group. This investigation will inform the design.

6.1 Procedure

After explaining the focus group and answering any open questions, we asked participants to fill out a consent form and demographics questionnaire. Then, the participants introduced themselves and were introduced to the topic. We introduced the general idea and discussed the differences,

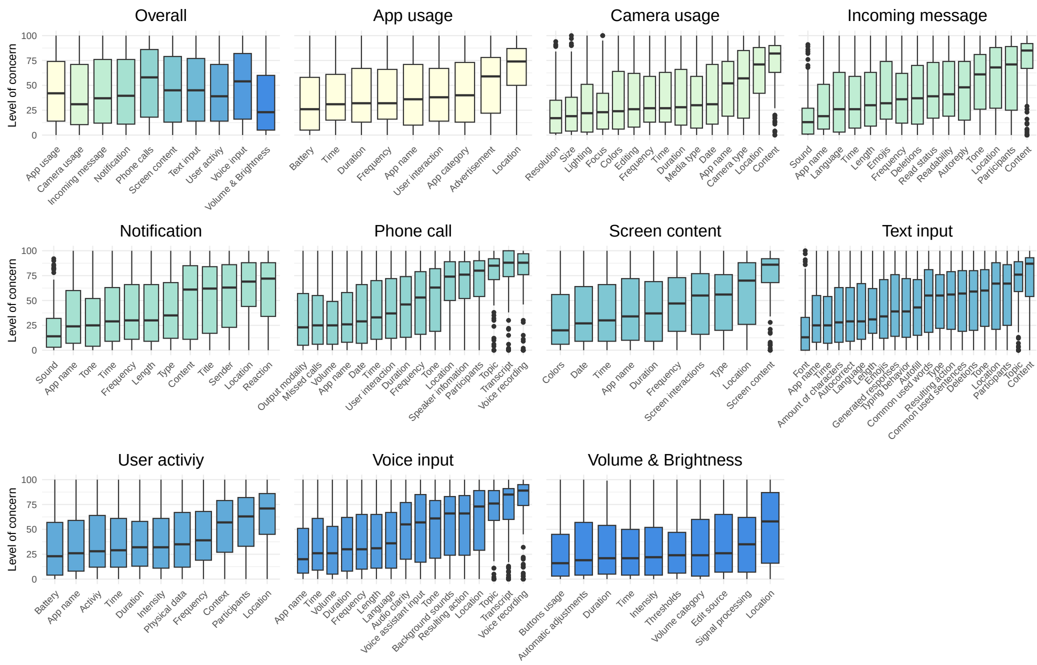


Fig. 4. Boxplot of the concern ratings in our item concern rating study. The black line indicates the median.

pros, and cons between toggles and sliders. As the next step, the focus group leader presented the collected steps from Study I augmented using the concerns of Study II for each datatype (see supplementary materials). With this information, we asked the participants to envision to group and potentially sort the steps with the goal of keeping transparency and control high but at the same time also the usability. Finally, the group discussed how the sliders could be best integrated into smartphone usage, i.e., when users would use them and what is needed for effective use.

6.2 Participants

The focus group was conducted with 5 participants (3 female, 2 male) and led by the two first authors. The participants were between 24 and 29 years old ($M = 26.6$, $SD = 2.4$). We were aiming for the perspective of both experts and the user side, so we recruited two experts and three smartphone-experienced users. The experts were HCI researchers who are currently pursuing their Ph.D. The three users were two students and one public service employee.

6.3 Results

The focus group took just over one hour. We did an audio recording and transcribed this into a text file, which we then coded using ATLAS.ti. This resulted in 49 distinct codes that were assigned a total of 90 times. We grouped the codes into 7 code groups, which constitute the topics presented in the following.

Use Case and Target Audience of Privacy Sliders. The focus group identified privacy sliders as **a way to simplify privacy settings for users who are not willing to spend time or don't have sufficient technology understanding** to do so. P1 mentioned *"I don't think the idea of the slider is a bad one because it would make it easier for a lot of people who don't deal with such things that* *much."* - [P1], and P2 came up with a concrete example of a family member *"[...] I can tell my mom that once you are halfway through the slider, the app can do more, but it also knows more about you."*. The participants also pointed out that it is important not to curtail expert users in their control over their data, i.e., still **have detailed control options available on demand** *"But maybe it would be good, as [P2] says, that you would then still have the possibility to set individual things differently."* - [P1] and proposed separate toggles, e.g., to turn off single aspects. P2 summarized the combination of privacy sliders and on-demand toggles as *"Good thing for people without much IT knowledge [...], but if I deal with it, then I can use the fine limb ticks."*

Privacy Slider Scope. The focus group came up with the idea of having **one central, default privacy configuration that overarches all apps and data types**: *"I would expect to be able to set it in the system once, all abide by it, and if they need something extra then I am asked."* - [P1]. When users are about to perform some action, they are least willing to deal with privacy configuration and would benefit from a default configuration *"If you want to take a picture, it should be fast, but first you have to adjust everything"* - [P3]; *"Therefore already before!"* - [P1].

Finer Granularity for Continuous data types. When the group discussed how much sense sliders would make for specific data types, P1 and P2 came up with examples of use cases where a reduced granularity of data would be sufficient. P1: *"I have an example for the location theme. If you could then just go in again and change that again, then it's enough if I can set the city, state, and country. Or I would like to say more precisely that I am currently in XY street."*. The group had the opinion that ordering steps for a slider specifically on location data is easy, concluding that **a slider to control location granularity** would be good. *"Although I would say with location, within locations, I would find it exciting if it was a slider. From not at all, to city or urban area at 300m."* - [P1]. Similar ideas arose for content, such as texts, speech, and images. *"Kind of like the direct content, it is obvious what's on the far right and everything before that is what you can infer through the content. So like tone, emoji, language."* - [P2]. A level of *"content abstraction"* [P2] was proposed as a continuous scale that could be mapped onto a slider.

Grouping of Steps. Participants suggested to rather **group steps by topic** instead of strictly adhering to privacy concern levels. They proposed various groups that make sense to them, e.g., P3 suggesting that *"Time and Duration could be put together, so everything that has this time and duration aspect."* or P1 who distinguishes between personal and contextual data: *"I would try to separate it like this: personal data, the data that is more context and something like location or context plus data related to something like app name"*. A general **desire for grouping** was expressed especially in cases where many steps exist *"It's just a lot. So you couldn't display it like that on the slider; you would have to group it in any case."* - [P3].

Ordering of the steps. We discussed the order of steps in the focus group, which was derived from Study II (Item Concern Rating). Participants **overall agreed with the resulting order**. However, the difficulty of deciding on an appropriate order varied with the datatype. P1 and P2 stated that they **did hard ordering the steps of app usage and activity**, while they found that ordering text input went intuitively easy through the degree of content abstraction. The focus group participants could not comprehend why camera type and duration were rated relatively concerning, while physical data and emojis received a surprisingly low concern rating.

The Relation between Data Privacy Concern and Importance. When discussing the privacy concern rating in turn of the step order, the focus group also discussed whether the concern is the right ordering criterion in this case. P3 mentioned that she doesn't find the location very private if it is really necessary: *"I don't think that's so bad because you need the location for many apps. Be it* *renting a car or scooter or Google Maps."*. In line with this, the idea is to order by the ratio of privacy sensitivity and importance in a specific use case.

User Desires and Design Decisions. When a system contains multiple privacy sliders (e.g., for various data types), it is important that **consistency of similar steps positions** is guaranteed. Otherwise, users might face unexpected behavior. *"The location should always be specified the same. Also, if you now have different sliders and I would now set everything to 60 or so, then I would also expect that it is somehow everywhere the same "safe". And if then suddenly a location is already at 50, then that would be super stupid, just because I do not want to read every time."* - [P1]. The exact position of steps on the slider was not deemed that important. P2 suggested mapping them with equal distances instead of trying to represent the exact concern values.

6.4 Summary

The focus group gave us a good understanding of people's opinions on how our insights from Study I and II could be fused into a privacy slider design. They agreed that sliders are appropriate, especially for data types that impose a natural order, such as location or content. A slider interface might especially benefit non-expert users, but we also note that it is important not to restrict expert users by removing detailed controls. The privacy slider design should thus incorporate both concepts, system-level settings, and runtime permission slider.

7 Privacy Sliders: The Final Design (RQ2)

Based on our two surveys, the focus group, and a review of related work, we propose a concept for privacy sliders – a novel user-centered mobile data permission system. Privacy sliders realize two central aspects: First, a simpler, easier user interface that enables quick and easy privacy setting-making. It targets users who are either novices or not willing to spend much time on their data privacy configuration. Second, privacy sliders enable users to choose a custom level of granularity, at which they want to allow to pass data to an app. Both are presented in detail in the following two subsections.

7.1 The System-Level Settings Slider - Sliders as Simplification for Fast and Consistent Privacy Configuration

We propose to implement one slider as a central, default privacy configuration, which overarches all apps and data types. A prototype is sketched in Figure 5: The more to the right the user pushes the system-level slider, the more detail is granted for every datatype. To meet expert users' needs and individual needs on specific data types, the access level to a datatype can be overwritten. One slider per datatype allows overriding the system-level slider's setting (e.g., in Figure 5: For the location, the user has configured lower granularity data access).

Based on the results of our focus group, we envision that this simplifies the way users indicate their privacy preferences. Especially novice users and those who do not want to spend much time on privacy configurations might benefit from the intuitive and fast UI of a slider.

7.2 Enhanced Permission Popups: Information Minimization of Continuous data types

In the focus group, we found that for some data types, such as location and content (text, speech, and camera were mentioned), it makes sense to configure granularities. Steps for location data could, for example, be reduced to an accuracy of +/- 500 m, city, or country. For many use cases, that might be sufficient. For example, when using a weather forecast app, it would be sufficient if the OS passes the city name to the app instead of the user's precise location. Content abstraction procedures could similarly be applied to content, such as text messages.

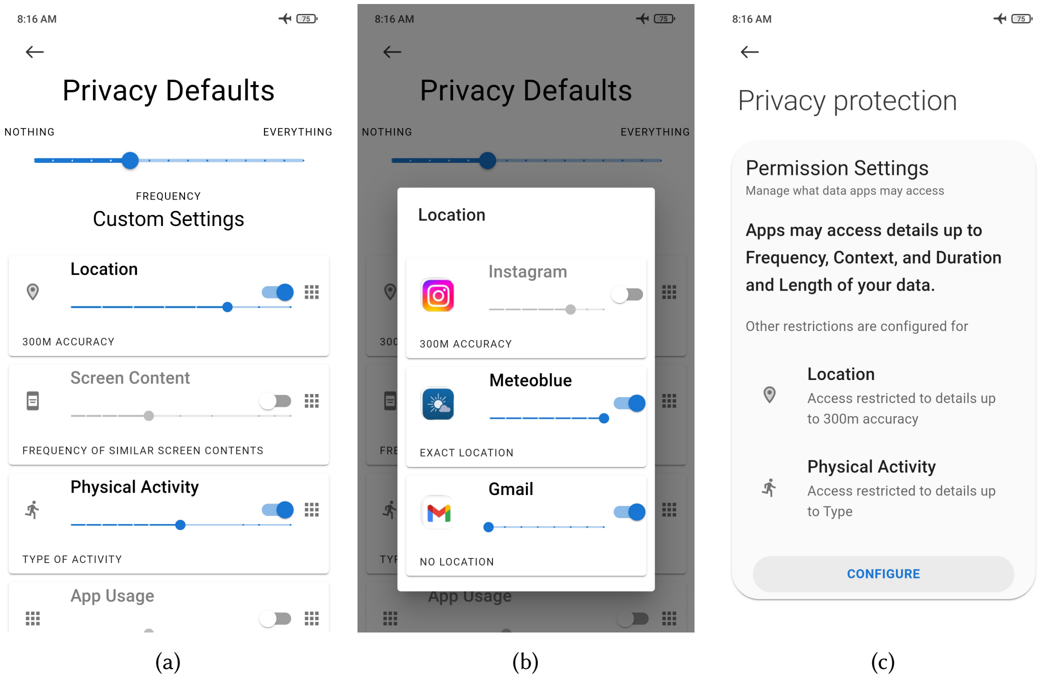


Fig. 5. The system-level slider (a) is used to configure the phone's general privacy settings, per default applying to all apps and overarching all data types. It especially targets users who do not want to spend much time making single privacy decisions. The sub sliders below allow to set overriding configurations for single data types. A popup (b) allows to make settings per app, and the overview screen (c) summarizes the settings.

Supplementing the previously presented system-level slider, our privacy slider concept introduces such configuration options for location and content. These sliders (see Figure 6 (a) and (b)) are meant to replace the current permission UIs, e.g., the *only one time, always, when using the app* single-choice radio button interface that Android currently uses for location access permission.

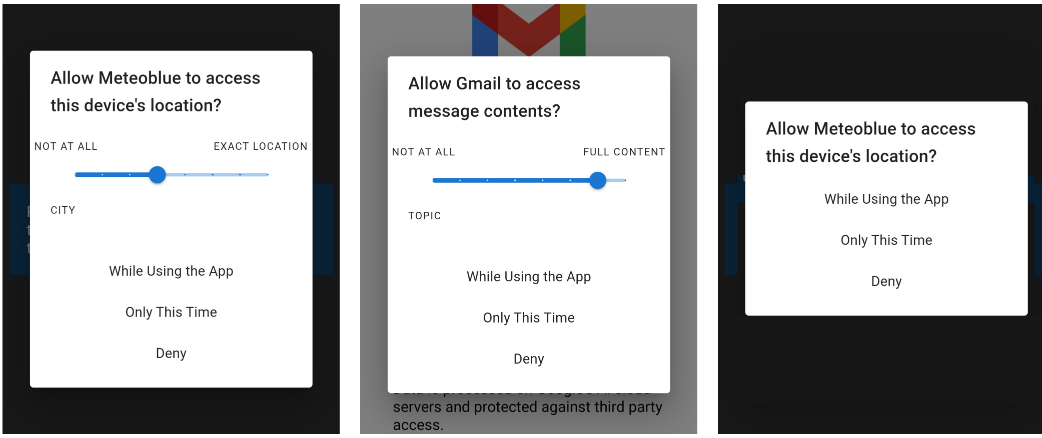
8 Study IV: Slider Validation (Lab Study - RQ3)

To evaluate our privacy slider concept, we implemented it as a prototype and conducted a lab study. Participants were asked to use both a UI mockup of a traditional permission interface and a mockup of the privacy slider interface concept. We assessed both interfaces' effects in a mixed-method approach, using survey items and interview questions. The study consisted of 4 scenarios, with participants going through them two times, once using traditional Android permission UI and once more using the slider interface. Three of the scenarios were runtime permission popup situations (see Figure 7), and the remaining one was the general privacy settings menu deploying our system-level slider (see Figure 5). The order in which the four scenarios were presented was randomized.

8.1 Apparatus

We mocked the Android permission UI (runtime popups see Figure 6 (c), and the settings menu see Figure 5 (c)) with a Progressive Web App[1]. The runtime permission popup scenarios consisted

[1]https://web.dev/progressive-web-apps/, last accessed 2024–07–28



(a) Location Slider (b) Content Abstraction Slider (c) Control Condition

Fig. 6. We enhance permission popups with a slider that allows to choose a level of granularity. (a) visualizes this in the example of the location permission, (b) for text message contents. On the very right (c), we show our control condition, consisting of a slider-less permission popup as it is implemented in the Android UI nowadays.

mainly of a series of app screenshots that the users clicked through, augmented with button and slider UIs that mimicked the permission interface. Launched in fullscreen mode and being tailored specifically to the study device, the UI experience was very close to real Android UI. To rule out the effects of the mock, we also mocked the traditional Android permission popup UI with this approach, instead of using the OS implementation.

8.1.1 Slider Steps: System-Level Slider. In Section 4, we collected potential steps for privacy sliders for each datatype and ranked them by their level of privacy concern in Section 5. However, in Section 6, we found that a strict order by privacy concern does not make sense to users, as the varying order of similar steps on different data types might lead to unexpected configurations. We thus follow the idea of the focus group to group the steps by topics *"that make sense"*. These groups then constitute the steps of the system-level slider and its sub-sliders (except the continuous data types location and content). Thus, the sliders for all data types are designed to be equal. We order the steps on their slider by the median concern value that our participants in Study II rated them.

8.1.2 Slider Steps: Location and Content. As pointed out by the focus group, location, and content pose an inherent granularity, which can be mapped to a continuous slider design. We chose the following steps, based on mentions from the focus group and proposed order in Section 5:

Location: not at all, country, state, city, urban area, 500m, 300m, street name, exact location

Content: not at all, language, length, tonus, emojis, common words/sentences, topic, raw content

8.2 Procedure

The study conductor met each participant in our lab in a separate room with a table. After explaining the study, the participants read and signed the consent form. We then started with a questionnaire on one's individual information privacy concern level using the IUIPC questionnaire [43]. Furthermore, we assessed affinity for technology interaction (ATI) [26] and demographics.

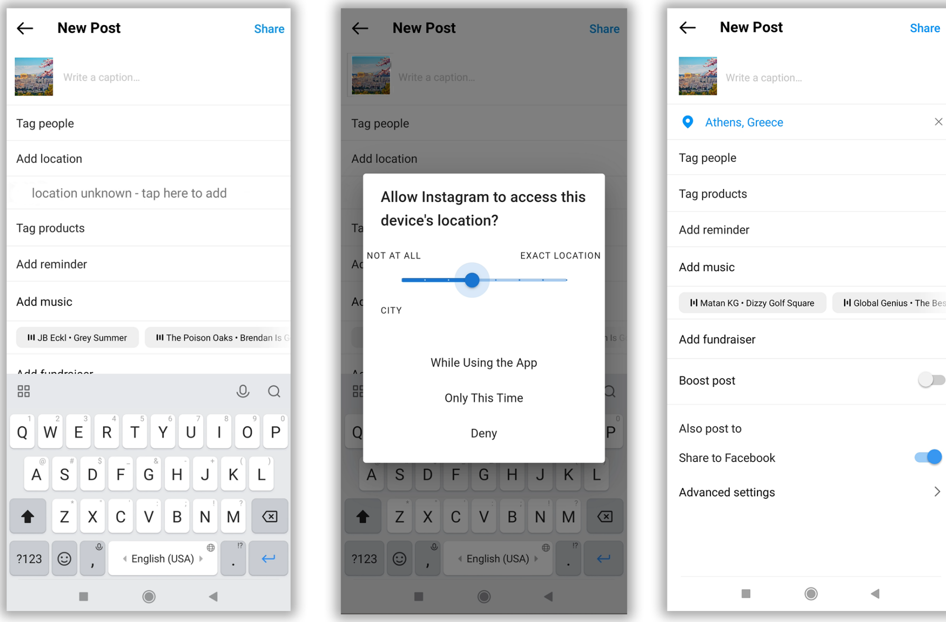


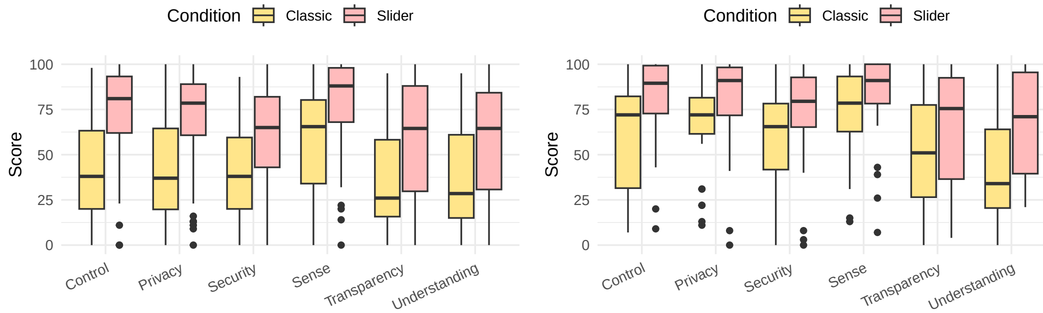
Fig. 7. A series of screenshots that shows one of the scenarios that we used in our studies from left to right: Here, the participant is advised to craft an Instagram post that is tagged with its location. This figure shows the privacy slider condition of the experiment.

To get participants into the thinking mode and to affiliate with the scenario of giving permissions, the study conductor talked with them for a couple of minutes about their last contact with smartphone permissions, what they thought and felt in that situation, and what the decision was like. Then we introduced them to one of the two conditions *Classic* or *Slider* in randomized order. For both conditions, we ran participants through the same procedure: a demo of the condition, then they tested the three showcases, and finally, they tested the system-level settings application. After each but the demo, they filled in a system usability scale (SUS) [34] questionnaire and answered six items on perceived control, privacy, security, making sense, transparency, and understanding. These items were assessed on a continuous slider scale; we disclose the wording in the supplementary materials. At any time, participants could verbally or in writing articulate additional feedback.

In the end, we asked participants additionally if they had any further feedback. We audio-recorded the full procedure and rewarded participants with 10 EUR per hour or the respective amount of study credit points. Participation took approximately 30 minutes to complete the study.

8.3 Participants

We recruited 32 participants via our university mailing list, Slack channel, Instagram, and personal contacts. We required participants to be smartphone users daily and fluent in English. Participants were between 21 and 70 years old ($M = 28.0$, $SD = 8.5$), with 18 female and 14 male participants. They reported having a Master's degree (16), a Bachelor's degree (9), a high school degree (4), a doctoral degree (1), not finished school (1), and a vocational education (1). All participants reside in Germany, besides one participant from the United States. To understand our sample's privacy



(a) Permission Runtime Popups (b) Permission Device Settings

Fig. 8. Ratings on five aspects around privacy compared for the classic permission UI and the slider UI. On the left (a) regarding permission popups on runtime, on the right side (b) for the device's settings menu.

perception, we assessed the IUIPC questionnaire [43]. Our participants rated their Awareness on average with 6.2 (SD = 1.3), Control with 5.7 (SD = 1.3), and Collection with 5.7 (SD = 1.2) (higher scores mean more privacy-affine). Their mean score of affinity for technology interaction (ATI) was 4.1 (SD = 1.0). This indicates a rather technology-affine sample. According to the classification of Franke et al. [26], the ATI of an average population is to be expected at around 3.5, with high ATI samples around 4.

8.4 Results

We run the statistical evaluation in Python and R. Moreover, we applied non-parametric tests when the normality was violated. We did the qualitative coding again in ATLAS.ti.

8.4.1 Usability. The users' rating on the system usability scores (SUS) was higher for the slider UI than for the classical UI, for both the runtime permission popup comparisons and the system-level settings menu, see Table 1. According to the adjective classification of Brooke [10], all interfaces' usability can be regarded as *excellent*; only the classic device settings menu was rated as *good*. However, only in the runtime comparison does the slider significantly outperform the classic approach, see Table 1.

8.4.2 Privacy Effects. For the system-level settings, we can use the classical Wilcoxon signed-rank test after confirming the non-normality of the data. However, for the permission runtime popups, we perform an ART-ANOVA [71] with task and participant as random factors to account for the differences between the three showcases. We compared the effects of the classic and the slider UI on their users' privacy perception, see Figure 8. We show that *Privacy Slider* outperforms the classic approach significantly in nearly all measures. The only non-significant items are the measures for usability and making sense in the system-level settings menu. However, descriptively, the slider also performs better for these items. See Table 1 for all measures and test results.

8.4.3 Qualitative Feedback. We coded the free text responses, transcribed audio recordings, and interview notes in ATLAS.ti. We then organized the codes into code groups, which constitute the following topics.

Slider Interface is Preferred over Classic Button Interface. In general, comments on the slider interface were better than on the classic button-only interface. Many participants mentioned that they preferred the slider interface, while none said that they'd rather stay with the classical version.

P39 described it as *"a big improvement over the usual UI and would definitely prefer this in all cases."*. Similarly, P12 *"No, I think its a great addition."* and P21 *"liked it much better than the previous one."*. In contrast, the classic condition was described as having *"not enough options for data privacy"* (P26) and being *"too general"*. P53 expected a *"more detailed option display"*. For continuous data types, such as location, the slider interface was more intuitive to use for some participants. One mentioned that they'd prefer it for continuous data types only: *"Slider, for me, is only useful for continuous values like distance."* (P51). Especially in the weather app scenario, the ability to configure a granularity makes sense to the participants, as, e.g., P60 stated: *"The weather apps don't require my exact location, so I like this slider feature here"*.

System-Level Settings: Better Overview and Easier Getting-Into with Sliders. People liked the ability to use sliders for the device-wide privacy settings as well. Participants liked the overview that the sliders gave on data collection. P39 reported on the system-level slider: *"This was close to perfect, I think this is how it should be. The granularity of specific sliders also grants insight into all the different data that is being collected, which the normal UI completely lacks."*. In contrast, the classical settings menu is often criticized as it is hard to get into it and lacks an overview. *"Especially at first glimpse, the system is not that easy to get an overview of."* (P62). The lack of transparency of the classical interfaces also leads to a lack of trust, as a further mention of P39 shows: *"Many options were hidden, and you have to kind of guess what each thing does. Also, not sure if the options will be reverted after an update."*. P26 complained that *"you have to click through more"* with the classic interface. Besides clear benefits, our participants also pointed out some drawbacks of the new slider interface. Criticism mainly evolved around the system-level slider, which stood on top of the settings screen above all individual permission sliders. e.g., P22: *"I don't think I would use one slider on the top. Especially as the different categories only make sense for some apps. Instead, I would get rid of the slider on top and instead have a categorical setting like privacy level high/medium/low, for example."*. P10 saw privacy risks for lazy, speeding users introduced by the system-level slider: *"On further reflection, this feature now strikes me as very risky to dangerous. For example, it could tempt me as an annoyed user to be happy to easily set the location permission for all my navigation and sports tracking apps to maximum, and thus unintentionally set e.g., the memory access permission for all apps ever downloaded to completely open as well."*

Besides some points of criticism, the participants liked the slider version overall. *"It is very sexy; please install it on every phone."* (P40). They saw the main benefit of the slider-based system-level settings menu in its intuitive understandability and overview. *"The permission settings were very clear and concise, it was easy to gain an impression of how the data would be used."* (P53). Less technology-experienced users would benefit: *"[The slider] controller [is] more intuitive for older people or people who do not have smartphone affinity."* (P25).

Table 1. The statistical results of Study IV. * we report F values for all but SUS using the ART-ANOVA.

	Runtime Popups								Device Settings							
	Classic		Slider		Normality		Wilcoxon*		Classic		Slider		Normality		Wilcoxon	
	M	SD	M	SD	W	p	W/F	p	M	SD	M	SD	W	p	W	p
SUS	81.9	9.2	88.2	11.1	.925	<.001	88.5	<.001	78.0	17.0	80.0	18.1	.887	<.001	203	.382
Control	39.7	26.2	73.7	24.8	.939	<.001	133.98	<.001	60.5	27.7	80.7	23.6	.876	<.001	63	<.001
Privacy	40.6	25.9	70.5	25.0	.939	<.001	107.21	<.001	66.1	24.6	80.4	25.2	.86	<.001	83.5	<.001
Security	39.8	24.4	61.9	26.1	.964	<.001	65.951	<.001	59.8	25.9	73.5	27.2	.9	<.001	84.5	<.003
Sense	59.7	28.2	81.0	21.2	.885	<.001	52.23	<.001	73.2	25.0	82.2	23.3	.835	<.001	117	.086
Transparency	33.6	24.9	58.6	31.3	.93	<.001	54.58	<.001	48.8	31.5	66.7	29.9	.922	<.001	114	<.009
Understanding	35.2	26.2	58.2	29.4	.935	<.001	54.183	<.001	40.6	29.6	66.2	29.4	.92	<.001	58.5	<.001

Sliders Improve Transparency. Besides improved control, participants also perceived higher transparency about the data collection. The sliders, with their steps, make transparent which aspects a permission encompasses *"The granularity of specific sliders also grants insight into all the different data that is being collected, which the normal UI completely lacks."* (P39), and even give the user more sense about how their data is used *"The permission settings were very clear and concise, and it was easy to gain an impression of how the data would be used."* (P53). Having an overview of the active steps of each permission slider, the user could quickly grasp what is collected *"They explained what exactly would be collected."* (P22). P28 further saw an explanatory effect and triggered reflection processes: *"Offers control but also explains the usage of the data, and by showing the different levels of data abstraction, people get a feeling of how much the data can actually capture and gives an opportunity to realistically reflect on their own boundaries."*.

More Perceived Control on How Data is Used. Participants mentioned that the system-level slider gives them control on *how* data is used: *"The permission settings were very clear and concise, and it was easy to gain an impression of how the data would be used."* (P53). However, we found that, independently of the applied method, participants felt a general lack of control over what happens with their data after granting access to it. Especially regarding the classic interface, many participants mentioned that the given control options only give control over what data is *passed* to an app, but not at all what thereafter *happens* with their data; i.e., with whom it is shared, how it is processed, where it is stored. We observed a general lack of trust in all that happens behind/after the granting interface, independent of the method. It was mentioned that *"trust [is] missing, the method is not the problem"* (P13). Similarly, P38 expresses issues with control over the later stages in the processing pipeline: *"This Interface suggests some form of privacy control, but unless one denies everything, there is limited control once data is in the app."*. P28 expressed missing *"control over where the data is stored, with whom it is shared, and what information is drawn from it."*. This issue is out of the scope of permission granting methods which we focus on in this paper, but nevertheless noteworthy for future work.

Slider Design. A couple of participants expressed different preferences of the slider's step order; for example, P21 generally expressed that *"The order of some levels of privacy didn't make much sense to me."* or P13 proposing based on their cultural background that *"emojis should go to the last. In India, different emojis are differently interpreted."*. Customization of steps per app was suggested by P38 *"The slider might be adjusted by application, since, for example, weather is no more accurate than a couple of 100 meters anyway."*. On the other hand, some participants were concerned about too many differences between the sliders. P10 said that inconsistencies in the slider steps could lead to unexpected behavior. A medium slider value should express a similar level of data and privacy across all sliders. In general, it was perceived as a *"very sufficient interface, and with a bit of background knowledge, it is easy to understand how it works and what it does."* (P52).

Detailed UI Comments. As for the nature of a high-fidelity prototype study, participants also pointed out many detailed UX improvement suggestions and criticisms of our prototype. During the study, a couple of unclarities in the UI were pointed out, especially regarding the slider-based system-level settings (e.g., *"not clear what gradations mean."* (P51)). The behavior of the sub sliders and their toggles was unclear to some participants (*"unintuitive what you turn on with the toggle?"* (P10)), also explanations on the slider steps, for example, with context menus, were desired. A few participants generally misconceived the slider steps as selecting instead of summing up. However, in general, the participants made themselves familiar with the slider UIs quickly, and further explanations by the study conductor were necessary in individual cases only.

8.5 Summary

We conclude that the concept of privacy slider was perceived very positively. Participants saw benefits in several scenarios, the usability was rated better than with the traditional privacy settings UI, and we found positive effects on transparency and control. We collected points of criticism that can be improved in future iterations. For example, step positions on the sliders should be determined by their concern level instead of the percentage of the slider scale, and the cumulative behavior has to be better explained.

9 General Discussion

9.1 Runtime Permission Sliders Outperform the Standard Permission UI

The feedback on runtime permission popup sliders was overall very good. Extending the current button UI with a continuous choice of data granularity made sense to our participants and was perceived as intuitive; regarding the system usability score, it significantly outperformed Android's current UI. Especially for data types that impose a natural degree of granularity (such as location), it was liked, and participants envisioned situations where they see an advantage in continuous permissions. With its straightforward user flow, which is close to Android's current design, users got into it easily, and there is not much that could trigger confusion. We argue for including this in future runtime permission popups. While fine-granular permission concepts have been published in the past occasionally, for example, by Jeon et al. [33] and Scoccia et al. [58], the present study is, to the best of our knowledge, the first study that implements it as a well-usable slider UI and studies its usability and applicability with lay smartphone users.

9.2 System-Level Settings Slider

Also, our participants preferred menu sliders in the system-level settings. We see a benefit, especially in the transparency and overview that they provide, what participants confirmed in their qualitative statements. The system-level slider on top was deemed a good feature for novice users, and the flat menu structure required users to click through less. However, the more complex nature of a whole settings menu in contrast to a single-case runtime popup makes designing challenging. This is reflected in a couple of remaining usability issues that we found in our study, and they need to be addressed before rolling this out in the wild.

Most importantly, user support should be included in helping users get into the principle of how the slider-based menu is working, such as a tour, as proposed by Carlèn [13]. Furthermore, it has to be ensured that users do not experience unexpected behavior across the sliders. In our study, we found that users perceived privacy concerns of specific steps differently, and thus would have expected a different order. However, with the system-level slider on top, it is essential that the subsliders that are moving alongside do not show unexpected configurations.

9.3 A Method-Independent Lack of Control of What Happens with the Data

In the qualitative feedback, participants mentioned that they desire more transparency and control over what happens with their data after permission has been granted. They also admit that this is out of the scope of our study on the permission-granting interface; however, we think this finding is nevertheless important to note. Sliders could, for this issue, be part of the solution as well. In our case of granting data access, sliders enabled control and conveyed transparency to their users. By generalizing privacy sliders to a modality for configuring data transactions, they could also find applications at other stages of the data pipeline. The setting options of how far data is passed on, or in what depth it is analyzed pose a natural order (for example, data not leaving the device, going to the app company's server only, being processed on a cloud server, being disclosed to third party companies, being made available publicly).

9.4 The Tradeoff Between Warning Fatigue and User Control

Permission interfaces have to deal with the tradeoff of warning fatigue, i.e., users' desire for control and, on the other hand, being overwhelmed by too much information and options. Users tend to ignore privacy-enhancing technologies (also coined *the challenge of user ignorance*) [1, 4] and concepts that foster their usage have to be considered, such as nudging approaches (e.g., Thompson et al. [64]). Control-providing concepts have to be designed with care, as sophisticated concepts may quickly annoy their users and thereby fail [51]. The privacy slider faces this issue for the runtime permission slider, which is to be used on permission requests. However, we expect the issue to be rather short-lived: After getting used to the privacy slider and its options, decision times might not be longer than for other interface concepts. Learning effects occurring in the long-term should mitigate the initially higher required effort. Literature on novel interface concepts in other domains, such as authentication [19], also follows such assumptions.

9.5 Contextual Privacy and Personalization

The privacy slider configuration could also be context-dependent. Users prefer data disclosure differently depending on their context, as Wang et al. [67] show in the example of online behaviors. Including context in runtime permissions helps, users make their decision [58] and enable an even more fine-grained choice, also called *flexible permission*[58]. A system that is able to understand and extract a contextual difference given, would even be possible without additional user burden. Contextual privacy has shown to be beneficial in various use cases, such as online privacy policies [70] or IoT [48]. Regarding smartphone permissions, research has shown that the incorporation of contextual cues can improve decisions [68] and studied machine-learning-based decision support [65]. We think that our fine-granular approach to permissions integrates well with such approaches. The non-binarity of continuous privacy configurations could be used to reflect model uncertainties, i.e., instead of a prediction model requiring the output to be a binary all-or-nothing decision, an insecure prediction could lead to a slider value somewhere in the middle. Furthermore, the context could be another dimension of configuration that could be controlled through a slider (e.g., rating private situations on weekends as more concerning and worthy of protection than behavior during office days).

9.6 Privacy Sliders Enable Novel Adaptive Use Cases

To avoid the unpleasant consequences of privacy issues, data usage by applications is restricted. Access to potentially sensitive resources, such as screen contents and detailed device activity, is in Android, for example, organized into the Android Accessibility services. Therefore, access is highly restricted to a few purposes only. By going from the current binary approach to fine-grained configuration, we envision that such resources could be opened to wider application purposes. Screen contents, for example, could be leveraged for adaptive application scenarios, such as predicting next-action sequences, if the data was abstracted to the smallest necessary level of detail. Exact text contents, like text messages, names, or login credentials, could be abstracted to tokens like *textmessage*, *name*, and *logindata*. They would thereby still be useful for several application scenarios but way less privacy-invading. Continuous permissions, realized through privacy sliders, thus not only have a privacy-preserving effect on the users but also enable novel opportunities for application and system developers.

9.7 Generalizability and Actionability of Privacy Slider

Defining the *one* slider configuration is difficult - our study (c.f. Section 5) has shown that users perceive the privacy implications of data type characteristics differently, and our focus group (c.f. Section 6) has come up with different ways on how to group and arrange slider steps. Furthermore, different apps and different permissions may require different slider configurations. The level of privacy leakage varies across apps and contexts (Chitkara et al. [14]). Privacy decisions should be contextualized, i.e., users should be able to decide in the context of the data's use case, as, for example, Chitkara et al. [14] propose in regard to third-party libraries. Research should explore ways to customize privacy slider per application and use case, either through manual parametrization by their developers, or leveraging automatized approaches such as proposed by Qu et al. [53].

The actionability of our findings for app developers is limited: Its practical application of privacy slider requires steps at the operating system level. Permission interfaces are an operating system feature that cannot be changed by individual apps. Apps need to become tolerant of possibly low-granular data. Therefore, changes to the software interfaces between the operating system and apps might also need to be made to allow the passing of information on the user-chosen data granularity level.

9.8 Future Work: Field Study

In the present study, we have focused on users' opinions on the privacy slider. We deliberately asked end-users because they are the major stakeholders regarding privacy; their data is worked with and they opt for buying and using their smartphone. In the next iteration of the privacy slider, developers should also be taken into account to see which effects fine-granular permissions would have on them and what changes from the development perspective, and find solutions on how developers could deal with that. Developers would need to deal with data of different granularity. If they, in the worst case, simply reject all except the finest data levels and thus force users to push the privacy slider to the finest level, not much would be won for the user. They still would be in the dilemma of granting (full) data access or not using the application (c.f. Stach and Mitschang [62]). Flexible data structures might be needed in mobile app frameworks, to make it easy to work with varying granularities of data. Furthermore, an in-the-wild study has to be conducted. Our lab study was appropriate for getting the first insights on privacy sliders, showed that it is promising, and yielded valuable insights for the next iterations. However, to see how users actually use them in real situations and which effects that has, a field study, where privacy sliders are distributed to the users' own devices, has to be conducted.

10 Conclusion

In this paper, we designed and evaluated *Privacy Slider*. They go beyond the current binary permission decisions and thereby empower users to make fine-grain privacy decisions. We ran two online surveys (N=123 & N=109) and a workshop (N=5) to develop the initial design of *Privacy Slider*. A lab study (N=32) that we conducted based on an implemented prototype showed that users prefer privacy sliders over the current smartphone permission interface. They are especially advantageous for novice users and when applied in runtime permission decisions. Furthermore, the privacy slider outperformed the classic interfaces in all measures, including increased perceived control and transparency.

11 Open Science

We encourage readers to reproduce and extend our results. Therefore, we made the data collected in our study and our analysis scripts available on the Open Science Framework https://osf.io/xj5qe/.

References

[1] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. 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* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 787–796. https://doi.org/10.1145/2702123.2702210

[2] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, Phillipa Gill, and David Lie. 2011. Short paper: a look at smartphone permission models. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (Chicago, Illinois, USA) *(SPSM '11)*. Association for Computing Machinery, New York, NY, USA, 63–68. https://doi.org/10.1145/2046614.2046626

[3] Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky. 2013. AppGuard-Enforcing User Requirements on Android Apps. In *TACAS*, Vol. 13. Springer, Berlin, Heidelberg, Germany, 543–548. https://doi.org/10.1007/978-3-642-36742-7_39

[4] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[5] David Barrera, H. Güneş Kayacik, Paul C. van Oorschot, and Anil Somayaji. 2010. A methodology for empirical analysis of permission-based security models and its application to android. In *Proceedings of the 17th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '10)*. Association for Computing Machinery, New York, NY, USA, 73–84. https://doi.org/10.1145/1866307.1866317

[6] Florian Bemmann, Maximiliane Windl, Jonas Erbe, Sven Mayer, and Heinrich Hussmann. 2022. The Influence of Transparency and Control on the Willingness of Data Sharing in Adaptive Mobile Apps. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 189 (sep 2022), 26 pages. https://doi.org/10.1145/3546724

[7] Alastair R. Beresford, Andrew Rice, Nicholas Skehin, and Ripduman Sohan. 2011. MockDroid: trading privacy for application functionality on smartphones. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (Phoenix, Arizona) *(HotMobile '11)*. Association for Computing Machinery, New York, NY, USA, 49–54. https://doi.org/10.1145/2184489.2184500

[8] Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer. 2011. Falling Asleep with Angry Birds, Facebook and Kindle: A Large Scale Study on Mobile Application Usage. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (Stockholm, Sweden) *(MobileHCI '11)*. Association for Computing Machinery, New York, NY, USA, 47–56. https://doi.org/10.1145/2037373.2037383

[9] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. 2017. Exploring decision making with Android's runtime permission dialogs using in-context surveys. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 195–210. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bonne

[10] John Brooke. 1996. Sus: a "quick and dirty'usability. *Usability evaluation in industry* 189, 3 (1996), 189–194.

[11] Lucas Brutschy, Pietro Ferrara, Omer Tripp, and Marco Pistoia. 2015. Shamdroid: gracefully degrading functionality in the presence of limited resource access. *ACM SIGPLAN Notices* 50, 10 (2015), 316–331.

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

[13] Filip Carlèn. 2017. *User Onboarding An investigation in how to increase the activation of new customers using design.* Master's thesis. Chalmers University of Technology. https://hdl.handle.net/20.500.12380/252779

[14] Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, and Yuvraj Agarwal. 2017. Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 42 (sep 2017), 22 pages. https://doi.org/10.1145/3132029

[15] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81 (2018), 42–51. https://doi.org/10.1016/j.chb.2017.12.001

[16] Delphine Christin, Andreas Reinhardt, Salil S Kanhere, and Matthias Hollick. 2011. A survey on privacy in mobile participatory sensing applications. *Journal of systems and software* 84, 11 (2011), 1928–1946. https://doi.org/10.1016/j.jss.2011.06.073

[17] Mauro Conti, Vu Thien Nga Nguyen, and Bruno Crispo. 2011. Crepe: Context-related policy enforcement for android. In *Information Security: 13th International Conference, ISC 2010, Boca Raton, FL, USA, October 25-28, 2010, Revised Selected Papers 13*. Springer, Berlin, Heidelberg, Germany, 331–345. https://doi.org/10.1007/978-3-642-18178-8_29

[18] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115. https://doi.org/10.1287/orsc.10.1.104

[19] Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2389–2398. https://doi.org/10.1145/2470654.2481330

[20] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8 (2019), 1824–1839. https://doi.org/10.1177/1461444819833331

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

[22] William Enck, Machigar Ongtang, and Patrick McDaniel. 2009. On Lightweight Mobile Phone Application Certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '09)*. Association for Computing Machinery, New York, NY, USA, 235–245. https://doi.org/10.1145/1653662.1653691

[23] Zheran Fang, Weili Han, and Yingjiu Li. 2014. Permission based Android security: Issues and countermeasures. *computers & security* 43 (2014), 205–218.

[24] Johannes Feichtner and Stefan Gruber. 2020. Understanding Privacy Awareness in Android App Descriptions Using Deep Learning. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy* (New Orleans, LA, USA) *(CODASPY '20)*. Association for Computing Machinery, New York, NY, USA, 203–214. https://doi.org/10.1145/3374664.3375730

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

[26] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[27] Frederik Funke and Ulf-Dietrich Reips. 2012. Why semantic differentials in web-based research should be made from visual analogue scales and not from 5-point scales. *Field methods* 24, 3 (2012), 310–327. https://doi.org/10.1177/1525822X12444061

[28] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. Privacy perception when using smartphone applications. *Mobile Networks and Applications* 25, 3 (2020), 1055–1061. https://doi.org/10.1007/s11036-020-01529-z

[29] Hongcan Gao, Chenkai Guo, Yanfeng Wu, Naipeng Dong, Xiaolei Hou, Sihan Xu, and Jing Xu. 2019. AutoPer: Automatic Recommender for Runtime-Permission in Android Applications. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1. IEEE, New York, NY, USA, 107–116. https://doi.org/10.1109/COMPSAC.2019.00024

[30] Gabriella M Harari. 2020. A process-oriented approach to respecting privacy in the context of mobile phone tracking. *Current opinion in psychology* 31 (2020), 141–147. https://doi.org/10.1016/j.copsyc.2019.09.007

[31] Gunnar Harboe and Elaine M. Huang. 2015. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proc. 33rd Annual ACM Conf. Human Factors in Computing Systems*. ACM, New York, NY, USA, 95–104. https://doi.org/10.1145/2702123.2702561

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

[33] Jinseong Jeon, Kristopher K. Micinski, Jeffrey A. Vaughan, Ari Fogel, Nikhilesh Reddy, Jeffrey S. Foster, and Todd Millstein. 2012. Dr. Android and Mr. Hide: fine-grained permissions in android applications. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (Raleigh, North Carolina, USA) *(SPSM '12)*. Association for Computing Machinery, New York, NY, USA, 3–14. https://doi.org/10.1145/2381934.2381938

[34] Aycan Kaya, Reha Ozturk, and Cigdem Altin Gumussoy. 2019. Usability measurement of mobile applications with system usability scale (SUS). In *Industrial Engineering in the Big Data Era: Selected Papers from the Global Joint Conference on Industrial Engineering and Its Application Areas* (Nevsehir, Turkey) *(GJCIE 2018)*. Springer, Cham, Switzerland, 389–400.

[35] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *Financial Cryptography and Data*

Security: FC 2012 Workshops, USEC and WECSR 2012, Kralendijk, Bonaire, March 2, 2012, Revised Selected Papers 16. Springer, Cham, Switzerland, 68–79.

[36] Paul E Ketelaar and Mark Van Balen. 2018. The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior* 78 (2018), 174–182. https://doi.org/10.1016/j.chb.2017.09.034

[37] Florian Keusch, Bella Struminskaya, Christopher Antoun, Mick P Couper, and Frauke Kreuter. 2019. Willingness to participate in passive mobile data collection. *Public opinion quarterly* 83, S1 (2019), 210–235. https://doi.org/10.1093/poq/nfz007

[38] Florian Künzler. 2019. Context-aware notification management systems for just-in-time adaptive interventions. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, New York, NY, USA, 435–436. https://doi.org/10.1109/PERCOMW.2019.8730874

[39] Nicholas D Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, and Andrew T Campbell. 2010. A survey of mobile phone sensing. *IEEE Communications magazine* 48, 9 (2010), 140–150.

[40] Hansoo Lee, Joonyoung Park, and Uichin Lee. 2022. A Systematic Survey on Android API Usage for Data-Driven Analytics with Smartphones. *ACM Comput. Surv.* 55, 5, Article 104 (dec 2022), 38 pages. https://doi.org/10.1145/3530814

[41] Yuanchun Li, Yao Guo, and Xiangqun Chen. 2016. PERUIM: Understanding Mobile Application Privacy with Permission-UI Mapping. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 682–693. https://doi.org/10.1145/2971648.2971693

[42] Andrew Lowe, Anthony C Norris, A Jane Farris, and Duncan R Babbage. 2018. Quantifying thematic saturation in qualitative data analysis. *Field methods* 30, 3 (2018), 191–207.

[43] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[44] Vikas Kumar Malviya, Chee Wei Leow, Ashok Kasthuri, Yan Naing Tun, Lwin Khin Shar, and Lingxiao Jiang. 2023. Right to Know, Right to Refuse: Towards UI Perception-Based Automated Fine-Grained Permission Controls for Android Apps. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering* (Rochester, MI, USA) *(ASE '22)*. Association for Computing Machinery, New York, NY, USA, Article 186, 6 pages. https://doi.org/10.1145/3551349.3559556

[45] Kristopher Micinski, Daniel Votipka, Rock Stevens, Nikolaos Kofinas, Michelle L. Mazurek, and Jeffrey S. Foster. 2017. User Interactions and Permission Use on Android. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 362–373. https://doi.org/10.1145/3025453.3025706

[46] Mohammad Nauman, Sohail Khan, and Xinwen Zhang. 2010. Apex: extending Android permission model and enforcement with user-defined runtime constraints. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (Beijing, China) *(ASIACCS '10)*. Association for Computing Machinery, New York, NY, USA, 328–332. https://doi.org/10.1145/1755688.1755732

[47] Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux. 2017. Smarper: Context-aware and automatic runtime-permissions for mobile devices. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 1058–1076. https://doi.org/10.1109/SP.2017.25

[48] Emmanuel Onu, Michael Mireku Kwakye, and Ken Barker. 2020. Contextual Privacy Policy Modeling in IoT. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, New York, NY, USA, 94–102. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00030

[49] John O'Donoghue and John Herbert. 2012. Data Management within mHealth Environments: Patient Sensors, Mobile Devices, and Databases. *J. Data and Information Quality* 4, 1, Article 5 (oct 2012), 20 pages. https://doi.org/10.1145/2378016.2378021

[50] Paul Pearce, Adrienne Porter Felt, Gabriel Nunez, and David Wagner. 2012. AdDroid: privilege separation for applications and advertisers in Android. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security* (Seoul, Korea) *(ASIACCS '12)*. Association for Computing Machinery, New York, NY, USA, 71–72. https://doi.org/10.1145/2414456.2414498

[51] Jan Pennekamp, Martin Henze, and Klaus Wehrle. 2017. A survey on the evolution of privacy enforcement on smartphones and the road ahead. *Pervasive and Mobile Computing* 42 (2017), 58–76.

[52] Sarah Prange, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In *Human-Computer Interaction–INTERACT 2021: 18th IFIP TC 13 International Conference* (Bari, Italy). Springer, Cham, switzerland, 339–360. https://doi.org/10.1007/978-3-030-85610-6_20

[53] Yiting Qu, Suguo Du, Shaofeng Li, Yan Meng, Le Zhang, and Haojin Zhu. 2020. Automatic permission optimization framework for privacy enhancement of mobile applications. *IEEE Internet of Things Journal* 8, 9 (2020), 7394–7406. https://doi.org/10.1109/JIOT.2020.3039472

[54] Ulf-Dietrich Reips and Frederik Funke. 2008. Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator. *Behavior research methods* 40, 3 (2008), 699–704. https://doi.org/10.3758/BRM.40.3.699

[55] Alireza Sahami Shirazi, Niels Henze, Tilman Dingler, Martin Pielot, Dominik Weber, and Albrecht Schmidt. 2014. Large-Scale Assessment of Mobile Notifications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 3055–3064. https://doi.org/10.1145/2556288.2557189

[56] Kanthashree Mysore Sathyendra, Shomir Wilson, Florian Schaub, Sebastian Zimmeck, and Norman Sadeh. 2017. Identifying the provision of choices in privacy policy text. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, Kerrville, TX, USA, 2774–2779. https://doi.org/10.18653/v1/D17-1294

[57] Albrecht Schmidt, Michael Beigl, and Hans Gellersen. 1999. There is more to context than location. *Computers & Graphics* 23, 6 (1999), 893–901. https://doi.org/10.1016/S0097-8493(99)00120-X

[58] Gian Luca Scoccia, Ivano Malavolta, Marco Autili, Amleto Di Salle, and Paola Inverardi. 2019. Enhancing trustability of android applications via user-centric flexible permissions. *IEEE Transactions on Software Engineering* 47, 10 (2019), 2032–2051. https://doi.org/10.1109/TSE.2019.2941936

[59] John S. Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering Resignation: There's an App for That. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 552, 18 pages. https://doi.org/10.1145/3411764.3445293

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

[61] Gulshan Shrivastava, Prabhat Kumar, Deepak Gupta, and Joel JPC Rodrigues. 2020. Privacy issues of android application permissions: A literature review. *Transactions on Emerging Telecommunications Technologies* 31, 12 (2020), e3773. https://doi.org/10.1002/ett.3773

[62] Christoph Stach and Bernhard Mitschang. 2013. Privacy management for mobile platforms–a review of concepts and approaches. In *2013 IEEE 14th International Conference on Mobile Data Management*, Vol. 1. IEEE, New York, NY, USA, 305–313. https://doi.org/10.1109/MDM.2013.45

[63] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. 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* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 168, 24 pages. https://doi.org/10.1145/3544548.3581060

[64] Christopher Thompson, Maritza Johnson, Serge Egelman, David Wagner, and Jennifer King. 2013. When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 1, 14 pages. https://doi.org/10.1145/2501604.2501605

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

[66] Na Wang, Bo Zhang, Bin Liu, and Hongxia Jin. 2015. Investigating Effects of Control and Ads Awareness on Android Users' Privacy Behaviors and Perceptions. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 373–382. https://doi.org/10.1145/2785830.2785845

[67] Yang Wang, Huichuan Xia, and Yun Huang. 2016. Examining American and Chinese Internet Users' Contextual Privacy Preferences of Behavioral Advertising. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 539–552. https://doi.org/10.1145/2818048.2819941

[68] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2018. Dynamically Regulating Mobile Application Permissions. *IEEE Security & Privacy* 16, 1 (2018), 64–71. https://doi.org/10.1109/MSP.2018.1331031

[69] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. 2018. Contextualizing Privacy Decisions for Better Prediction (and Protection). In

Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173842

[70] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 18 pages. https://doi.org/10.1145/3491102.3517688

[71] Jacob O. Wobbrock, Leah Findlater, Darren Gergle, and James J. Higgins. 2011. The Aligned Rank Transform for Nonparametric Factorial Analyses Using Only Anova Procedures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 143–146. https://doi.org/10.1145/1978942.1978963

[72] Kuang-Wen Wu, Shaio Yan Huang, David C Yen, and Irina Popova. 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior* 28, 3 (2012), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

[73] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and Vincent W Freeh. 2011. Taming information-stealing smartphone applications (on android). In *Trust and Trustworthy Computing: 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011. Proceedings 4*. Springer, Berlin, Heidelberg, Germany, 93–107.

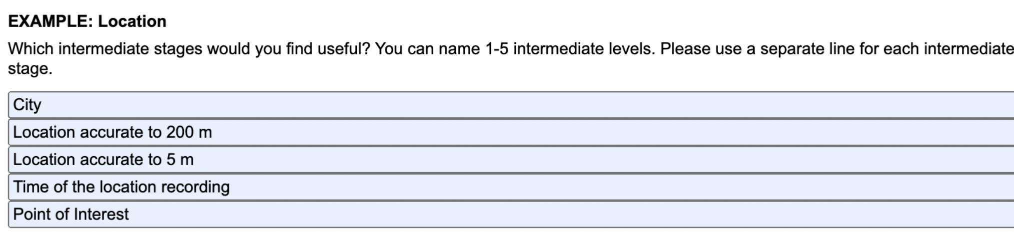
12 Appendix

12.1 Study I - Item Gathering Survey

12.1.1 Demographics.

(1) How old are you? (numeric text field)
(2) What gender are you? (radio button item)
   - Female
   - Male
   - Diverse
   - Not specified
(3) What is your highest educational qualification? (radio button choice)
   - School finished without graduation
   - Secondary school diploma
   - High school diploma
   - Completed apprenticeship
   - Bachelor's degree
   - Master's degree
   - Doctoral degree
(4) In which professional field do you currently work or will you work someday? (radio button)
   - IT, Electrical, Engineer
   - Economy, Logistics
   - Service, Sale
   - Social, Pedagogy
   - Art, Media
   - Health
   - Unemployed/looking for work
   - Other (*text field*)
(5) If you are a researcher, in which areas are you currently conducting research? (text field)
(6) If you are a researcher, in which research areas do you have particular expertise? (text field)
(7) Please rate how much you agree with the following statement. (slider items; strongly disagree - strongly agree)
   - I am an expert in Human Computer Interaction.
   - I am an expert in IT-Security.
   - I am an expert in Data Privacy.

12.1.2 Introduction. We want to give smartphone users more control over their data. With the current Android Permission Manager, you can only turn data tracking (e.g., the location) completely on or off. For many applications, e.g., a weather app, an exact location that allows a conclusion about your home address is not necessary. The information about the city would already be sufficient. Therefore, we would like to give users the possibility to control the data tracking more precisely with the help of a slider. We ask you to think about which intermediate slider levels there could be for each data item. Here you can see an example using the data item "location":


EXAMPLE: Location

Which intermediate stages would you find useful? You can name 1-5 intermediate levels. Please use a separate line for each intermediate stage.

City
Location accurate to 200 m
Location accurate to 5 m
Time of the location recording
Point of Interest

12.1.3 Intermediate Steps. For each of the datatypes listed below:

(1) Which intermediate stages would you find useful? You can name 1-5 intermediate levels. Please use a separate line for each intermediate stage. (text field with 5 separated lines)
(2) I would find it useful to control the accuracy of *DATATYPE* (continuous slider [0-100])
  - Text inputs – texts you type into text fields, e.g., text messages or search queries
  - Phone calls – contents of your phone calls
  - Activity – What you are currently doing (e.g., whether you are cycling, driving, ...)
  - App usage – All the apps you use
  - Using the camera – taking photos, selfies, ...
  - Notifications - (push) messages you receive from apps
  - Volume and brightness – sounds, music, day, night in your environment
  - Voice input – All voice input you give to your smartphone (e.g., Siri).
  - Screen contents – everything that is displayed on your smartphone screen.
  - Incoming text messages – Received messages, e.g., via WhatsApp
  - Besides accuracy, the frequency of data recording also plays a role. We explain this again with the weather app: While a complete motion profile can be created if the location is checked every minute, this is not possible if only one location query per day is allowed. For the purpose of a weather app, however, one location query per day is usually sufficient.
(3) Other comments: Do you have any further suggestions, ideas, comments or criticism? You are also welcome to note any comprehension problems here. (text field)

12.2 Study II - Concern Rating Survey

12.2.1 Demographics.

(1) How old are you? (numeric text field)
(2) What gender are you? (radio button item)
  - Female
  - Male
  - Diverse
  - Not specified

(3) What is your highest educational qualification? (radio button choice)
- School finished without graduation
- Secondary school diploma
- High school diploma
- Completed apprenticeship
- Bachelor's degree
- Master's degree
- Doctoral degree

(4) In which professional field do you currently work or will you work someday? (radio button)
- IT, Electrical, Engineer
- Economy, Logistics
- Service, Sale
- Social, Pedagogy
- Art, Media
- Health
- Unemployed/looking for work
- Other (*text field*)

(5) Which country are you currently living in? (text field)

(6) In a typical week, the devices that I use on a near daily basis are: (multiple choice)
- Mobile phone
- Tablet reader
- Tablet
- Laptop
- Desktop
- Non of these

(7) If you are a researcher, in which areas are you currently conducting research? (text field)

(8) If you are a researcher, in which research areas do you have particular expertise? (text field)

(9) Please rate how much you agree with the following statement. (slider items; strongly disagree - strongly agree)
- I am an expert in Human Computer Interaction.
- I am an expert in IT-Security.
- I am an expert in Data Privacy.

12.2.2 Introduction. How concerned are you about smartphone data tracking?

Nowadays, smartphones track a lot of their users' data, such as 'location'. With the following questionnaire, we would like to find out how much the tracking of certain data concerns you. We present you different intermediate levels for each type of data tracking (e.g. location data). Using a slider from 'strongly disagree' to 'strongly agree', you should indicate how concerned you would be if your smartphone tracked this type of data. Whereas 'strongly disagree' means that you would not be concerned at all and 'strongly agree' means that you would be very concerned if the smartphone tracked this data about you.

12.2.3 Concern Rating. We asked the following questions once for each datatype We would like to find out how much the tracking of certain data concerns you. We present you different intermediate levels for each type of data tracking (e.g. location data). Using a slider from 'strongly disagree' to 'strongly agree', you should indicate how concerned you would be if your smartphone tracked this type of data. Whereas 'strongly disagree' means that you would not be concerned at all and 'strongly agree' means that you would be very concerned if the smartphone tracked this data about you.

(1) Please rate the following statements, assuming your smartphone would track the following aspects of *[DATATYPE]*. I am very concerned with my smartphone tracking... (one continuous slider [strongly disagree - strongly agree] for each step that we found in Study I)
(2) Do you have any further feedback, comments or concerns?

12.3 Study III - Focus Group

12.3.1 Pre Questionnaire: Demographics.

(1) How old are you? (numeric text field)
(2) What gender are you? (radio button item)
  - Female
  - Male
  - Diverse
  - Not specified
(3) What is your highest educational qualification? (radio button choice)
  - School finished without graduation
  - Secondary school diploma
  - High school diploma
  - Completed apprenticeship
  - Bachelor's degree
  - Master's degree
  - Doctoral degree
(4) In which professional field do you currently work or will you work someday? (radio button)
  - IT, Electrical, Engineer
  - Economy, Logistics
  - Service, Sale
  - Social, Pedagogy
  - Art, Media
  - Health
  - Unemployed/looking for work
  - Other (*text field*)
(5) Which country are you currently living in? (text field)
(6) In a typical week, the devices that I use on a near daily basis are: (multiple choice)
  - Mobile phone
  - Tablet reader
  - Tablet
  - Laptop
  - Desktop
  - Non of these
(7) If you are a researcher, in which areas are you currently conducting research? (text field)
(8) If you are a researcher, in which research areas do you have particular expertise? (text field)
(9) Please rate how much you agree with the following statement. (slider items; strongly disagree - strongly agree)
  - I am an expert in Human Computer Interaction.
  - I am an expert in IT-Security.
  - I am an expert in Data Privacy.

12.3.2 Examples presented during the focus group.

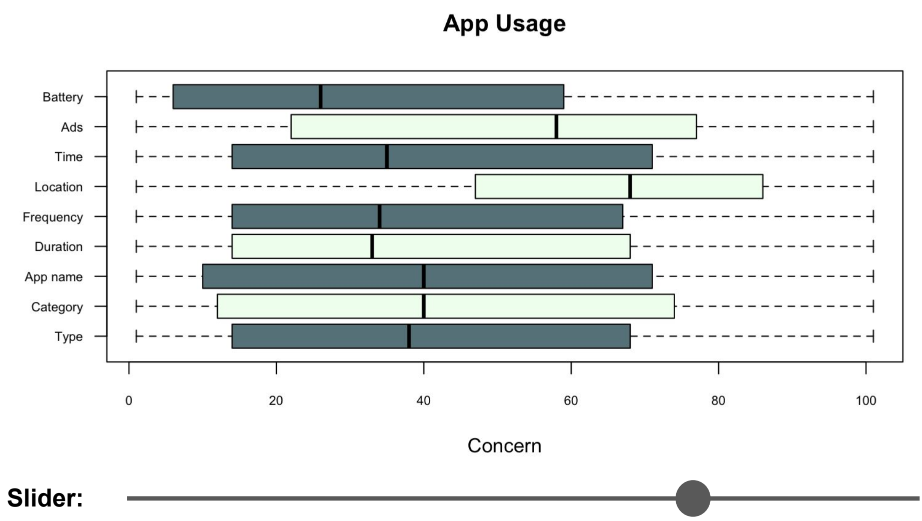


Fig. 9. Example visualizations used in Study III: a list of collected steps with their privacy concern rating as boxplots.

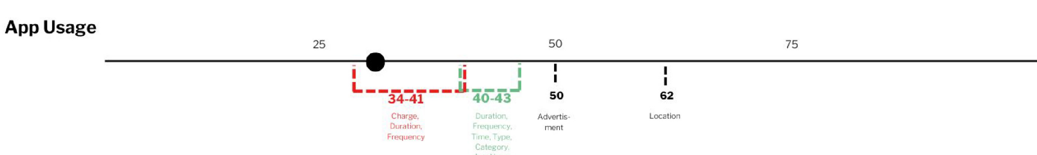


Fig. 10. Example visualizations used in Study III: a privacy slider draft with group steps.

12.4 Study IV

Study flow and randomization: There was one block of slider interface trials and one block of classic button interface trials. Their order was randomized. Within these two blocks, participants was first presented an isolated demo of the UI without a scenario; afterward, they were asked to click through 3 scenarios each (in order of these randomized). After each scenario and after each block, they had to fill out questions. Finally, participants had to use the system-level settings once in the classical condition and once in the slider condition (order randomized, same order as with the runtime permissions).

12.4.1 Pre Questionnaire.

(1) IUIPC: 10 items on 7 point Likert scale [strongly disagree - strongly agree]
(2) adapted items of Prange et al. based on Malhotra's causal model
(3) Affinity for Technology Interaction: 9 items on a 6 point Likert scale [completely disagree - completely agree, with in-between labels]
(4) Which smartphone (manufacturer + model) are you using as your private main device? (text field)
(5) I check the permission that are granted to apps on my smartphone in the device's privacy settings. (single choice)

- At least once a day
- At least once a week
- At least once a month
- At least once every 6 months
- At least once a year
- Never

(6) I spend time making good privacy decisions on my smartphone (continuous slider [strongly disagree - strongly agree])
(7) In which country do you currently reside? (single-choice dropdown)
(8) Which gender do you most identify with?
- Male
- Female
- Non binary
- Self-described *(text field)*

(9) How old are you? (numeric text input)
(10) What is the highest degree you have received? (single choice)
- Less than high school degree
- High school graduate
- Some college but no degree
- Bachelor's degree
- Master's degree
- Doctoral degree
- Vocational education

(11) What is your current primary occupation? (free text)

12.4.2 Questions after each runtime permission scenario. All items were continuous slider items from Strongly disagree to Strongly agree, unless specified otherwise.

(1) This method strongly protects the privacy of my data.
(2) This method allows me to control my data fully.
(3) This method clearly expresses how my data is used.
(4) This method lets me easily understand how my data is used.
(5) The options that this UI offers make sense to me
(6) The options given to me were sufficient
(7) Additional feedback? Please elaborate on your above decisions. (text field)

12.4.3 Questions after each runtime permission block. All items were continuous slider items from Strongly disagree to Strongly agree, unless specified otherwise.

(1) This method strongly protects the privacy of my data.
(2) This method securely protects my data.
(3) This method allows me to control my data fully.
(4) This method clearly expresses how my data is used.
(5) This method lets me easily understand how my data is used.
(6) I am familiar with this kind of interface
(7) *Sytem Usability Score: 10 items on 5 point Likert scale from Strongly disagree to Strongly agree*
(8) Do you miss any functionality regarding permission privacy configuration? (text field)
(9) Other feedback (text field)

12.4.4 Questions after each System Level Settings condition. All items were continuous slider items from Strongly disagree to Strongly agree, unless specified otherwise.

(1) This method strongly protects the privacy of my data.
(2) This method securely protects my data.
(3) This method allows me to control my data fully.
(4) This method clearly expresses how my data is used.
(5) This method lets me easily understand how my data is used.
(6) The options that this UI offers make sense to me
(7) The options given to me were sufficient
(8) I am familiar with this kind of interface
(9) *Sytem Usability Score: 10 items on 5 point Likert scale from Strongly disagree to Strongly agree*
(10) Do you miss any functionality regarding permission privacy configuration? (text field)
(11) Additional feedback? Please elaborate on your above decisions.

Received February 2024; revised May 2024; accepted June 2024