European Users' In-Depth Privacy Concerns with Smartphone Data Collection

FLORIAN BEMMANN, LMU Munich, Germany
MAXIMILIANE WINDL, LMU Munich, Germany
TOBIAS KNOBLOCH, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany and TU Dortmund University, Germany

Today's context-aware mobile phones allow developers to build intelligent and adaptive applications. The data demand induced by context awareness leads to decreased trust and increased privacy concerns. However, users' deeper reasons and real-world fears that underlie these concerns are not fully understood. We conducted an online survey (N=100) and semi-structured interviews (N=20) to understand users' concerns about smartphone data privacy. We investigated three key areas: general user understanding and misconceptions, specific in-depth concerns, and mitigation strategies. We found that effective transparency and control are the central themes across all areas. Users are concerned about privacy issues negatively impacting their lives, especially through financial loss, physical harm, or manipulation. We show that privacy measures should be implemented with a stronger focus on the user by keeping the user in the loop through transparency and control.

CCS Concepts: • **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → **Human computer interaction (HCI)**.

Additional Key Words and Phrases: human-computer interaction, privacy, concerns

ACM Reference Format:
Florian Bemmann, Maximiliane Windl, Tobias Knobloch, and Sven Mayer. 2025. European Users' In-Depth Privacy Concerns with Smartphone Data Collection. *Proc. ACM Hum.-Comput. Interact.* 9, 5, Article MHCI038 (September 2025), 32 pages. https://doi.org/10.1145/3743719

1 Introduction

Today, mobile apps create benefits for the user, such as displaying information only when needed [45] or deriving optimal navigation routes [3], by tracking various data types, e.g., mobile behavior [65], physiological data [62], or location data [67]. Especially for intelligent applications based on large language models (LLMs), mobile sensing data will be critical to providing apps with sufficient context awareness to help users effectively. However, the use of data increases users' privacy concerns, especially when the data leaves the user's device. Current research has already identified privacy concerns as the most important barrier to the proliferation of sensor-rich context-aware apps [43, 51]. Although this is a known issue, it has not been mitigated yet [9]. Understanding the underlying reasons for privacy concerns is thus crucial to solving this issue - they yet remain poorly understood today, cf. [11, 16, 30].

Authors' Contact Information: Florian Bemmann, LMU Munich, Munich, Germany, florian.bemmann@ifi.lmu.de; Maximiliane Windl, LMU Munich, Munich, Germany, maximiliane.windl@ifi.lmu.de; Tobias Knobloch, LMU Munich, Munich, Germany, tobias.knobloch@hotmail.com; Sven Mayer, LMU Munich, Munich, Germany and TU Dortmund University, Dortmund, Germany, info@sven-mayer.com.

ACM 2573-0142/2025/9-ARTMHCI038
https://doi.org/10.1145/3743719

Existing research studied barriers to the adoption of smartphone apps that use passive sensing (e.g., Chin et al. [17], Schessler et al. [66]) and mobile sensing research apps [43, 64], see Christin et al. [18] for an overview of technical privacy issues and measures. A plethora of papers propose technical concepts to reduce security issues (e.g., Bemmann and Buschek [8], Lin et al. [48]). Yet, making an app technically safe and privacy-friendly does not guarantee to ensure user acceptance - designers need to achieve actual user trust and lower privacy concerns to reach satisfactory adoption rates. To implement transparency and control, the two essential building blocks of user-centered privacy interfaces [10], we need to understand users' conceptions and assumptions of mobile sensing data procedures. Today, we argue that the specific underlying concerns [34, 63] are not well understood. Research often focuses on the what, who, and how, but only a few papers investigate *why* users are concerned. Insights on underlying reasons and fears are often a byproduct of studies (e.g., Frik et al. [34]) or in narrow domains (e.g., Maseeh et al. [53] who study marketing). Thus, the criteria of *specific* are not satisfied through existing research. Although the relevance of privacy issues has yet been sufficiently stressed, and directions for mitigation (e.g., transparency, control, human-centered privacy) have been proposed, the area still requires research attention as the issues from the user perspective still exist - researchers and developers have not managed sufficient mitigation in the wild yet. Users' perspectives on what would reduce privacy concerns are especially highly relevant but rarely regarded by research. Thus, understanding the real-world consequences users fear and the privacy violations they infer from data sensing is essential for designing effective privacy-friendly systems.

Our work explores smartphone users' privacy concerns in depth, focusing on their assumptions, feared real-world consequences, and mental models of how these aspects interconnect. With this, we extend existing work with our study through a deeper investigation than merely finding that privacy concerns are an important issue. Thus, we aim to extend the currently limited knowledge base with in-depth perspectives. We conducted a survey study ($N = 100$) investigating (a) users' knowledge of general smartphone data practices and privacy-enhancing technologies (PETs), (b) what users are concerned about, and (c) how their concerns can be mitigated. Through additional interviews ($N = 20$), we enrich the mainly quantitative results with a more qualitative-driven user perspective. Using a mixed methods approach, we investigate contextual factors influencing privacy concerns and analyze concrete user concerns. In detail, we show the underlying reasons causing the concerns, the specific privacy issue and feared consequences, the involved actors, the actions causing users' privacy concerns, the especially dangerous data types, and mitigation measures that, from the users' perspective, could solve the issues. We sampled participants across multiple European countries to collect European perspectives on users' smartphone privacy concerns.

As privacy in the context of mobile apps has been studied for years, the in-depth privacy concerns presented in this paper may not appear to be novel. However, our work extends previous studies on smartphone privacy perceptions (e.g., [19, 34, 53]) by providing in-depth user perspectives. This will help researchers understand why privacy developments are still not easy to proliferate. Therefore, our insights inform an important stage in the data pipeline of intelligent systems: We highlight real-world concerns and users' mental models regarding the privacy of their ubiquitous data. Considering these factors during system design is essential for fostering trust and acceptance in using user data to power LLMs and recommendation systems. After all - without accurate, contextual user data, even the smartest model will not generate relevant output.

2 Related Work

In the following, we will present past work on smartphone privacy research from the user perspective. We aim to understand what users are concerned about when using their smartphones.

2.1 Concern Mental Models

We need to consider the users' mental models to understand how they perceive the inner workings of technical systems and which assumptions are present. Coopamootoo and Groß [20] compile definitions of mental models from privacy-independent research of Johnson-Laird [41] and Craik [22] as "internalized, mental representations of a device or idea that facilitates reasoning. They [mental models] are simplistic and small-scale representations of reality." The model of *Privacy As Expectations* [47] explains privacy issues as a mismatch between expectations and reality. Thus, privacy concerns arise if what the system does deviates from the user's mental model. From a *Cognitive Behavioral Theory* perspective, informing one's behavior starts from a privacy attitude learned and developed throughout life [2, 20]. Moreover, Wash [77] compiled a set of mental folk models on security threats. While these models that explain users' underlying imagination of how a system works can become quite complex, privacy decision-making mainly happens through a rather simple cost-benefit tradeoff. Here, the *Privacy Calculus* states that users outweigh anticipated risks and potential benefits when deciding for or against disclosing personal data [23]. Thus, users mostly accept the cost of data being collected if they want to use a service (cf. Price of Convenience) [42].

Colnago et al. [19] defined privacy concern as "an expression of worry towards a specific privacy-related situation." Thus, privacy concerns have two underlying components: (1) users' predisposition, which is a result of past experiences and learned values and standards, and (2) situations. These two aspects are processed through the user's mental model of how a system is working (c.f. *Privacy as Expectation* [47]), possibly leading to feared consequences that might happen (= *privacy concerns*). To decide on a consequence, e.g., refusing to provide data to an app, users apply the Privacy Calculus, outweighing situational perceived risk and potential benefits.

2.2 Privacy in Mobile Sensing Smartphone Apps

Research on privacy in mobile sensing apps finds that existing privacy-enhancing systems lack clarifications about implications for privacy (e.g., [13]), and users behave inconsistently with their concerns [18]. At the same time, privacy surveys face a high risk of biasing responses with their methodology [20], as users are often unaware of their privacy concerns before becoming aware of possible consequences [36]. Thus, Braunstein et al. [15] developed a solution to indirectly ask about privacy concerns to reduce emotional reactions and biased responses. Importantly, Wang et al. [76] introduced a threat model and a taxonomy for privacy issues to bring structure to the space of potential attacks. They distinguish between *task privacy*, *identity privacy*, *attribute privacy*, and *data privacy* to propose privacy protection schemes for each privacy issue.

Today, many implementations exist to address privacy concerns, e.g., differential privacy [26, 49], on-device preprocessing [8, 26, 83], early data aggregation [46], and anonymous assessment [18]. At the same time, related work concludes that privacy is the most important barrier to app adoption [11, 16, 30]. Studies on adoption rates and reasons against the usage of (context-aware) mobile sensing apps identified a wide range of privacy concerns: General privacy and data security [16, 43, 51, 64], poor personalization [16], lack of usefulness/trust in provided information [16], and general trust [64]. More than half of smartphone users do not want to install an app when they discover how much personal data is collected [12, 84], and about a third uninstall applications when learning about collected information [12].

2.3 Understanding Concerns: User's Disposition + Mental Model

The smart homes privacy literature [85], distinguishes between *assets*, *adversaries*, *vulnerabilities*, and *threats*. Following this approach, we compile an overview of how the disposition, situation, and mitigation behavior of the users relate to each other in Figure 1. Insights on how such factors affect

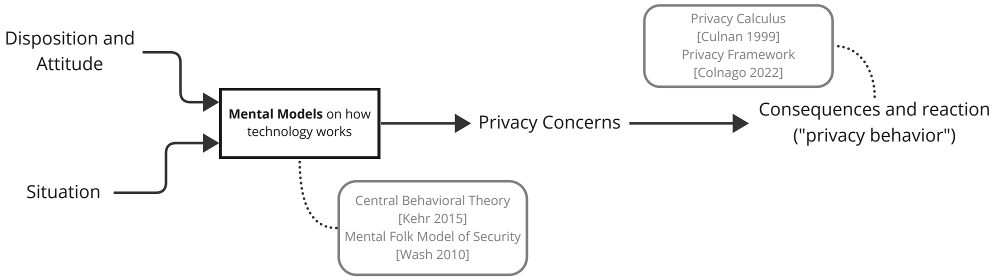

Disposition and Attitude
Situation
Mental Models on how technology works
Privacy Concerns
Consequences and reaction ("privacy behavior")
Privacy Calculus [Culnan 1999]
Privacy Framework [Colnago 2022]
Central Behavioral Theory [Kehr 2015]
Mental Folk Model of Security [Wash 2010]

Fig. 1. A model compiled from related work that visualizes how various constructs in the privacy domain interplay. Privacy concerns are based on users' disposition and situation, depending on how a user assumes that a system is working. Thereon, users decide on consequences, i.e., mitigation behaviors, as described by decision theories such as the privacy calculus theory.

users' privacy perception have yet been researched by existing work, e.g., [9, 24, 28]. While this research is valuable in tackling the cause (e.g., removing sensitively perceived datatypes), research still lacks in-depth insights into what users are actually afraid of happening in the real world. This is where we continue with our paper to gain a better understanding of user concerns and show the potential to lower these concerns.

Assets: *Differences Between Datatypes.* Literature reveals that users are most concerned about login credentials [17, 34, 35, 63], which might lead to financial loss or identity theft. It is followed by contextual data, especially text messages [35] and address book/contact information [31]. Next comes personal high-level behavioral data like GPS [34, 35, 44]. Behavioral sensor data like accelerometers were judged less concerning [44], likely due to the missing direct relation to personal high-level behaviors.

Adversaries: *Differences Between Whom One is Sharing With.* Giving (un)authorized access to personal data is the largest factor in sharing decisions and an essential aspect of privacy concerns [29, 31]. Data sharing can be categorized into *second-party* (sharing with the device or OS developing company [42]) or *third-party* (advertising companies or data brokers) data sharing. Users' attitudes and opinions towards third parties have been extensively studied [42]. Yet, it is unclear whether third- or second-party sharing is more concerning, cf. [34, 40, 70]. Finally, generally aware users lack awareness of the actual sharing scope (frequency, target, apps) [6], which also depends on the surveyed population [1].

Threats: *Underlying Events.* Users are generally unaware of which real-world implications they are afraid of and, as such, can not specify the purpose and reasons [34]. Among the few concrete reasons, financial and physical loss is most prominent [34, 35], followed by concerns about location data, which can lead to fears of physical threats [44]. However, users are more precise regarding specific domains and situations. For instance, the fear of being disproportionately subjected to security checks [1], the fear of sharing behavioral data in the workplace [30], and the fear of financial loss and destruction of personal reputation [60]. Users become especially concerned when they lose awareness and control of what happens to their data [70].

Vulnerabilities: *Underlying Reasons.* Unauthorized remote access, like hacking, malware, data breaches, or compromised passwords, is mentioned frequently [34, 85]. Wifi and mobile networks are also often perceived as unsafe [17, 85]. Companies deliberately transmitting/selling data to others is also a frequently mentioned issue [1, 34, 40, 70]. Some people also fear the physical loss of their device, fearing that someone finding it could access their data [17].

2.4 Privacy Behaviors: The User Perspective on How to Mitigate Privacy Issues

The first group of privacy behaviors we found in the literature is about *improving a device's actual security*. Within the limited room for measures from a user perspective, studies primarily report actions on authentication management [34]. Such measures include using strong passwords, 2FA, and password managers [35]. Further security strategies include clearing history data where possible [84, 85] and using security software [34]. As the second step of privacy behaviors, when users still do not have sufficient trust in a technology's security, literature distinguishes between measures that aim to *avoid behaviors* and *control data collection*. In the first case, users apply behavioral changes, leading to less data being provided to a device [34]. For example, making voice calls only in specific environments [29] or avoiding certain things in rooms with a smart home device [85]. In the online context, measures include avoiding behaviors by not doing certain tasks via mobile devices, such as opening attachments [34].

3 Research Gap

As discussed in Section 2, prior work provides several markers for user concerns; however, when investigating the specific issues, we found only very limited insights and explanations for the specific user concerns in related work. With *specific* issues, we refer to incidents in people's lives that directly impact the physical, social, or societal sphere. For instance, prior studies directly asked users about privacy concerns, in which they reported a diverse set of privacy and security issues and only a few specific, underlying concerns [34, 63]. Findings on user concerns exist in specific domains, such as Maseeh et al. [53], which focused on app marketing; however, they lack a broader HCI perspective and depth. Thus, they do not regard interface and interaction aspects as missing the user perspective on mitigation opportunities. Moreover, insights on underlying reasons and fears are often rather a byproduct of studies and can be imprecise and superficial [34]. Finally, following the definition *privacy concern* as *"an expression of worry towards a specific privacy-related situation"* [19]. We did not find sufficient insights in related work into the *specific* situations that raised users' privacy concerns. From a system design perspective, the end-users' concerns and expectations are not sufficiently considered in the design process of privacy characteristics and features in systems [5]. To accomplish privacy by design, designers and developers need to take a more user-centered approach by putting a stronger emphasis on users' views and feedback, which requires understanding the *specific* concerns. With this, they will overcome trust and adoption issues. Therefore, it is important to go beyond the vague and broad construct of privacy to make concerns more graspable and actionable.

With this work, we aim to understand the *specific* in-depth user concerns, the underlying reasons, and the user perspectives. With this, we first raise awareness for the *specific* privacy concerns which will lead a better foundation for the development of future privacy-enhancing measures in smartphones; and thus, to fewer privacy concerns and to higher app adoption of context-aware mobile-sensing apps. To achieve this, we have set out the following three research questions.

RQ1*: What is people's level of knowledge regarding privacy and security practices of the data collected through their smartphones?* In the context of apps, it is known that users weigh perceived risks against benefits when deciding for or against the installation [82]. Thus, to make an informed decision, users have to be knowledgeable. Moreover, from research on privacy policies in the context of online services, it is known that users barely read them [55, 59]. However, without understanding how an app and its privacy protection measures work, it is difficult for users to reach a low level of concern.

RQ2*: What are people's detailed privacy concerns and feared real-world consequences of smartphone privacy issues?* While RQ1 will give an understanding of users' preconceptions, we lack crucial insights about the actual concerns. So far, researchers have only investigated other domains, such as IoT [63], online advertisements [71], or smart homes [80]. Therefore, we investigate the users' privacy concerns about mobile sensing apps in depth.

RQ3*: What are solutions to mitigate privacy concerns from the users' perspective?* To complement the insights on concerns and their influencing factors, we investigate the user's perspective on how their concerns could be mitigated.

Methodology. To address these RQs, we conduct two user studies. In the first survey, we collected a broad perspective on various privacy aspects by asking a large sample across multiple countries about different smartphone app scenarios. Afterward, we build on this and get more specific through in-depth, semi-structured interviews.

4 Study I: Online Survey

We first conducted a large-scale online survey to gain quantitative insights into our research questions. The questionnaire consisted of three phases: 1) demographics and knowledge, 2) understanding users' concerns in general, and 3) specific concerns and envisioned mitigation measures. We provide the questionnaire in the Supplementary Material.

4.1 Survey Design

We presented all statement questions with a slider ranging from *Strongly disagree* to *Strongly agree* on a continuous (technically 100-point) scale without ticks and default selection, cf. [54]. To ensure high data quality, we included attention checks as a slider item, which had to be moved to the very left or right at the end of each phase.

Phase 1: Demographics and Knowledge. This phase consists of six blocks: 1) demographics, 2) participants' general privacy perception (IUIPC questionnaire [52]), 3) technology affinity (ATI scale [33]), and 4) a set of self-constructed free text items on which smartphones the participants own and which mobile sensing apps they are familiar with. Here, we also introduced a definition of mobile sensing apps. Afterward, we had 5) a self-constructed set of items on the knowledge and understanding of 4 privacy-enhancing measures occurring in mobile sensing systems (encryption, anonymous data collection, hashing, remote server). This knowledge assessment method was adopted from Smit et al. [71] and Bemmann et al. [10]. For each concept, the participants had to indicate for three statements whether they were true or false (randomized order). The last item in this first phase is 6) one self-constructed item about how much users familiarize themselves with the privacy implications before installing an app.

Phase 2: Understanding Users' Concerns. In the second phase, we openly asked about the users' concerns. To avoid biasing the participants, we deliberately asked open questions before letting them rate items that tackled specific aspects. The open questions asked the participant to name one specific concern, define what exactly they are afraid of happening, which situations, data types, and involved actors they considered particularly concerning, and how they envisioned their concerns to be mitigated. This structure was derived from previous work on privacy (e.g., [85], refer to Section 2.3 for details), which structures privacy aspects into assets (here: datatypes), adversaries (here: actors), vulnerabilities, and threats (here: situations). We wanted to ensure that participants think about all of these aspects, as well as mitigation measures, and therefore ask for them individually. This phase was implemented as an optional loop so that participants could potentially express multiple concerns.

Phase 3: Specific Concerns. Afterward, we presented four mobile sensing app use case scenarios in a randomized order, namely *Ambient Noise App*, *Navigation App*, *Sports and Fitness App*, and *Travel Advice App* (see Supplementary Material for a scenario description). For each scenario, we asked questions on the general concern, familiarity, perceived usefulness, and envisioned concern mitigation options. Subsequently, the survey again went through the scenarios in a randomized order and let the participants answer some quantitative items and some open-ended free-text items. We asked for concerns about the presented scenarios, compiled of threats and privacy issues from Windl and Mayer [80], Barbosa et al. [7], and Wang et al. [76], such as third-party data access or profile building. This concept of presenting scenarios and asking participants open-ended questions about them was adapted from Psychoula et al. [63], who successfully applied it to privacy research in the IoT context. Scenarios are presented through a short description text, and do not require participants to install anything. We did not mention existing app names in order not to bias participants through potential previous experiences or prejudices. We selected four smartphone app use cases that rely on smartphone sensing data. All scenarios share data with remote servers, give users some direct benefit, and are presented neutrally regarding companies and organizations. In line with recommendations for scale development, we phrased the statements involving quantitative rating strongly, as mildly phrased statements have shown to result in too much agreement [27]. We deliberately do not compare the results of the different scenarios, as the scenarios each impose various hard-to-control variables (e.g., people's prior experience with a use case and perceived personal benefit, see Bemmann and Mayer [9]).

4.2 Pilot Testing

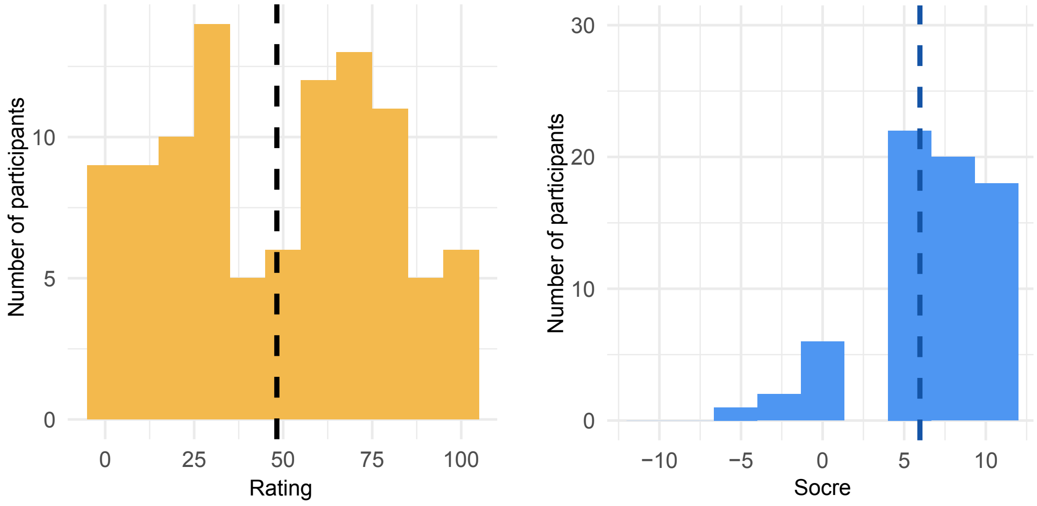
We piloted the study with 20 participants, including a full qualitative data analysis. We ensured that all questions were understandable, the questionnaire was working well technically, and that we received the desired kind of responses. After analyzing those 20 pilot responses, we made significant changes, especially to the open questions of the second phase. Moreover, we tested and discussed the design of the self-constructed set of items on knowledge and understanding of privacy-enhancing technologies with three researchers from our lab who were not involved in the project.

4.3 Procedure

We asked participants to fill out our questionnaire using Qualtrics. We balanced the participant pool by gender, age, country of residence, and occupation, and required participants to live in Europe and speak English fluently. We rewarded participation with 3.34£ as the study took approximately 25 minutes. The study was carefully designed in line with our federal and university's data protection regulations, and approved by the local ethics committee (reference number EK-MIS-2023-150).

4.4 Participants

We recruited 100 participants (48 female, 51 male, and 1 non-binary) aged 19 to 72 ($M = 31.5$, $SD = 9.2$) through Prolific. Most participants were either full-time (49) or part-time employed (14). A third (31) were students, and half held a university degree (34 master's degrees and 27 bachelor's degrees). Most participants lived in Poland (17), France (11), Portugal (8), and Hungary (8); including participants from 13 European countries. On the affinity for technology interaction scale (ATI) [33] (scale ranges from 1 least to 6 highest possible affinity), our sample had an average score of around



(a) Personal engagement with privacy information

(b) Knowledge about privacy-enhancing technologies

Fig. 2. Distribution for our two measures of engagement with privacy information (a) and knowledge about privacy-enhancing technologies (b). The dashed lines represent the means of each measure.

4 (M = 3.87, SD = 0.97). This indicates a tendency towards a slightly higher technology-affine sample than the average population, according to the classification of Franke et al. [33].

4.5 Data Analysis

We preprocessed the questionnaire data with Python and imported the free text answers into ATLAS.ti for coding. Two researchers independently coded the first 20 participants. We then discussed the coding and revised these participants' codings before one researcher coded the remaining participants. With all participants coded, three authors met in person to discuss the codes and form initial themes. We iteratively reworked the codes and themes in multiple sessions by comparing the coded snippets across all themes. The final coding consists of 765 distinct codes organized into 42 code groups. Each code expresses a specific aspect (e.g., *take out a loan*), while code groups categorize them to a broader level (e.g., *financial loss*). The code groups *Underlying Cause: The User* and *Consequences: Emotional Damage* were initially not found in the survey data analysis but later discovered during the interview coding (see Section 5.2). We, therefore, recoded the survey data with respect to these new code groups after the interview study.

4.6 Results

In this section, we present our results along with our research questions. We start with general concerns and influencing factors before we describe the detailed types of concerns expressed by participants. We show how concerning our participants rated several aspects of sensing applications and how they imagined their concerns could be mitigated.

4.6.1 User Knowledge (RQ1). In our quiz, for items that assessed how knowledgeable and informed users are about technology, privacy, and security in the smartphone context, participants mostly reached 6 points (M = 5.62, SD = 3.34; scale [-12;12], the expected random response is 0). The score distribution is skewed towards the right and not normally distributed; see Figure 2b.

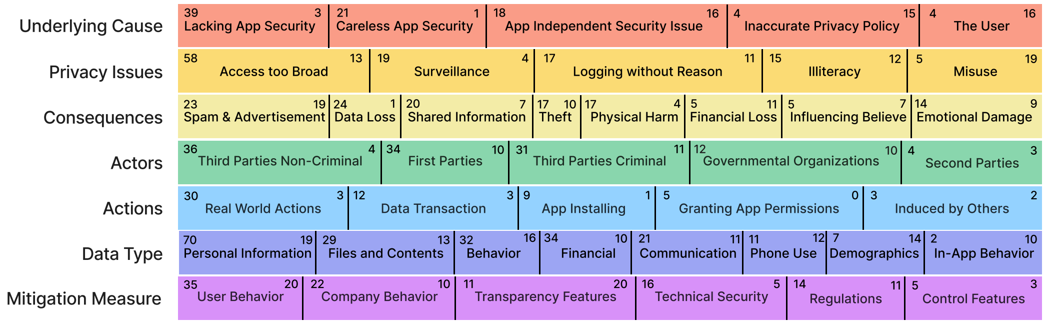


Fig. 3. Our code groups that underlay the seven themes of our privacy concern model. Numbers in the upper left corner of each code indicate the number of *online survey* participants expressing the code, the number in the top right corner indicates the number of mentions in the *interviews*.

We also asked participants how much they familiarized themselves with the data practices before installing new apps. On a continuous scale between 0 and 100, the average answer is in the middle ($M = 48.22, SD = 30.73$). Taking a look at the distribution (cf. Figure 2a), we found a gap in the middle, i.e., very few participants replied with values around 40. Additionally, we found two peaks, one at around 30 and one at around 70. Thus, we identified two types of users: Those who care very little and those who care rather much about the data handling practices of an app.

4.6.2 Privacy Concerns in the Sensing Data Pipeline (RQ2). We found that *data misuse* ($M = 72.68$), *3rd party data access* ($M = 71.79$) and *data getting stolen* ($M = 69.45$) were the most concerning aspects. *3rd party data access* was rated significantly more concerning than *2nd party data access* and *1st party data access* using Kruskal-Wallis rank sum test and Dunn's Test [61]; see Figure 4 and Table 1. Furthermore, we found significantly lower concerns for *local data processing* and *local data storing* in comparison to their global alternatives.

4.6.3 Qualitative Analysis: Users' Privacy Concerns Regarding Smartphone Data (RQ2). Our thematic analysis revealed seven overarching themes that describe the scenarios evoking privacy concerns. Figure 3 gives an overview of how the discovered aspects are reflected in code groups, while Figure 5 explains how the themes connect: An UNDERLYING CAUSE (for example, a weakly secured server) triggers a PRIVACY ISSUE (for example, data being stolen from that server by hackers). Privacy issues provoke a (REAL WORLD) CONSEQUENCE (for example, the stolen data being leveraged to withdraw money from an online banking account). A PRIVACY ISSUE is caused by ACTIONS, involves

Table 1. The two-way F-statistics of users' privacy concerns regarding different types of threats. P-values of Dunn's test are Bonferroni adjusted.

	KRUSKAL WALLIS			DUNN'S TEST	
	chi-squared	*df*	*p*	*Z*	*p*
1st party data access vs. 2nd party data access				−1.471	1.
1st party data access vs. 3rd party data access				−4.794	<.001
2nd party data access vs. 3rd party data access	228.36	12	<.001	−3.323	.070
Global Data Storing - Local Data Storing				6.667	<.001
Global Data Processing - Local Data Processing				6.736	<.001

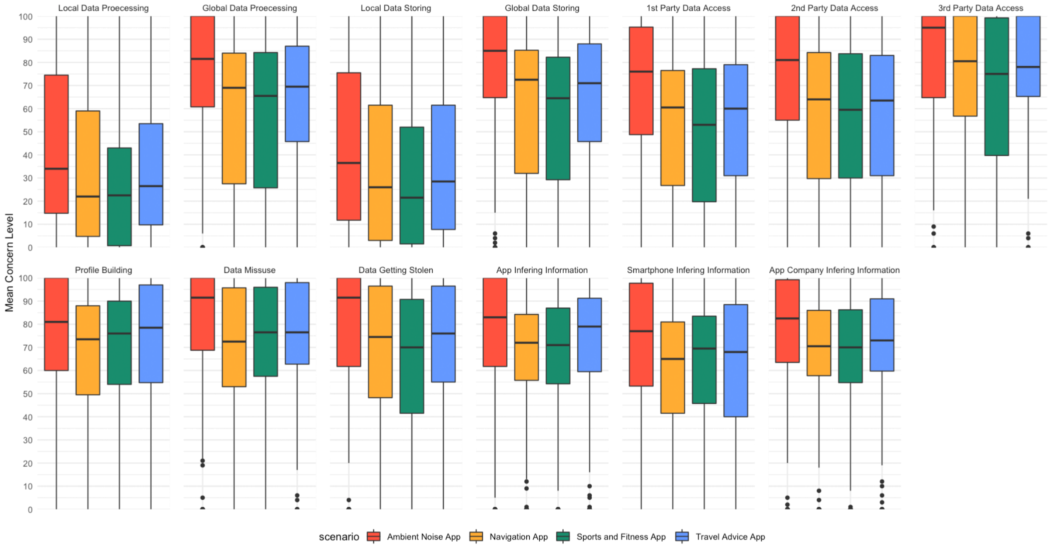


Fig. 4. The rated concern level of specific privacy-threatening aspects of mobile sensing apps regarding four mobile sensing app usage scenarios.

Actors (e.g., hackers, companies), and affects specific Data Types. Mitigation Measures can be employed to tackle a Privacy Issue. Figure 3 shows an overview of all themes and their affiliated code groups. In the following, we describe the themes in more detail.

Underlying Cause. Most (82) users see the fault for privacy issues in the app companies. Of these, most (49) users believed security issues occurred without companies' malicious intent but due to *Lacking App Security*. Users described scenarios, such as data leaks, security breaches, or hacker attacks. However, several (28) users also believed that privacy issues are caused by companies not employing sufficient measures (*Careless App Security*), as P63 stated: *"I am concerned about lack of proper care from a company."* Moreover, several participants (19) also mentioned app-independent security issues, such as *"viruses and spyware"* (P89). Finally, five participants also mentioned *Inaccurate Privacy Policies* as a trigger for privacy concerns, as P35 explained: *"[I am] concerned that sometimes terms of privacy don't tell everything about the use of my data. That maybe they are lying about [...] what happens to my data."*

Privacy Issues. Most (80) participants were concerned about too many people having access to their data. Precisely, data theft (28) and their data being sold (24) were mentioned. For example, P1 is concerned that *"the company that had my data could have sold it, or another way would be that they were hacked and the database was compromised."* Data theft and trade are followed by the feeling of being surveilled (23), for example, by tracking their location. Logging data without reason was also frequently mentioned (20), which included the collection of personal histories, constantly logging in the background, or accessing data sources that the user did not authorize. Participants also mentioned concerns caused by not knowing what an app is doing (18), such as using or sharing data without their knowledge. Data misuse by the company, e.g., for profit, was mentioned least often.

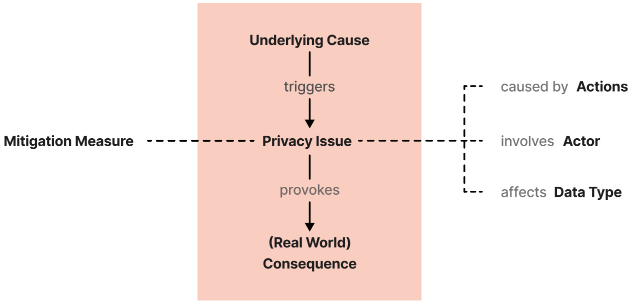


Fig. 5. Our privacy concern model. Privacy issues are at the center, triggered by causes and leading to consequences.

Consequences. Most (28) participants feared not necessarily harmful but annoying consequences, such as personalized advertisements or being manipulated regarding their shopping behavior. Participants also frequently (25) mentioned consequences that represent a loss of control, for example, that big datasets about them could be gathered or that their identity is stolen and misused, leading to further consequences such as *"[..] the possibility of identity theft"* (P7). Moreover, several (21) participants feared that their data might become publicly available, or even directly affect participants' lives beyond the online world through theft (19), or even physical harm (18), such as stalking. A different aspect of consequences with real-life impact is financial loss (6), as P66 describes *"[...] my financial data. Let's say I did not pay one month of my mortgage. This info can then be spread all over the globe, and I will not be able to get a loan from a bank [...]."* Lastly, manipulation was also mentioned by a few (5) participants.

Actors. Participants most frequently (46) mentioned third parties without criminal intent, such as advertising companies, when asked who triggered their privacy concerns. The second most frequently (38) mentioned actor was the first party, i.e., the app company. Interestingly, 35 participants fear that third parties with criminal intent, such as hackers, pose a danger to their privacy. Our participants also named government organizations (15) and secondary parties (4), such as phone manufacturers, as actors evoking privacy concerns.

Actions. Participants mentioned most frequently (42) that actions "in the real world" trigger their concerns, especially the use of public WiFi networks. Users also expressed concerns during data transactions (14), i.e., while documenting, viewing, or working with data. When interacting with an app, most users (10) were more concerned when installing an app (10) than when being asked to grant permissions (6). Lastly, participants were also concerned about other people causing a privacy issue for them (4).

Data Types. The most frequently mentioned data type was personal information (131), such as login details, phone numbers, or home addresses, followed by files and content (37), such as photos. Moreover, participants often named behavioral data (36), such as location and habits, and financial data (34). Finally, participants mentioned communication protocols (27) (e.g., WhatsApp messages), phone use (13) (e.g., screen time), demographics (8) (e.g., age and gender), and in-app behavior (3) (e.g., the time they spent in an app) least frequently.

4.6.4 Solutions to Mitigate Privacy Concerns (RQ3). Interestingly, the most mentioned measures to reduce their concerns were changes in their own behavior (mentioned by 45 participants). Most ideas are related to using an app less or not at all, blocking permissions, or only choosing trusted companies. Behavior changes by the app company were mentioned second most frequently (25). Most suggestions were related to data minimization: Apps and companies should ask for and use less data (e.g., *"companies not requiring as much data and not tracking online activity,"* P33), and store data only for the necessary amount of time. Next, we recognized a desire for more transparency features (18) (better understandable privacy policy, more clearly stating what, when, and how data is used) and the wish to have more control over what happens with their data. For example, P35 expressed the desire to learn *"how the app works and collects [their] data."* Suggestions for technical security (18) included safer storage and transmission of data, e.g., by encryption or processing and storing data locally. Regulatory measures are often mentioned (16). Here, participants desired more laws for data safety, global standards, and institutions that enforce the rules. Least frequently (6) were statements that we categorized as control features, e.g., the ability to turn off data access.

4.7 Summary

Our survey shows that users generally know about privacy-enhancing technologies (RQ1). However, we found that they are ambivalent about informing themselves about the privacy aspects of new apps and denounce that they are not well informed. The online survey's qualitative part revealed themes around the topic of smartphone privacy and gave us an impression of which aspects are relevant to users (RQ2). Quantitative questions confirm that third-party data theft and misuse concern users the most. Furthermore, the quantitative questions revealed high concerns, especially for passively sensed data on contextual variables. However, due to the nature of an online survey, it is hardly possible to get a detailed understanding of users' concerns and possible mitigation measures. Therefore, we decided to supplement these insights with interviews to gain a more in-depth understanding. This will especially help answer RQ2 (in-depth concerns of the users) and RQ3 (mitigation measures).

5 Study II: Interviews

We conducted an interview study to get a more in-depth understanding of the patterns that participants came up with in our online survey. In semi-structured interviews, we dig deeper into the users' concerns and possible mitigation measures. Furthermore, we want to confirm our privacy concern model (cf. Figure 5) with a second participant sample.

5.1 Procedure

We decided to conduct semi-structured interviews with a guideline (see Supplementary Material) whereby the order of the questions does not have to be strictly followed, and the interviewer can ask follow-up questions whenever appropriate [38]. The guideline contained three key topics: Users' knowledge Level, users' concerns and fears, and mitigating factors, including knowledge of protective measures. Each section had three to five questions, and we also added possible follow-up questions. We designed the questions open-ended [78], and we explicitly noted that the questions did not suggest particular answers so that each participant could reflect on their knowledge or opinions without biases. When developing the guideline, we first formed the topic areas before we formulated the concrete questions: (1) the participants' current knowledge regarding smartphone privacy and apps' data practices, (2) their concerns and fears, and (3) factors that mitigate concerns and knowledge on protection measures. In the next step, we critically reviewed these questions and reformulated them whenever necessary. Thus, the questionnaire creation was roughly based on Helfferich [37]. We focused on not suggesting answers through the question design.

At the beginning of the interview, participants had to fill out an online questionnaire to assess their demographics, affinity for technology interaction (ATI) [33], and their individual information privacy concern level using the IUIPC questionnaire [52] and three items adapted by Prange et al. [62] based on Malhotra's causal model [52]. In addition, we formulated three statements on concerns about smartphone data collection and disclosure (i.e., general concern about smartphone data collection and second and third-party sharing), where participants had to indicate their level of agreement on a continuous 100-point slider, ranging from "strongly disagree" to "strongly agree." We recorded the interviews and compensated the participants with 5€. The study was carefully designed in line with our federal and university's data protection regulations, and approved by the local ethics committee (reference number EK-MIS-2023-219).

5.2 Data Analysis

Each interview took, on average, 22 minutes and 33 seconds ($SD = 9m20s$), resulting in 7.5 hours of audio material. The interviews were transcribed using the transcription software Trint,. Afterward, we proofread all transcriptions and corrected any errors. We analyzed the interviews using ATLAS.ti and thematic analysis [14], meaning that three researchers first independently open-coded two interviews. We then met to discuss our codes, resolve ambiguities, and form a joint codebook. One researcher then coded the rest of the interviews, after which a fourth researcher joined to form code groups and overarching themes through multiple rounds of hour-long discussions.

5.3 Participants

We recruited 20 participants, half through the university's mailing list and half via convenience sampling. Through this, we hoped to recruit a more diverse sample, including different professions and age groups. The participants from the interview study are, on average, older than our first sample from the online survey, i.e., closer to a societal average ($M = 39$, $SD = 20$, $min = 18$, $max = 82$). Nine participants were full-time employed, eight were students, two were retired, and one was currently undergoing training. Their affinity for technology interaction is slightly below average ($M = 3.55$, $SD = 1.04$, cf. the classification of Franke et al. [33]). Regarding the questions on perceived information privacy, our participants rated their Awareness on average with 6.17 ($SD = .95$), Control with 5.32 ($SD = 1.15$), and Collection with 5.38 ($SD = 1.15$) (higher scores correspond to higher privacy). Participants indicated medium general concern about their smartphone collecting their information ($M = 63.60$, $SD = 27.45$), a little higher concerns about data being shared with second parties (i.e., the device manufacturer or operating system developers) ($M = 70.0$, $SD = 20.81$), and rather high concerns on data being shared with third parties ($M = 80.95$, $SD = 20.15$).

5.4 Results

We mapped the interview citations to our privacy concern model codes developed based on the survey results (cf. Figure 5). The interview data fits well with our model, and we could rediscover all the codes. Additionally, we added the new code *The User* to the code group *Underlying Cause*, and *Circumstances* to *Mitigation Measures. The User* entails statements of users seeing themselves as the cause of privacy issues, a pattern we did not find in the online survey. *Circumstances* include mitigating factors that are passive factors instead of actively performed measures.

5.4.1 Underlying Causes (RQ1). Regarding the underlying causes of their privacy concerns and present privacy issues, interview participants mainly mentioned topics that affect the current privacy information mechanisms (code group *Inaccurate Privacy Policy*) and issues that they see among themselves (code group *The User*).

Inaccurate Privacy policies. Users mention that they would like to know more about what happens with their data, but the given information mechanisms make it hard for them. Our participants especially criticized that privacy policies are too long and hardly understandable. Moreover, P13 explained that they *"tried to read privacy statements, but it's a lot of text."* Even when users overcome the issue of time, they are not satisfied, as P18 describes in their experience: *"Sometimes, I also read the explanation, but all the conditions are unclear."* P10 even accuses companies of deliberately hiding details, saying *"that is of course somewhere already intentional that you make it so complicated [...]"*. P9 formulates precisely what they would prefer, namely *"not such a mega long text, but one that is so probably presented in bullet points or so"*, aiming for knowledge about *"how this data is processed and whether it is passed on to third parties."* Many participants admit that they usually do not really read but blindly accept privacy policies.

The User. Our participants saw the most common causes of privacy issues among themselves. Due to the current weak informed consent mechanisms, participants expressed unknowingness 22 times. In 19 quotes, they describe that for them, *comfort outweighs concerns*, resulting in the user being the cause of privacy issues. Eleven quotes even indicate that users reached *resignation* on the topic of privacy. They lack a general feeling and understanding of what happens with their data behind the scenes: *"These Internet giants, which I can't assess at all, and which are like a black hole for me, and where I don't know at all what they are doing with it and what they are capable of when it really matters"* (P5). Besides what happens with their data, participants *"do not know how many years that the data will be stored"* (P9), and wonder *"to what extent that then saves in the long term"* (P3). What kind of data gets logged and processed by default, and to what users agree simply by purchasing a device, are also unclear. Furthermore, the reasons for data usage are often unclear, meaning that data logging often lacks a justification, as P9 explains: *"I can not understand that [why location is requested] and I have no idea why the location is then requested and therefore I click on deny because I have no idea"* (P9). Our interviews indicate that this lack of justification leads to both concerns and an increased tendency to deny data access. In general, we found a perceived lack of control. P19, for example, states that *"I don't think we have any influence at all, because we don't know what's in the technology"*. However, people do not feel alone with these issues and do not see themselves as the problem; rather, they think that most people face similar problems, as P16 describes: *"I don't think I'm the only one who knows so little about it."*

Security Issues. We aggregated the mentioned security issues into the code groups *Lacking App Security*, *Careless App Security*, and *App Independent Security Issues.* Participants mentioned only very few technical security issues with apps, and if so, they were vague. They believe that the risk of hackers accessing resources can hardly be ruled out. Besides these few technical concerns, participants mentioned many soft causes involving app-providing companies. They often criticize that they are forced to disclose their data to use a service, making them feel powerless: *"So I don't have the feeling that I have any influence on it"* (P1). Moreover, a lack of trust in the companies is omnipresent: *"I don't think that this is one hundred percent certainty, that only data that you agree to be used is actually collected"* (P14).

5.4.2 Privacy Issues (RQ1-2).

Illiteracy. As a result of the previously observed dissatisfaction with privacy information, illiteracy is a central theme that we found among the participants' privacy issues, e.g., P7 stating *"sometimes it's not quite clear to me exactly which data is being provided."* The lack of understanding evokes skepticism. Our interviews show that people would be less concerned if they were better informed about what happens with their data.

Third Party Data Sharing. Concerns arise, especially around who the data is shared with and for what purposes. Disclosure to third parties is the most mentioned privacy issue. *"There is the discomfort of not knowing how it will be used and, above all, to whom it will be passed on"* (P19). People believe that companies might sell their data to others, and are even afraid that their data will become publicly available. Besides deliberate disclosure by companies, our participants also believe that data is frequently stolen. Such concerns were mentioned half as many times as the aforementioned concerns: *"There are so many, these data leaks, these bank data leaks or PayPal data leaks"* (P4).

Misuse. Participants mentioned concerns about misuse, especially the creation of profiles: *"I actually don't want user profiles to be created about me and all the data, so all this data ends up coming together in a user profile"* (P3). With such user profiles *"it may also be possible to read off interests, attitudes, and the like. I would subsume that under the term personality profile."* Thereby, participants are especially afraid of technology's ability to reveal information that is uncomfortable or not even known to themselves. For example, P8 envisioned a case of the smartphone being aware of one's pregnancy earlier than the woman herself: *"There is a teenage girl who was pregnant, but she did not know that she was pregnant and googled her symptoms. And then some company sent her a sample pack of Pampers".*

Acceptance of Data Logging. The acceptance of data usage is generally quite low, as users believe data is logged without valid reasons. Overall, they dislike data getting logged: *"On the whole, I find it generally bad that data are collected"* (P12). Some participants think beyond themselves and complain that information on other people is also logged without their consent. *"I don't think that's okay because what can my friends do if I agree and then their data is passed on?"* (P16).

5.4.3 Consequences (RQ2). After looking at privacy issues and their underlying causes, we were interested in what *consequences* users are actually afraid of. Consequences can be real-life events that might happen as a result of privacy issues or outcomes in the digital world that affect the user. As major topics concerning the user, we mostly found real-world consequences like *financial loss* and *influencing beliefs*. The participants further mentioned criminal activities like *Theft*, *Physical Harm*, and *Shared Information*. Furthermore, *Emotional Damage* and *Data Loss* were mentioned.

Financial Loss. Participants are afraid of *"that your bank account is emptied"* (P12) and *"that you just get bills that you have to pay because you ordered goods but didn't get them"* (P12). Furthermore, participants envision that activity and health data could have an influence on their creditworthiness and insurance rates. While users find direct monetary loss to be likely through hacking, they expect that insurance companies would rather buy data from app companies to fuel their risk assessment.

Manipulation. Our participants are aware of procedures that make use of user data to *influence beliefs* and manipulate the behaviors of their users. They see risks in derived profiles being used to subconsciously influence one's beliefs, especially regarding political opinions, shopping behavior, and increased device usage: *"Manipulations happen in people unconsciously. And I think this is a very difficult and dangerous topic for our society"* (P7). They mention political manipulation more often than other factors like shopping, and stress that the impact is more severe: *"I find it difficult when I am manipulated in a way to vote for a party that wants to come to power. I find that has a very different effect than if I buy the top from the brand because it was advertised to me"* (P7). P8 generalizes this to the issue of filter bubbles: *"What's problematic is when you then use that to reinforce some opinions, or spread certain content more. So I don't know, for example, if you think about the US elections or all these fake news scandals, that you get the same information over and over again instead of somehow getting a broader picture of it."* On the bigger picture, P3 mentioned the concern of *"a change in the political landscape".*

Criminal Activities. Participants mentioned many criminal activities they believed to be enabled by privacy issues. For instance, having one's location data *"they see exactly when you are not at home, [and] could take advantage of that to break into your house"* (P17). Identity theft is an issue that some participants came up with, envisioning it for various use cases. Beyond buying things on one's behalf, which is closely related to the aforementioned issue of financial loss, impersonation was brought up: *"They naturally use your data to take your entire identity and then use it to either go shopping or impersonate you"* (P12). P10 is afraid of being dragged into criminal activities by their accounts being misused: *"you are pulled into some criminal stories and have no idea at all about it, because your email was tapped"*. P7 even envisions that *"my whole identity could be erased and someone else could take my identity. Now, to put it bluntly, if there are photos, if my whole character can be recreated, if you want to have me away from society, you can achieve that through that"*. Further criminal points of attack are fraud via telephone or postal mail. Forged documents could be created by using signatures and photos. As a less sophisticated, but nevertheless annoying consequence, participants mentioned *spam and advertisement*: *"Consequences are simply that you are spammed too much by companies"* (P9). Spam can result in fraud by requesting payments or asking to enter login credentials.

Shared Information. Participants mentioned the vague concern of being spied out: *"And so there can even be spy features in there that we don't know about, that we don't even know what the purpose is of collecting and evaluating this message somewhere"* (P19). This is especially concerning as it may happen in the background without the user's awareness. *"That's just this paranoia that you always have a little bit. I have [camera and microphone] disabled, but maybe it still works somehow, maybe that's running in the background"* (P20).

5.4.4 Actors, Actions, and Datatypes (RQ2).

Actors. In contrast to the online survey, participants mentioned criminal third-party actors more often than non-criminal third-party actors. Participants are especially afraid of hackers gaining illegal access. Second-party actors, such as the device or OS developer company or big tech companies, were only mentioned a couple of times. Governmental organizations, such as governments, parties, or the police, were mentioned often. Not surprisingly, the first-party company, i.e., the developing company of an app or platform, sometimes raises concerns in our participants.

Actions. Participants expressed most concerns during real-world actions and active data entry. Having their phone with them yielded concerns during arbitrary activities. Situations where people have to enter data into an application manually also raise concerns about the usage of services. Here, participants brought up examples about photos, contact management, and search. The lifecycle steps of an app, i.e., installing it and granting permissions, were mentioned only sporadically.

Datatypes. In the interviews, participants often mentioned *Personal Information* as a matter of concern. Many stayed rather general and did not specify this further, while concrete aspects like interests, contact information, and name and phone number were mentioned. Among behavioral data, everything that is related to one's location is a big matter of concern. More device-related data, like files, contents, and communication details, were also mentioned but did not stand out.

5.4.5 Solutions to Mitigate Concerns (RQ3).

User Behavior. Most mentioned mitigation measures evolve around *user behavior*, i.e., actions that users themselves can and should do. This mostly includes active non-disclosure of data, for example, by denying apps' permission requests, disabling data sources in the device settings (e.g., disabling location or even being in flight mode), leaving input fields empty where possible, or otherwise entering falsified data, as P2 describes: *"by disclosing as little data as possible, so that if I have to give personal data somewhere, I just give a false date of birth, a false name, and so on."* As it is not always possible to use a service without giving data, participants mention the non-use of services or devices as their last option to protect their data. Some participants also described that they do some tasks only on their laptops instead of on their smartphones: *"When I log in to PayPal, it is not on my cell phone most of the time, but rather on my laptop"* (P7). Others describe that they leave their smartphone at home at some times, which makes them feel less surveilled, or do not use some kinds of devices at all (especially smart home devices; *"So that's why I don't have Alexa in the house either"* (P17)). Some participants admit that better password management or using separate email addresses would be beneficial. They suggest making use of data deletion options more often, for example, clearing cookies and histories, or actively requesting the deletion of their collected data with app companies.

Transparency. The two most frequently mentioned concern mitigations were (1) transparency on the data usage and (2) using data for a purpose that users find beneficial. The latter is, for example, *"(market-)research"* (P12, P8), *"location for location-based services"* (P3, P9), and in general use cases where users see a direct benefit for them by granting access to data. They admit that *"a lot of data is also necessary for the services that are offered there"* (P13). Continuing closely on the results of bad transparency through privacy policies (cf. Section 5.4.1), users would like to know what data is logged, would like to get insights into created profiles, and wonder for how long data is stored. What is happening to their data is also interesting, i.e., how it is processed and whether it is passed on to third parties. They lack knowledge of the reasons for data processing and possible effects. Participants mention many suggestions on how these information needs could be satisfied: Information on data usage should be *"as concise and informative as possible and as understandable as possible"* (P5). To improve current consent mechanisms, P13 suggests visual means to convey what happens: *"Sometimes, it would be nice if there was a bit of a simple overview. Somehow no idea, little pictures, little pictures that tell me what happens with my data. I would find that practical."*

Regulations. Another frequently mentioned suggestion to improve the users' privacy situation is *regulations*. While P13 formulates it rather soft *"there should be standards that encourage companies to handle data responsibly and not sell it to third parties"*, P15 sees a chance in strict laws: *"if there were clearer laws about how those could be used, if I knew, okay, they can use them, but if they're used past a certain point, then it's sort of illegal."* To avoid loopholes, regulations would ideally be on a supra-national level. P16 believes that *"it would, of course, be great if something like this were regulated throughout the EU [...] because that would be more effective, I imagine."* Participants thereby emphasized that *"[governmental agencies] then have to monitor it accordingly"* (P5). As users do not trust governmental organizations to stick to such rules and control themselves, *"then there might have to be external control systems there to control that"* (P5).

Company Behavior and Technical Security. Fewer participants envision that behavior changes by the companies and the application of technical security measures could mitigate their privacy concerns. Wishes include simply collecting less data (P5, P7, P2), deleting data as soon as possible (P2, P4, P7), and not selling or disclosing data to others (P4, P6, P10, P13). An idea of P19 includes managing data in a similar way to how it is done with artistic content. They propose that *"when data is resold, I think it's right that, as in the case of copyright, you should also be involved, so to speak. And not to get rich, but simply to limit the whole thing a bit"*. Purely technical security measures such as encryption (P13, P17), two-factor-authentication (P18, P20) or very general *"more security"* (P12) were mentioned only sporadically.

Circumstances. Also, sporadically, some participants said that their current living circumstances contribute to mitigating concerns. P1 mentions being less concerned *"because I have not yet had any very bad experiences"*, and P2, P3, and P20 mention that they are less concerned due to our solid political system. Also, a couple of participants believe that *"on an individual level, no one* *bothers to get our personal data, my personal data, because there is simply too little to get"* (P11) what contributes to mitigated concerns.

6 Discussion

In the following, we discuss the results of our research questions and contextualize them in prior work. Based on our findings, we extract actionable items for developers and lawmakers to ensure users are knowledgeable about privacy risks posed by mobile sensing apps and, thus, empower users to make informed decisions.

6.1 RQ1: Users are Knowledgeable in General but Lack Information about Concrete Apps

We found that the major issue regarding knowledge about smartphone privacy is a lack of information about the apps' data practices. Users' general knowledge and understanding of how smartphones and privacy-enhancing technologies work were rather good. 90% of our participants could answer most of our quiz correctly. However, it has to be noted that the survey sample was rather young and reported an above-average ATI score.

Regarding concrete apps, participants mentioned that they are often not completely aware of what data apps are logging and what happens with their data afterward. They are further unsure about the kinds of data apps can obtain from the device. Privacy policies are criticized for not being understandable. In our quantitative assessment of engagement with privacy information, we found that users behave ambivalently; while some people state to engage a lot and try to inform themselves, others do the opposite.

People's concerns were partially vague; they mentioned many uncertainties and things they were unsure about, but had "heard about." We found that uncertainties and the laborious nature of informing oneself about privacy lead to reduced motivation. This negative feedback loop finally reduces trust and transparency and increases concerns. Thus, we conclude on RQ1 that **the users' general knowledge of smartphones and privacy-enhancing technologies is good, but they lack information and understanding of apps' data practices**.

6.2 RQ2: Users are Concerned About Uncertain Incidents that Affect their Real-World Lives

The quantitative and qualitative results of both studies show that users are most concerned about third parties stealing and misusing their data. Users are able to name concrete consequences and especially fear real-world consequences, such as financial loss and burglary. This extends the findings of Bemmann and Mayer [9], who identified wallet and account information as the most sensitive data types, and reveals that users regard these as the critical connection to their real-world assets and identity. Participants considered data processing on global and remote servers more concerning than local data processing. We expected this in the light of previous work [74]. Our findings show that the implications, which, among others, Van Kleek et al. [74] made nearly a decade ago, are still not yet spread and applied. Our participants' concerns revolve mostly around uncertainties, demanding better transparency and control. Especially regarding the redistribution of data, for example, to third parties, we need to find ways to build trust. Our study showed that people fear unwanted data access by non-criminal third parties similarly often, even slightly more, than criminal access acquisition. We argue for more focus on real-world implications and incorporating them in the full system design pipeline. Some positive examples are Ferra et al. [32], which incorporates real-world consequences in privacy impact assessment, or Cote and Albu [21], studying societal implications of ubiquitous computer vision devices.

Overall, it is noticeable that most concerns are based on uncertainties, loss of control, or missing information about hidden or remote sections of the smartphone data processing pipeline. Such concerns play an essential role in constituting (often subconscious) concerns that are not new (cf., [9, 29, 31]). Our study identifies the specific underlying *Privacy Issues* (i.e., underlying reasons) that people are afraid of, and thereby enhances our understanding of these issues. Privacy-enhancing technologies should focus on conveying the access scopes (i.e., tackling our privacy issues *Access to Broad*) and reasons for data usage (i.e., *Logging without Reason* and *Misuse*) to mitigate consequences regarding unintentionally *Shared Information.* Approaches leveraging physicalization and tangible approaches, therefore, seem promising. For example, in the context of smart homes, Windl et al. [81] and Delgado Rodriguez et al. [25] showed the strength of physical mechanisms in raising privacy awareness and providing control, and Windl et al. [79] reached a better understanding of security issues through a physical smart home dashboard. Due to their mobile and portable nature, it might be hard to adapt tangible approaches to smartphones. Nevertheless, as configuring a smartphone's privacy settings and informing oneself about privacy practices are not regularly performed tasks, which would require carrying the tangible around at all times, such approaches might still be promising.

Approaches leveraging physicalization and tangible approaches seem promising, for example, providing users guarantees of not giving away this information. As Shklovski et al. [69] summarizes the privacy conceptualizations of Altman [4] and Nissenbaum [58], smartphones constitute an extension of one's personal space. Thus, the design of an access control system's identity management should be closely tied to real-world humans. Studies in the context of smart homes (cf. [25, 81] showed the strength of physical mechanisms in raising privacy awareness and providing control, and Windl et al. [79] reached a better understanding of security issues through a physical smart home dashboard. As configuring a smartphone's privacy settings and informing oneself about privacy practices are not regularly performed tasks, tangibles could be decoupled from mobile devices so as not to burden users with additional hardware to carry.

We could also quantify that users who know and understand more about privacy-enhancing technologies have greater concerns. This finding aligns with prior literature [36] that found that users initially ignore privacy but show greater concerns when they become aware of the possible consequences. Our qualitative insights also stress illiteracy as a factor that reinforces privacy issues. As work by Ketelaar and Van Balen [42] discovered, an increase in smartphone literacy lowers privacy concerns and fosters a positive attitude towards privacy-enhancing technologies. Literacy contributes to the three factors that reduce privacy concerns by Malhotra et al. [52], namely collection, control, and awareness.

Regarding the reported qualitative statements on concerns and real-world events, it is important to note that these stories are not always based on lived experiences but are often rather imaginary stories. As concerns are, by nature, not necessarily based on real-world experiences but often about imaginary events resulting from uncertainties and word of mouth, such imaginary stories are essential to understanding users' perceptions of privacy concerns.

We conclude on RQ2: **Smartphone users are concerned about their data being misused by unknown third parties and data being used against them with negative implications on their lives.**

6.3 RQ3: Mitigation of Privacy Concerns: User-Centered Privacy Measures

In **RQ3**, we probed users on how they think their concerns can be mitigated. Our participants suggested various measures that they can take themselves to overcome privacy risks, such as changing their own behavior. These actions feel more in control for them, and they can easily understand their effects. However, this situation is rather unsatisfying for the users and expresses despair. Research needs to find solutions to offload the users from these duties. Our findings support the directions of Momen et al. [57], showing that recent regulatory additions made a difference but are still not comprehensive and specific enough. Legal requirements should prohibit feared privacy issues that are beyond the user's scope of control. Our findings suggest that remote actions do not meet user expectations, such as third-party data access, logging without reasons, and too broad access scopes. Our findings provide details on important characteristics that such regulations should encompass. We thereby enhance and further specify existing recommendations to legislators, such as those proposed by van Hoboken and Fathaigh [73] or Miltgen and Smith [56].

Although regulations are a good first step, they have limitations and show a rather weak connection to actual privacy perception (cf. Schomakers et al. [68]). In the long run, privacy-by-design should be implemented: Through technical measures such as differential privacy (e.g., Machanavajjhala et al. [50]), synthetic data (e.g., Hu et al. [39]), and a shift to more local processing on the user's device (e.g., Bemmann and Buschek [8]), we need to guarantee privacy-friendly data processing to our users. Thereby, focusing on the HCI in technical privacy measures is essential. Sole technical solutions do not bridge the gap to perceived privacy, as recent work stresses [5]. Our findings show the importance of a human-centered design; trust in and the effect of sole technical concepts was low and only sporadically mentioned as a potential improvement.

Thus, we see a clear need to incorporate user-centered privacy in apps to increase users' trust in their apps.

6.4 Context and Perspective

Privacy research, as it is mostly about subjective perceptions, is highly sensitive to how opinions are assessed/asked and individual contexts, e.g., by country. When comparing our two studies, this is reflected in a number of "code flips," i.e., some codes occurring rarer in the online survey than in the interviews. For example, *Inaccurate Privacy Policy* (3x in the online survey, vs. 15x in the interviews) and *Misuse* (5 vs. 19) occurred more often in the interviews. The two codes *The User* and *Emotional Damage* could only be identified clearly in the interviews. The reasons therefore, lay in the natures of survey and interview data collection: While in the online survey, people tend to mention many, but rather superficial aspects (e.g., *Lacking App Security* (39 vs. 3) and *Access too Broad* (58 vs. 13)), a semi-structured interview enables to dig deeper and is very valuable to obtain insights into the user perspective of underlying privacy concern reasons and mitigation paths.

6.5 Lack of Transparency Across All Areas

Our survey and the interviews reveal that a lack of transparency is the overarching topic touching all code groups and stages of our privacy concern model. Uncertainty and a lack of information, knowledge, and understanding constitute the cause of many privacy issues and feared consequences. Thus, the most desired mitigation measures revolve around increasing transparency: Better consent mechanisms and short and concise information that highlights essential aspects were mentioned by nearly all participants. This information has to be easy to understand and could be augmented with visual elements to support understanding one's data flow. It could also be advantageous to clarify the aim and purpose of data processing. Although we saw a generally low acceptance for data logging and processing, our interviews have shown that people mostly agree with data usage if the purpose is clear and they consider it meaningful. Thus, we conclude that **system designers and developers should emphasize concise, transparent, and understandable information and consent mechanisms**.

6.6 Users Demand More Control

Strongly tied to the aforementioned lack of transparency is the desire for more control, albeit not yet as present as transparency. When digging deeper into interview responses, we saw that participants feel like they are not the owners of their data anymore. However, having direct control over one's data from logging to processing is considered an effective concern mitigation measure. We saw that participants most frequently mentioned measures they themselves can do rather than mitigation measures performed by the data processor or other third parties. We argue that **users should be offered full control over their data and what happens with it at all times**. Recent research by Bemmann et al. [10] has shown that control is the integral component of concern reduction. While the sole increase of transparency can increase users' concerns, giving users control features is what actually reduces the perceived concerns.

6.7 Lack of Trust - Call for Regulations

Transparent information mechanisms and control features require trust in the information being true. Respectively, control features affect what they are claiming. However, in the interviews, we noticed that participants were skeptical about companies' honesty. Participants accused them of providing incomplete information, not implementing what they promised, and a general reluctance to act for the users' good. Hence, many suggested mitigation measures are regulations, which are a way to force companies to guarantee user-friendly behavior. (Tech) companies should, therefore, **work on their reputation and find ways to guarantee privacy**. Role models from the technical perspective could be approaches like differential privacy (cf. Zhao and Chen [86]) or digital signature approaches.

6.8 Limitations and Future Work

We tried to collect a balanced sample for our study. However, our data is still limited to a European view. This might have skewed our results as Europeans are generally recognized as being more privacy-aware than countries like India, China, or the U.S. [72, 75]. An analysis of different populations was out of the scope of this paper. However, we would like to motivate future work that compares different privacy perspectives. Taxonomies could be developed for population groups based on their specific concerns. Thereby, developers could be given an overview and design guidelines on improving their application designs so that the needs of as many specific population groups as possible are incorporated. Furthermore, selection biases might have occurred in the participant sampling. The motivation to deal with privacy belongings follows a bipolar distribution, and thus rather attracts people on the high-motivation pole of this distribution. We designed the study call as neutral as possible; However, selection biases cannot be ruled out completely.

Lastly, it is important to keep in mind that our study reports a European perspective, with further differences between the samples from the two studies. While the first survey included participants from various European countries, the interviews were conducted specifically in Germany.

7 Conclusion

This work uncovered detailed user concerns regarding smartphone privacy, which have only been vaguely understood so far. For this, we conducted a large-scale online survey (N=100) and semi-structured interviews (N=20). We found that users are mostly concerned about financial loss, being manipulated, and criminal activities being targeted against them. They see the underlying privacy issue mostly in data being shared or stolen by third-party actors, such as companies or hackers. Overall, we found a lack of transparency across all investigated areas. Finally, we found that to mitigate users' privacy concerns, app developers should mind user-centered privacy, including transparency, control, and trust. Although these concepts are not completely new, our work contributes by extending existing studies around smartphone privacy perceptions with up-to-date, in-depth user perspectives. The concepts of transparency and control, and the researcher's awareness of the importance of user-centered design, are already prominent. However, our work reveals that they are still not implemented sufficiently and that further efforts need to be made. Research and industry struggle with their implementation, and have a hard time solving the tradeoff of providing privacy features while not bothering the user too much or endangering their business model. In contrast to previous work, we especially regard the mitigation perspective - i.e., gain an understanding of how the present concerns could be mitigated from the users' perspective.

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/d3fe8/.

Author Contributions

Florian Bemmann: Conceptualization, Formal Analysis, Investigation, Methodology, Visualization, Writing – original draft, Writing – review & editing; **Maximiliane Windl**: Conceptualization, Formal Analysis, Methodology, Writing – original draft, Writing – review & editing; **Tobias Knobloch**: Formal Analysis, Investigation, Methodology, Writing – original draft; **Sven Mayer**: Conceptualization, Formal Analysis, Funding acquisition, Methodology, Supervision, Writing – original draft, Writing – review & editing

Acknowledgments

This work has been partly supported by the Research Center Trustworthy Data Science and Security (https://rc-trust.ai), one of the Research Alliance centers within the UA Ruhr (https://uaruhr.de).

References

[1] Tanisha Afnan, Yixin Zou, Maryam Mustafa, Mustafa Naseem, and Florian Schaub. 2022. Aunties, Strangers, and the FBI: Online Privacy Concerns and Experiences of Muslim-American Women. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS'22)*. USENIX Association, USA, 387–406. https://www.usenix.org/system/files/soups2022-afnan.pdf

[2] Icek Ajzen. 1985. *From intentions to actions: A theory of planned behavior.* Springer, Cham, Switzerland, 11–39. doi:10.1007/978-3-642-69746-3_2

[3] Akbar Ali, Nasir Ayub, Muhammad Shiraz, Niamat Ullah, Abdullah Gani, and Muhammad Ahsan Qureshi. 2021. Traffic Efficiency Models for Urban Traffic Management Using Mobile Crowd Sensing: A Survey. *Sustainability* 13, 23 (2021), 13068. doi:10.3390/su132313068

[4] Irwin Altman. 1975. *The environment and social behavior: privacy, personal space, territory, and crowding.* ERIC, USA.

[5] Oshrat Ayalon and Eran Toch. 2019. Evaluating Users' Perceptions about a System's Privacy: Differentiating Social and Institutional Aspects. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX, USA, 41–59. doi:10.5555/3361476.3361480

[6] 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. doi:10.1145/2501604.2501616

[7] Natã M Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 211–231. doi:10.2478/popets-2019-0066

[8] Florian Bemmann and Daniel Buschek. 2020. Languagelogger: A mobile keyboard application for studying language use in everyday text communication in the wild. *Proceedings of the ACM on Human-Computer Interaction* 4, EICS (2020), 1–24. doi:10.1145/3397872

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

[10] 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 (Sept. 2022), 26 pages. doi:10.1145/3546724

[11] Jan Blom, Daniel Gatica-Perez, and Niko Kiukkonen. 2011. People-Centric Mobile Sensing with a Pragmatic Twist: From Behavioral Data Points to Active User Involvement. 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, 381–384. doi:10.1145/2037373.2037431

[12] Jan Lauren Boyles, Aaron Smith, and Mary Madden. 2012. Privacy and data management on mobile devices. *Pew Internet & American Life Project* 4 (2012), 1–19.

[13] Petter Bae Brandtzaeg, Antoine Pultier, and Gro Mette Moen. 2019. Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. *Social Science Computer Review* 37, 4 (2019), 466–488. arXiv:https://doi.org/10.1177/0894439318777706 doi:10.1177/0894439318777706

[14] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[15] Alex Braunstein, Laura Granka, and Jessica Staddon. 2011. Indirect content privacy surveys: measuring privacy without asking about it. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania) *(SOUPS '11)*. Association for Computing Machinery, New York, NY, USA, Article 15, 14 pages. doi:10.1145/2078827.2078847

[16] Mauro Cherubini, Rodrigo de Oliveira, Anna Hiltunen, and Nuria Oliver. 2011. Barriers and Bridges in the Adoption of Today's Mobile Phone Contextual Services. 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, 167–176. doi:10.1145/2037373.2037400

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

[18] 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. doi:10.1016/j.jss.2011.06.073

[19] Jessica Colnago, Lorrie Faith Cranor, Alessandro Acquisti, and Kate Hazel Stanton. 2022. Is it a concern or a preference? An investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, USA, 331–346. https://www.usenix.org/conference/soups2022/presentation/colnago

[20] Kovila PL Coopamootoo and Thomas Groß. 2014. Mental models: an approach to identify privacy concern and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 9–11.

[21] Melissa Cote and Alexandra Branzan Albu. 2017. Teaching computer vision and its societal effects: A look at privacy and security issues from the students' perspective. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, New York, NY, USA, 1378–1386. doi:10.1109/CVPRW.2017.180

[22] Kenneth James Williams Craik. 1967. *The nature of explanation*. Vol. 445. CUP Archive, Cambridge, UK.

[23] 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. doi:10.1287/orsc.10.1.104

[24] Kenan Degirmenci. 2020. Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management* 50 (2020), 261–272. doi:10.1016/j.ijinfomgt.2019.05.010

[25] Sarah Delgado Rodriguez, Sarah Prange, Pascal Knierim, Karola Marky, and Florian Alt. 2022. Experiencing Tangible Privacy Control for Smart Homes with PriKey. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 298–300. doi:10.1145/3568444.3570585

[26] Paula Delgado-Santos, Giuseppe Stragapede, Ruben Tolosana, Richard Guest, Farzin Deravi, and Ruben Vera-Rodriguez. 2022. A Survey of Privacy Vulnerabilities of Mobile Device Sensors. *ACM Comput. Surv.* 54, 11s, Article 224 (sep 2022), 30 pages. doi:10.1145/3510579

[27] Robert F DeVellis and Carolyn T Thorpe. 2021. *Scale Development: Theory and Applications*. Vol. 26. SAGE Publications, Thousand Oaks, CA, USA.

[28] Leyla Dogruel, Sven Joeckel, and Nicholas D Bowman. 2015. Choosing the right app: An exploratory perspective on heuristic decision processes for smartphone app selection. *Mobile Media & Communication* 3, 1 (2015), 125–144. doi:10.1177/2050157914557509

[29] Aarthi Easwara Moorthy and Kim-Phuong L Vu. 2015. Privacy concerns for use of voice activated personal assistant in the public space. *International Journal of Human-Computer Interaction* 31, 4 (2015), 307–335. doi:10.1080/10447318.2014.986642

[30] Christos Efstratiou, Ilias Leontiadis, Marco Picone, Kiran K Rachuri, Cecilia Mascolo, and Jon Crowcroft. 2012. Sense and sensibility in a pervasive world. In *International Conference on Pervasive Computing*. Springer, Cham, Switzerland, 406–424. doi:10.1007/978-3-642-31205-2_25

[31] Serge Egelman, Adrienne Porter Felt, and David Wagner. 2013. Choice architecture and smartphone privacy: There'sa price for that. *The economics of information security and privacy* (2013), 211–236. doi:10.1007/978-3-642-39498-0_10

[32] Fenia Ferra, Isabel Wagner, Eerke Boiten, Lee Hadlington, Ismini Psychoula, and Richard Snape. 2020. Challenges in assessing privacy impact: Tales from the front lines. *Security and Privacy* 3, 2 (2020), e101. doi:10.1002/spy2.101

[33] 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. doi:10.1080/10447318.2018.1456150

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

[35] Carol Fung, Vivian Motti, Katie Zhang, and Yanjun Qian. 2022. A Study of User Concerns about Smartphone Privacy. In *2022 6th Cyber Security in Networking Conference (CSNet)*. IEEE, New York, NY, USA, 1–8. doi:10.1109/CSNet56116.2022.9955623

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

[37] Cornelia Helfferich. 2011. *Die Qualität qualitativer Daten*. Vol. 4. Springer, Cham, Switzerland.

[38] Christel Hopf. 2012. 5.2 Qualitative Interviews–ein Überblick. *Qualitative Forschung. Ein Handbuch* 9 (2012), 349–360.

[39] Yuzheng Hu, Fan Wu, Qinbin Li, Yunhui Long, Gonzalo Munilla Garrido, Chang Ge, Bolin Ding, David Forsyth, Bo Li, and Dawn Song. 2024. SoK: Privacy-Preserving Data Synthesis. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 4696–4713. doi:10.1109/SP54263.2024.00002

[40] Tun-Min Catherine Jai and Nancy J King. 2016. Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services* 28 (2016), 296–303. doi:10.1016/j.jretconser.2015.01.005

[41] Philip Nicholas Johnson-Laird. 1983. *Mental models: Towards a cognitive science of language, inference, and consciousness*. Number 6. Harvard University Press, Cambridge, MA, USA.

[42] 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. doi:10.1016/j.chb.2017.09.034

[43] 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. doi:10.1093/poq/nfz007

[44] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring privacy concerns about personal sensing. In *International Conference on Pervasive Computing*. Springer, Cham, Switzerland, 176–183. doi:10.1007/978-3-642-01516-8_13

[45] 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. doi:10.1109/PERCOMW.2019.8730874

[46] Ya-Cheng Li and Shin-Ming Cheng. 2018. Privacy preserved mobile sensing using region-based group signature. *IEEE Access* 6 (2018), 61556–61568. doi:10.1109/ACCESS.2018.2868502

[47] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (Pittsburgh, Pennsylvania) *(UbiComp '12)*. Association for Computing Machinery, New York, NY, USA, 501–510. doi:10.1145/2370216.2370290

[48] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, USA, 199–212. doi:10.5555/3235838.3235856

[49] Changchang Liu, Supriyo Chakraborty, and Prateek Mittal. 2017. DEEProtect: Enabling Inference-based Access Control on Mobile Sensing Applications. arXiv:1702.06159 [cs.CR] doi:10.48550/arXiv.1702.06159

[50] Ashwin Machanavajjhala, Xi He, and Michael Hay. 2017. Differential Privacy in the Wild: A Tutorial on Current Practices & Open Challenges. In *Proceedings of the 2017 ACM International Conference on Management of Data* (Chicago, Illinois, USA) *(SIGMOD '17)*. Association for Computing Machinery, New York, NY, USA, 1727–1730. doi:10.1145/3035918.3054779

[51] Elsa Macias, Alvaro Suarez, and Jaime Lloret. 2013. Mobile sensing systems. *Sensors* 13, 12 (2013), 17292–17321. doi:10.3390/s131217292

[52] 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. doi:10.1287/isre.1040.0032

[53] Haroon Iqbal Maseeh, Shamsun Nahar, Charles Jebarajakirthy, Mitchell Ross, Denni Arli, Manish Das, Mehak Rehman, and Hafiz Ahmad Ashraf. 2023. Exploring the privacy concerns of smartphone app users: a qualitative approach. *Marketing Intelligence & Planning* 41, 7 (2023), 945–969. doi:10.1108/mip-11-2022-0515

[54] Justin Matejka, Michael Glueck, Tovi Grossman, and George Fitzmaurice. 2016. The Effect of Visual Appearance on the Performance of Continuous Sliders and Visual Analogue Scales. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5421–5432. doi:10.1145/2858036.2858063

[55] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543–568.

[56] Caroline Lancelot Miltgen and H Jeff Smith. 2015. Exploring information privacy regulation, risks, trust, and behavior. *Information & Management* 52, 6 (2015), 741–759. doi:10.1016/j.im.2015.06.006

[57] Nurul Momen, Majid Hatamian, and Lothar Fritsch. 2019. Did app privacy improve after the GDPR? *IEEE Security & Privacy* 17, 6 (2019), 10–20. doi:10.1109/MSEC.2019.2938445

[58] Helen Nissenbaum. 2011. Privacy in context: Technology, policy, and the integrity of social life. *Journal of Information Policy* 1 (2011), 149–151.

[59] Jonathan A. Obar. 2016. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *SSRN Electronic Journal* (2016), 37. doi:10.2139/ssrn.2757465

[60] Obi Ogbanufe and Robert Pavur. 2022. Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management* 62 (2022), 102432. doi:10.1016/j.ijinfomgt.2021.102432

[61] Derek H. Ogle, Jason C. Doll, Powell Wheeler, and Alexis Dinno. 2022. *FSA: Fisheries Stock Analysis.* R package version 0.9.3.

[62] 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*. Springer International Publishing, Cham, 339–360. doi:10.1007/978-3-030-85610-6_20

[63] Ismini Psychoula, Deepika Singh, Liming Chen, Feng Chen, Andreas Holzinger, and Huansheng Ning. 2018. Users' privacy concerns in IoT based applications. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*. IEEE, New York, NY, USA, 1887–1894. doi:10.1109/SmartWorld.2018.00317

[64] Melanie Revilla, Mick P Couper, and Carlos Ochoa. 2019. Willingness of online panelists to perform additional tasks. *Methods, data, analyses: a journal for quantitative methods and survey methodology (mda)* 13, 2 (2019), 223–252. doi:10.12758/mda.2018.01

[65] 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. doi:10.1145/2556288.2557189

[66] Maxim Schessler, Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Replication: Measuring User Perceptions in Smartphone Security and Privacy in Germany. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 165–179. doi:10.1145/3481357.3481511

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

[68] Eva-Maria Schomakers, Chantal Lidynia, Dirk Müllmann, Roman Matzutt, Klaus Wehrle, Indra Spiecker genannt Döhmann, and Martina Ziefle. 2021. Putting Privacy into Perspective – Comparing Technical, Legal, and Users' View of Information Sensitivity. In *INFORMATIK 2020*. Gesellschaft für Informatik, Bonn, Germany, 857–870. doi:10.18420/inf2020_76

[69] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. 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, 2347–2356. doi:10.1145/2556288.2557421

[70] Janice C Sipior, Burke T Ward, and Linda Volonino. 2014. Privacy concerns associated with smartphone use. *Journal of Internet Commerce* 13, 3-4 (2014), 177–193. doi:10.1080/15332861.2014.947902

[71] Edith G Smit, Guda Van Noort, and Hilde AM Voorveld. 2014. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* 32 (2014), 15–22. doi:10.1016/j.chb.2013.11.008

[72] Sabine Trepte and Philipp K Masur. 2016. Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study. (2016).

[73] Joris van Hoboken and R Ó Fathaigh. 2021. Smartphone platforms as privacy regulators. *Computer Law & Security Review* 41 (2021), 105557. doi:10.1016/j.clsr.2021.105557

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

[75] Yang Wang, Gregory Norice, and Lorrie Faith Cranor. 2011. Who Is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on Social Network Sites. In *Trust and Trustworthy Computing*, Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse, and Yolanta Beres (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 146–153.

[76] Yongfeng Wang, Zheng Yan, Wei Feng, and Shushu Liu. 2020. Privacy protection in mobile crowd sensing: a survey. *World Wide Web* 23, 1 (2020), 421–452. doi:10.1007/s11280-019-00745-2

[77] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. doi:10.1145/1837110.1837125

[78] Angela Wichmann. 2019. *Quantitative und qualitative Forschung im Vergleich*. Springer, Cham, Switzerland.

[79] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S. Feger. 2022. SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proc. ACM Hum.-Comput. Interact.* 6, ISS, Article 586 (Nov. 2022), 20 pages. doi:10.1145/3567739

[80] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (Sept. 2022), 21 pages. doi:10.1145/3546719

[81] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. 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 70, 16 pages. doi:10.1145/3544548.3581167

[82] Verena M Wottrich, Eva A van Reijmersdal, and Edith G Smit. 2018. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision support systems* 106 (2018), 44–52. doi:10.1016/j.dss.2017.12.003

[83] Stephen Xia and Xiaofan Jiang. 2020. PAMS: Improving Privacy in Audio-Based Mobile Systems. In *Proceedings of the 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things* (Virtual Event, Japan) *(AIChallengeIoT '20)*. Association for Computing Machinery, New York, NY, USA, 41–47. doi:10.1145/3417313.3429383

[84] Tevfik Sukru Yaprakli and Musa Unalan. 2017. Consumer Privacy in the Era of Big Data: A Survey of Smartphone Users' Concerns. *PressAcademia Procedia* 4, 1 (2017), 1–10. doi:10.17261/Pressacademia.2017.509

[85] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, USA, 65–80. doi:10.5555/3235924.3235931

[86] Ying Zhao and Jinjun Chen. 2022. A survey on differential privacy for unstructured data content. *ACM Computing Surveys (CSUR)* 54, 10s (2022), 1–28. doi:10.1145/3490237

A Survey

A.1 Demographics

- (1) In which country do you currently reside? *(drop down of all countries)*
- (2) Which gender do you most identify with? *(single choice)*
  - Male
  - Female
  - Non binary
  - Self-described *(free text)*
- (3) How old are you? *(numeric input)*
- (4) 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
- (5) What is your current primary occupation? *(free text)*

A.2 Privacy: IUIPC

Many people spend a lot of time online, for example, on their smartphones, tablets, or computers. During this time online, people also share data, for example when signing up for online shopping, posting on social media, or using GPS in navigation apps. In the following questions, we are interested in your personal experience and perception when sharing your personal information online.

Please indicate the degree to which you agree/disagree with the following statements. *(7-point Likert scale ranging from strongly disagree to strongly agree.*

- I have been the victim of what I felt was an improper invasion of privacy.
- I am very concerned about the privacy of my data.
- I always falsify personal information needed to register with some websites.
- It usually bothers me when online companies ask me for personal information.
- When online companies ask me for personal information, I sometimes think twice before providing it.
- It bothers me to give personal information to so many online companies.
- I'm concerned that online companies collect too much personal information.
- Your online privacy is really a matter of your right to exercise control and autonomy over decisions about how your information is collected, used, and shared.
- Your control of your personal information lies at the heart of your privacy.
- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
- Companies seeking information online should disclose the way the data are collected, processed, and used.
- A good consumer online privacy policy should have a clear and conspicuous disclosure.
- It is very important to me that I am aware and knowledgeable about how my personal information will be used.

A.3 Affinity for Technology

Next, we are interested in how you deal with technology. Please indicate the degree to which you agree/disagree with the following statements. *(6-point Likert scale from completely disagree to completely agree.)*

- I like to occupy myself in greater detail with technical systems.
- I like testing the functions of new technical systems.
- I predominantly deal with technical systems because I have to.
- When I have a new technical system in front of me, I try it out intensively.
- I enjoy spending time becoming acquainted with a new technical system.
- It is enough for me that a technical system works; I don't care how or why.
- I try to understand how a technical system exactly works.
- It is enough for me to know the basic functions of a technical system.
- I try to make full use of the capabilities of a technical system.

A.4 Smartphone Usage

Next, we are interested in how you use your smartphone.

- (1) Of which brand and model is your smartphone? (e.g., Apple iPhone 11 Pro, Google Pixel 4a) *(free text)*
- *An explanation about mobile sensing:* In this survey, we investigate privacy and security issues of mobile sensing smartphone apps. These are apps that use sensors to acquire data about the user. That can be, e.g., the user's location, other apps they are using, or how much they are moving. This also includes data about the environment, e.g., ambient noise level and brightness. Sometimes the data is also transferred to a remote server, e.g., to enable an online dashboard summarizing the physical activity and draw a conclusion on the fitness level.
- (2)Do you have mobile sensing apps installed on your smartphone? If possible, please name three. *(three free texts, that have to be filled and ordered)*

A.5 Privacy & Technology: Knowledge

self-constructed quiz-like items to assess the knowledge and understanding of four privacy-enhancing technologies that are popular with mobile sensing: encryption, anonymous data collection, hashing

Next, we are interested in how you deal with privacy and technology.

In the following, you will see some statements describing technical measures to improve the privacy and security of mobile sensing apps. Please indicate for each statement whether you think that it is true or false.

(True or False single choice items)

A.5.1 Encryption. Encryption: Some apps use encrypted data transmission when sending the collected data to a remote server, for example via SSL or HTTPS.

- If an internet data transmission is encrypted (i.e., via SSL / HTTPS), only you, as the one who is sending the data, can read it.
- Encrypted internet data transmission (e.g., via SSL / HTTPS) ensures that others (e.g., internet network provider, others in your wifi network) cannot read the transmitted data.
- If an internet data transmission is encrypted (i.e., via SSL / HTTPS), nobody can decrypt it and read the original data.

A.5.2 Anonymous Data Collection. Anonymous Data Collection: For some use cases data is collected anonymously, to improve the user's privacy.

- If data is collected and transmitted anonymously, nobody besides you can read the collected and transmitted data.
- If data is collected and transmitted anonymously, it is NOT possible to assign the originating user (e.g., you) to the data stored on the remote server.
- If data is collected and transmitted anonymously, the data is NOT transmitted from your smartphone to a remote server.

A.5.3 Data Hashing. Data Hashing: Some apps are hashing data values that contain sensitive information.

- Hashing a location data log ensures that others (e.g., internet network provider, others in your wifi network) cannot read the logged location.
- If a location data log is hashed, nobody can decrypt it and read the original data value.
- If two location data logs are hashed and transmitted to a remote server, the app company that manages the remote server can check whether both locations are the same by comparing their hashes.

A.5.4 Remote Server. Remote Server: Most apps are connected to a remote server on the internet, where some or all of the collected data are transmitted to and stored.

- If a smartphone app transmits data to a remote server, it usually becomes accessible to everybody in the world.
- If a smartphone app transmits data to a remote server, you have full control over what happens to your data.
- The app company that manages the remote server has control over what happens with your data on the remote server and has to inform you about that in the privacy consent process.

A.6 Privacy & Technology: Familiarizing

Now please think about the moment when you install a new app on your smartphone through the app store.

(1) I am always making myself familiar with how my private data gets handled when installing an app. *(continuous slider item)*

A.7 Concerns with Mobile Phone Use

Concerning your data on your mobile phones, please think about one specific concern you have when you use your mobile phone. **Please write at least one sentence for each question.**

(All items are free text items)

- (1) With respect to mobile phone use, what **specifically** are you concerned about in terms of privacy?
- (2) **What could happen** to your data that makes you concerned?
- (3) In which **situations or locations** can this concern occur?
- (4) Which kinds of **data** are you concerned about in this situation?
- (5) How can this data that you are concerned about **be acquired**?
- (6) Which **actors** make you concerned?
- (7) How can you envision that your concern will be **reduced**?

This block could be repeated optionally up to three times, in order to enter multiple concerns.

A.8 Scenarios

In the following, we will present you with four scenarios of mobile sensing apps in daily life.

This section was prompted four times, once for each scenario (randomized). The current scenario was presented on the top of the page. You can find the scenario descriptions below.

- (1) I am very **familiar** with such apps. *(Continuous slider ranging from Strongly disagree to Strongly agree)*
- (2) I am very **concerned** about this scenario. *(Continuous slider ranging from Strongly disagree to Strongly agree)*
- (3) What exactly are you concerned about? What could happen when you have this app installed that makes you concerned? Please, name all concerns you might have. *(free text)*
- (4) How can you envision that your concerns will be **reduced**? *(free text)*
- (5) The *[scenario app name]* is very **helpful** in this scenario. *(Continuous slider ranging from Strongly disagree to Strongly agree)*
- (6) I would definitely **use** such an app in this scenario. *(Continuous slider ranging from Strongly disagree to Strongly agree)*
- (7) Do you have any additional feedback regarding this situation? *(free text)*

A.9 Specific Concerns

Finally, we are now going through the scenarios a second time for some more detailed questions. Afterward, you have finished this questionnaire.

This section was prompted another four times, once for each scenario (randomized). The current scenario was presented on the top of the page again for repetition.

All items are continuous sliders ranging from Strongly disagree to Strongly agree.

- (1) When I am using the *[scenario app name]*, I am strongly concerned about **local data processing** (the data is processed locally on your smartphone)
- (2) When I am using the *[scenario app name]*, I am strongly concerned about **global data processing** (the data is processed remotely - it gets sent to servers outside of your home network)
- (3) When I am using the *[scenario app name]*, I am strongly concerned about **local data storing** (your data is stored locally on your smartphone)
- (4) When I am using the *[scenario app name]*, I am strongly concerned about **global data storing** (you data gets sent and stored on remote servers)
- (5) When I am using the *[scenario app name]*, I am strongly concerned about **1st party data access** (the app company has access to your data)
- (6) When I am using the *[scenario app name]*, I am strongly concerned about **2nd party data access** (the smartphone manufacturer has access to your data)
- (7) When I am using the *[scenario app name]*, I am strongly concerned about **3rd party data access** (entities outside of the device manufacturer or app company having access to your data)
- (8) When I am using the *[scenario app name]*, I am strongly concerned about **profile building**, e.g. for targeted advertisements (your data gets analyzed to draw conclusions about your person)
- (9) When I am using the *[scenario app name]*, I am strongly concerned about my **data being misused** by the app company for purposes I am not aware of
- (10) When I am using the *[scenario app name]*, I am strongly concerned about the **app inferring further information** about myself from the data
- (11) When I am using the *[scenario app name]*, I am strongly concerned about my **smartphone inferring further information** about myself from the data
- (12) When I am using the *[scenario app name]*, I am strongly concerned about the **app company inferring further information** about myself from the data
- (13) When I am using the *[scenario app name]*, I am strongly concerned about my **data getting stolen** by a third person
- (14) I am very concerned about this scenario.
- (15) Use this field if you have any additional feedback regarding this situation. *(free text)*

A.10 General Feedback

(1) This is the end of the survey. If you have any further feedback, this is the last spot where you can let us know. *(free text)*

A.11 Scenarios

The following four scenarios were used in the questionnaire above

A.11.1 Navigation App.

scenario app name: navigation app

scenario description: Imagine you are driving a car to a new friend's place that you've not been to yet. You are using a navigation app on your smartphone. It uses your location for navigation and transmits location and movement speed to a remote server to detect traffic jams and thereby improve the routing for yourself and other users.

A.11.2 Sports & Fitness.

scenario app name: sports & fitness journaling app

scenario description: Imagine you are entering activity and vital data into a smartphone app daily, to keep track of your fitness. That is a record of the sports you've been doing, how much you were walking or biking approximately on that day, and a heart rate value which you measure with a separate heart rate measurement device every evening before going to bed. The data is transmitted to a remote server, so that you can access it from both your smartphone and a web app.

A.11.3 Ambient Noise.

scenario app name: ambient noise warning app

scenario description: In everyday life one is exposed to loud noise (e.g., emitted by cars, noisy offices, ...), which can be unhealthy. To become aware of that you install a smartphone app that passively senses the volume via the smartphone's microphone all day, and gives warnings when you are exposed to loud noise for a period of time, to protect your health. The app also displays statistics about the average ambient noise exposure across all users of the app, to help you compare your noise exposure level. Therefore the app transmits your noise values to a remote server of the app company. Besides the installation, you don't have to do anything, and the app does not affect your smartphone's battery and mobile data.

A.11.4 Travel Advice App.

scenario app name: travel advice app

scenario description: Imagine that you are in a foreign country where you enjoy visiting new places and restaurants. To choose places to visit you make use of a travel advice platform app, where users are rating places publicly. To gain full access to all ratings, you are also frequently engaging in posting ratings for places you have visited yourself. Therefore you install an app on your smartphone. A rating contains a description of what you did at the place, how you judge the experience and quality of the service, and one or more photos. By posting ratings publicly, you gain the ability to read other people's ratings.

B Interview Guideline

B.1 Introduction

Good afternoon, thank you very much for agreeing to do this interview with me. Today we'll be talking about smartphone data collection on your users and the issues of user privacy and security. Feel free to take your time to answer in detail, and at one point or another, I may ask some interposed questions. Before we begin, I would ask you to sign the following consent form. If there are any unanswered questions about this, please let me know.

B.2 Determine the level of knowledge of the users

(1) What data do smartphones and their apps collect about their users?
    - Can you think of any others?

(2) Now let's go through the data they said through one by one. What is this data being used for? And what consequences could that have?
  - What exactly do you think for? Can you give an example?

(3) Do you think that smartphone users have an influence on what and how much data is collected/used by your smartphone? If yes, to what extent?

B.3 Find out and structure user concerns and fears

(1) *Once for all mentioned datatypes:* How do you feel about this data being collected with smartphones?

(2) *For all mentioned fears:* Why do you have these concerns/fears OR why do you not have concerns?
  - Are there certain situations in which you feel anxious? If yes, which ones? What are the reasons for these concerns/what are these concerns based on?

(3) Possible concerns are certainly not equal. Reflecting on this, do you find collecting certain data more concerning than others? [Have data sorted] While you are sorting, can you please explain what you are concerned about when sorting?
  - Can you please reflect on the reasons for sorting?

B.4 Examine mitigating factors + knowledge of protective measures

(1) Do you have strategies (behaviors) that you use to reduce potential risks?
  - In which situations? *[Hint only if necessary] e.g. deny apps permission to do something, disable location services?*

(2) What safeguards do you know about to protect your data?
  - Which of these do you follow as well?
  - Why don't you follow the others?

(3) Would you like to know better about your smartphone's data collection?
  - Which aspects are exciting for you?
  - In what format would this knowledge need to be made available to you for it to reach you?
  - At which points would additional information be useful/?

(4) Are there factors over which you as a user have no control that would influence your concerns/fears? If yes, which ones?
  - What would help make you feel better about it?

(5) We're also slowly coming to the end of the interview. Are there any other things about smartphone data usage that we haven't discussed yet?

(6) Do you have any final questions or comments about the interview?

Thank you again for the interview.