Investigating How Users Imagine Their Personal Privacy Assistant

Alina Stöver
TU Darmstadt
Darmstadt, Germany
alina.stoever@tu-darmstadt.de

Sara Hahn
TU Darmstadt
Darmstadt, Germany

Felix Kretschmer
TU Darmstadt
Darmstadt, Germany

Nina Gerber
TU Darmstadt
Darmstadt, Germany

ABSTRACT

Personal Privacy Assistants (PPAs) can support users in managing their privacy. Conducting a user study, we provide qualitative and quantitative insights into how users imagine their PPA and how PPAs designs can appear for different user groups. We highlight five aspects derived from the literature that are essential when designing a PPA: What features should the PPA have? How should the PPA learn the users' preferences? What level of user involvement in its decisions should the PPAs have? Which vendor should offer the PPA? What data are users willing to disclose to their PPA? Our results provide a holistic view of user perceptions of PPAs. We identify two user groups that differ in their characteristics, such as technology affinity and privacy concerns, and have different ideas of a PPA in terms of automation level and provider, for example. We discuss our results in relation to the literature and derive recommendations for designing PPAs to fulfill user needs.

KEYWORDS

Personal Privacy Assistant, User Study, Interview, Privacy by Design, User Perception

1 INTRODUCTION

For many users, protecting their digital privacy remains a challenging task. So-called Personal Privacy Assistants (PPAs) are a promising approach to help users manage their privacy. The research literature already contains various concepts [8, 25, 53], prototypes [34, 38], and real world systems [1, 39] of PPAs for different contexts, such as online social networks [12, 38, 39], Internet of Things (IoT) devices [5, 9, 10, 19, 49] or mobile app permissions [34, 43, 45]. Previous studies have tended to focus on specific aspects of the PPA such as its functionality [31] or level of automation [8]. Moreover, users have mostly not been involved in the design of PPAs from the outset, but have only been asked for their opinions on prototypes or finished PPA designs already developed without user involvement as part of evaluation studies. However, this does not correspond to the user-centered product development process long established in UX design [23], which is intended to ensure that a product is designed precisely according to the needs of users and therefore takes them into account in all steps. We fill this gap by taking a holistic user-centered approach, which is state of the art in product development and begin by raising the research question:

- RQ 1: *How do users imagine their PPA?*

Answering this question will lead us to better understand the user context, the users' needs and perceptions. Previous research suggests that users differ in their perceptions of a PPA and one solution may not fit all [40, 46, 53]. Therefore, we investigate the existence of different user groups by answering the research question:

- RQ 2: *How do different user groups imagine their PPA?*

We picked mobile app permissions as a use case, because it is an everyday use case that is relevant for a broad target group and at the same time generic enough to derive implications for other contexts. To address our research questions, we first reviewed the literature and then conducted a user study. *(1) Literature Analysis:* We deeply analyzed the existing literature on PPAs and derived five essential aspects to consider when designing PPAs: functions and features of the PPA, preference learning of the PPA, level of user involvement in the PPAs decisions, vendor of the PPA, and data disclosure to the PPA. *(2) User Study:* We mapped the five aspects mentioned above in the form of stations in an online survey. For an overview see Figure 1. In these stations, we asked 636 participants in total to design their PPA. To ensure that participants understood the material and to understand the background to their design decisions, we initially accompanied 12 participants in the process with in-depth interview questions as part of a pilot study. The results indicate that users primarily want their PPA to set privacy settings for them and notify them of harmful app accesses. The preferred way for the PPA to elicit participants preferences is to use a questionnaire. Most participants consider a national hacker association to be the vendor of their PPA. Participants are most likely to disclose their data if they see a point in doing so, such as providing information about the purpose of their PPA. However, different users also imagine their PPA differently. Our analyses reveal two groups that differ significantly in a variety of user characteristics (e. g., age and privacy concerns) and their ideas about PPA design (e. g., level of user involvement, vendor, data disclosure). The contributions of this work are fourfold:

Proceedings on Privacy Enhancing Technologies 2023(2), 384–402

https://doi.org/10.56553/popets-2023-0059

- We provide a deep analysis of the literature on PPAs and a synthesis on five essential aspects to consider when designing PPAs.
- Building on the literature, we explore the design space of PPAs and present a holistic picture of how users imagine their PPA.
- We identify two statistically significantly different user groups and show their different ideas of a PPA.
- We show how different elements from the design space for PPAs can fulfill psychological needs of the users. Based on this, we give concrete recommendations for the design of the PPA to fulfill user needs and contribute to a positive user experience.

2 RELATED WORK

We have carefully analyzed the literature on Personal Privacy Assistants (PPAs) and derived five aspects that we think are essential to consider when designing PPAs: functions and features, preference learning, level of user involvement in the PPAs decisions, vendor of the PPA, and data disclosure to the PPA. In the following, we provide an overview of related work on PPAs and go on to review research on the aspects mentioned above.

2.1 Personal Privacy Assistants (PPAs)

Privacy is according to Westin [57, pg.7] *"the claim of individuals [...] to determine for themselves when, how, and to what extent information about them is communicated to others"*. However, users face a variety of challenges when trying to enforce this claim. These include a feeling of being overwhelmed [3], and a lack of awareness and knowledge by users of how they can protect their privacy [51]. PPAs are a promising approach to address these issues. These are systems that know the intentions of their users and support them in managing their privacy in their own interests [8, 54]. They are usually web applications [39] or applications that users install on their devices, such as smartphones [9].

One example for a PPA stems from Sadeh et al. [48]. Their PPA is a mobile app that allows users to discover and control what data is collected about them by Internet of Things (IoT) technologies in their environment. The PPA shows on a map the IoT devices, such as cameras, in the user's neighborhood. Beside this example, the research literature already contains various concepts [8, 25, 53], prototypes [34, 38] and real world systems [1, 39] of PPAs for different contexts, such as Online Social Networks (OSN) [12, 38, 39, 54], IoT devices [5, 9, 10, 19, 49] or mobile app permissions [34, 43, 45]. Despite of proposing design [43] and digital architecture [45] solutions for mobile app permissions, there is either a lack of a generalized design space [43] or the user's perspective remains quite unnoticed [45]. To account for this, in our study we will derive a design space for PPAs from related work and explore the user perception of the various aspect concerning a PPA design. By deriving a design space for PPAs and extensively analyzing the literature on PPAs we propose functions and features that are necessary and demanded by users.

Previous studies have focused on different aspects of PPAs, such as their functionality [31], their level of automation [8] or ways to learn users' preferences [40]. However, the number of studies on user perspectives on PPAs is limited. Notable studies come from Liu et al. [34], Colnago et al. [8], and Stoever et al. [53] that each follow a different methodological approach.

In a field study Liu et al. [34] showed the effectiveness of PPAs for mobile permission management when tailored to specific user groups, in this case tech-savy and privacy-conscious participants. For their PPA, they first developed privacy profiles for users, then determined which profile best fits each user, and finally determined mobile app permissions based on the selected profile. Further they provide evidence that profile-based recommendations are found helpful by users. Adding to this, in our study we examine how a broader range of users perceives preference learning giving important insights for developing user profiles and preference learning.

Using semi-structured interviews with 17 participants, Colnago et al. [8] investigated how users perceive PPAs with different levels of automation and expanded on the work of Liu et al. [34]. They find *"that participants weigh the desire for control against the fear of cognitive overload"* [8, pg.1] when choosing the automation level of the PPA and recommend modular PPAs with configurable levels of automation. As this finding shows the importance to pay attention to the users' needs in developing a PPA, it is only applicable to the three investigated hypothetical implementations with increasing levels of automation. While Colnago et al. [8] focus on qualitative findings through interviews, we complement their qualitative insights into user's perception of the three investigated implementations with a large-scale quantitative study. We take up the aspect of automation in terms of different user involvement in PPA decisions and look at both qualitatively and how it relates to other design aspects of a PPA.

Providing a novel research approach, Stoever et al. [53] explored in a pilot study with help of a user workshop users' perceptions on different aspects of a PPA. Their results give a hint that different user types have different ideas about their PPA. Following up on this, in research question RQ2, we investigate how different user groups imagine their PPA and identify two user groups (Pragmatists and Fundamentalists) which follow Westin's privacy classification [29, 57].

The given diversity of literature on PPAs suggests that there are a variety of aspects to consider when designing a PPA. Although there is evidence that it is important to consider different PPA aspects together from a user perspective because they influence each other [19], this has been little researched (e. g., [34]). We have analyzed the literature on PPAs in depth and clustered it into five aspects that we believe are essential to consider when designing PPAs. These aspects are the starting point for the five stations that form the core of our pilot and main study and are now described below.

2.2 Functions and Features of the PPA

PPAs can fulfill different functions. Functions describe the goal that a product should fulfill. Features are the implementations of functions [11]. We analyzed the literature on PPAs and assigned the features studied therein to a total of five functions. An overview of the extracted functions and features can be found in Table 1. These five functions with a total of ten associated features (see Table 1) form the basis for Station 1 of the user study.

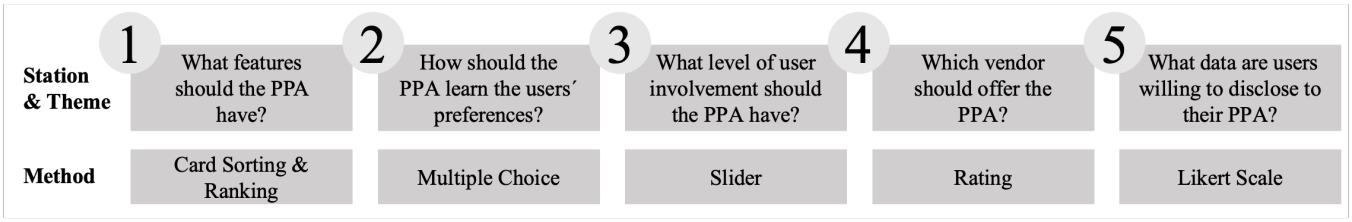

Figure 1: The figure shows the five stations with themes covered and methods used. The stations form the basis for the pilot and main study.

Table 1: Functions and features of a PPAs derived from the literature.

Functions	Features	Literature
Setting configuration: Wherever privacy settings are possible, the PPA sets them in the user's interest.	**Setting configuration**: Wherever settings are possible that affect the user's privacy, the PPA sets them in their interest.	[5, 34]
Support with decisions: The PPA helps the user to make their decisions in line with their privacy preferences.	**Indicator**: Privacy indicator that rates apps in the store. **Reminder**: Reminder of personal privacy preferences. **Recommendations**: Step by step guide for privacy settings.	[27, 52] [34] [19, 34, 39]
Create awareness: The PPA informs the user when their privacy is violated or not fulfilled in their sense.	**Notification - apps**: Notifications when applications want to access privacy compromising information. **Notification - devices**: Notification about devices in the user's environment that could affect their privacy. **Statistics**: Statistics about the user's privacy behavior.	[1, 34] [8, 10, 37, 42, 49] [2, 34]
Teach knowledge: The user can use their PPA to learn how to better protect their privacy.	**Learning units**: Learning units about privacy.	[14, 19]
Motivate: The PPA motivates the user to manage their privacy.	**Praise**: Praise for privacy-relevant behavior. **Gamification**: Gamification in form of privacy challenges and rewards.	[26] [14]

2.3 Preference Learning of the PPA

For optimal personalized functionality, the PPA can learn users' preferences and create a profile based on it [33–35, 39]. Here, the literature also provides multiple possibilities:

- *Data:* The PPA determines the users' preference based on the data they provide to them [44].
- *Automatically:* The PPA automatically determines the users' preference based on the existing permissions for the users' apps [30, 38, 54].
- *Questions:* The PPA determines the preferences based on questions [34, 44].
- *Fictitious Scenarios:* The PPA provides the users with fictitious scenarios with decision options, which are used to determine the users' preferences [21].
- *Select Profile:* The PPA presents profiles to the users to choose from [5]. These profiles can be based on Westin's personas (Fundamentalist, Pragmatist, and Unconcerned) [29, 57].
- *Notifications:* The PPA provides the users with fictitious notifications with decision-making options to determine their preference [34].

These six possibilities of how the PPA can learn users' preferences serve as the basis for Station 2 of the pilot and main study.

2.4 Level of User Involvement in the PPAs' Decisions

Related work shows, that the level of user involvement in the decisions of the PPA can range from high involvement, where the PPA is little automated (e. g., [24, 38]) to low involvement with a fully automated PPA (e. g., [58]). An example for high user involvement is described by Kasaraneni et al. [24]. Their self-learning privacy assistant gives users a privacy score at the moment they want to share information, and users can then decide whether or not to proceed. An example of low user involvement is Wijesekera's [58] approach, whose goal is to automatically make privacy decision without the user's intervention. Colnago et al. [8] investigated user perceptions of different levels of automation in PPAs and recommended that approaches are needed that address the differing automation preferences of users. In Station 3 of our study, we will therefore investigate what level of involvement in the PPAs decisions users prefer. We also aim to set these involvement preference in the context of various other PPA aspects.

2.5 Vendor of the PPA

Colnago et al. [8] found that users desire the possibility to choose the source of the PPAs recommendation. Also, Stoever et al. [53] suggest that the vendor's intent plays a role. Vendors can be large tech companies with different geographic locations (Europe, North America, Asia) with different products (telecomunication providers, OSNs, smartphone providers), NGOs, privacy activists, companies already offering a PPA, government organizations, or research institutions. In Station 4 of our pilot and main study, we want to shed light on which providers users prefer and why.

2.6 Data Disclosure to the PPA

Research shows that certain user data, e. g., extracted from Facebook posts [44], can be helpful to build a user profile and thus creating a helpful PPA. However, users are not always willing to share their data and differentiate which data they share and with whom [20]. What data users are willing to share with a PPA is still unclear and will be investigated in Station 5 of our study.

3 METHOD

We conducted a survey study to quantitatively explore the design space for a PPA (RQ1). Furthermore, we were interested in whether different user groups have different preferences for their PPA (RQ2). We first conducted a qualitative pilot study to gain a deeper understanding of users' ideas about the PPA. In this pilot study, we used think aloud and semi-structured interviews to understand why participants make certain choices when designing their PPA. Since we used the survey questionnaire as basis for the interviews, the pilot study also served to ensure that the study material was understandable and complete. In the following, we first introduce the method of the pilot study and then present in detail the method of the main study.

3.1 Pilot Study

In the following, we present the study procedure, information on data collection, data analysis, recruitment and participants and ethical considerations of the pilot study.

3.1.1 Procedure. The core of the pilot study is the online survey used in the main study (see Section 3.2 for details), which participants answered in a one-on-one interview setting using think aloud. In addition, the participants were asked several semi-structured interview questions before, during, and after completing the survey. We used think aloud, where a researcher encouraged the participants to speak out their thoughts while completing the study, to assess participants' understanding of the study material. The interview questions aimed to gain deep insights into the thoughts and decisions of the participants. For the survey and interview questions, the reader is referred to Appendix A. The entire study materials can be found here [55].

3.1.2 Data Collection and Analysis. Interviews were conducted remotely [36] using the Zoom video-call tool and recorded using Zoom's recording function and stored locally only [60]. The interviews lasted between 22-46 minutes. The responses from the five stations and the final questionnaire were collected using the online survey tool SoSci Survey [32]. We manually transcribed the audio recordings of the interviews into written form. We then conducted a thematic analysis following six phases suggested by Braun and Clarke [5] and using MAXQDA as software support [56]. First, one researcher went through all transcripts and coded the data on the sentence level to iteratively develop a codebook, going back and forth several times. The codebook was then discussed with another researcher and refined throughout the discussions. Then, two researchers independently coded the interview transcripts using the final codebook. Discrepancies between the results of the two coding runs were discussed and codes were adjusted accordingly. The codebook with its themes and categories can be found in Appendix B. For the descriptive analysis of the survey responses, we used SPSS [22].

3.1.3 Recruitment and Participants. To recruit participants, we designed a flyer that we distributed online and offline. For this we used mailing lists from our university, forum postings, local pin boards, and our personal network. As a prerequisite for participation, we specified that participants must be at least 18 years old and had access to a computer with Internet and audio out and in. Technical knowledge was not required. We offered to help with setting up the video conference, which some participants took advantage of. Participants were paid with 15€ for their participation with an average completion time of 34 minutes. Compensation was more than the minimum wage of 9.60€ in Germany at the time the study was conducted. The sample consisted of 12 participants residing in Germany. We stopped recruiting for the study because we already reached data saturation after the tenth interview. Eight of them identified as women and four as men. Four participants were full or part-time employees, two were self-employed and five were unemployed, retired or in education. Three participants were between 21-25 years old, two between 26-30, one between 31-35, one between 56-60, three between 61-65, one between 66-70 and one older than 70. All participants owned a smartphone. The technological affinity of the sample was $MD = 3.83$ out of 6 points (min=1.11, max=4.55, SD=1.10). The sample's privacy concerns were out of 7 points $MD = 7$ for all three subscales (control min=3, SD=1.14; collection min=3, SD=1.14; awareness min=6, SD=0.28).

3.1.4 Ethical Considerations. The study follows the guidelines of the ethics committee of our institution that also provides a comprehensive checklist for the review of the research project. To protect participants' privacy, we limited the collection of personal data to a minimal amount. Prior to the study, all participants received a consent form (contained data protection policy), which they had to agree to. All participants were informed that they could quit the study at any time without negative consequences, in which case all their data would be deleted, and ensured that their data was handled only by members of our research group. We furthermore provided the participants with contact information from the examiners and researchers, so participants could also reach out to them after study completion. The survey data was only stored on national servers that comply with national privacy regulations. Although we used a video-call tool, participants had the opportunity to turn off the camera for the interview. Furthermore, the data was anonymized during the transcription process. Recordings were only stored locally on computers of the research team and deleted after transcription. The study complied with national privacy regulations.

3.2 Main Study

After the exploratory nature of the pilot study, which was intended to provide qualitative insights into participants' design choices and ensure that the material was understood and complete, the goal of the main study was to gain quantitative insights into our research questions: (RQ1) How do users envision their PPA and (RQ2) How do different user groups imagine their PPA? In the following, we present the study procedure as well as information on data collection, data analysis, recruitment and participants and ethical considerations.

3.2.1 Procedure. After agreeing to the consent form, we asked participants to answer some preliminary questions, including their demographics and the Technology Affinity Scale [13]. Afterwards participants received an introduction about the goal of the study and a general definition of a PPA (see Appendix A). Using a survey questionnaire, we asked participants to create their PPA within five stations (see Figure 1). The implementation of the five stations was identical in both studies. We learned from the pilot study where participants had problems understanding our instructions and made small adjustments in the instructions for the main study. For example, in Station 4, we noticed that it was easier for participants to understand if we asked 'Who should develop the PPA?' instead of 'Who should offer the PPA?'. In the main study, the instructions were also written, in contrast to the pilot study. Furthermore, we made an adjustment in the main study in station 5, where we asked participants to rate what data they would disclose to the PPA using a 7-point Likert scale instead of a 5-point scale (as in the pilot study) to better represent possible variances. In contrast to the pilot study, participants in the main study received additional survey questions instead of the final interview. Finally we included the Internet User's Information Privacy Concerns (IUIPC) 8 Scale [17] to measure participants' privacy concerns. The survey questions are in Appendix A. The entire study material can be found here [55]. The basis of the participatory interviews is formed by five stations covering five essential aspects of a PPA, which we derived from the literature. The five stations are now described below.

Station 1: Features of the PPA In Station 1, the participants should determine what features their PPA should have. We decided to focus on features because they are more concrete and relevant for the participants than functions. We first asked participants to assign images of various features to a category (absolutely desired, nice to have, do not need) using drag and drop. In the second step, participants were asked to prioritize the features that their PPA absolutely must have. All features from which participants could choose were derived from the literature. An overview can be found in Table 1, an example illustration in Figure 2.

Station 2: Preferences Learning of the PPA In Station 2, participants explored ways how the PPA could learn about their privacy preferences and create a privacy profile. To do this, they were able to select the option that appealed to them most from six illustrated options: data, automatically, questions, fictitious scenarios, notifications. For an example see Figure 2.

Station 3: Level of User Involvement in the PPAs' Decisions In Station 3, we asked participants to use a slider to set their preferred level of involvement in the PPAs decisions between 1 (no automation) and 101 (full automation). No automation means that the PPA is in constant contact with the user, informs them about every decision and always involves them. Full automation means that the PPA runs in the background and the user does notice as little of the PPA as possible.

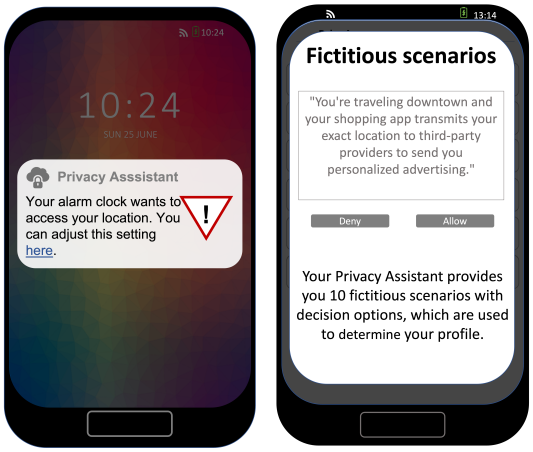

Figure 2: The figure shows examples of design choices in Station 1 (Feature: Notification - apps) and Station 2 (Preference learning: Fictitious scenarios).

Station 4: Vendor of the PPA In Station 4, 12 different vendors (including a short description) who could possibly provide the PPA were presented to the participants. Participants were asked to rate which vendor they consider more trustworthy and which less trustworthy and finally chose a vendor for their PPA. The possible vendors were large tech companies with different geographic locations (Europe, North America, Asia) with different products (telecommunication or smartphone providers, OSNs), NGOs, privacy activists, companies already offering a PPA, governmental organizations, and research institutions. For the detailed and complete list of vendors, see Appendix A.

Station 5: Data Disclosure to the PPA In Station 5, we asked participants to determine the data they are willing to disclose to their PPA. This data is used by the PPA to generate a user profile and thus to fulfill its function more optimally. Using a Likert scale, we assess the extent to which participants are willing to disclose the following data to their PPA: demographic variables, identity, personality traits, knowledge of data protection, purpose of the PPA, organizations about which they have privacy concerns, and information from OSN profiles.

3.2.2 Data Collection and Analysis. The survey was implemented using SoSciSurvey [32]. For the analysis of the survey responses, we used SPSS Version 28.0.1.0 [22] to perform descriptive and inferential statistical analyses.

3.2.3 Recruitment and Participants. The participants were recruited via the online participant recruitment platform Clickworker [16] with random sampling within the country's population to achieve heterogeneity in terms of the participants' gender, age, education and location. Our research questions are purely exploratory and do not involve any concrete hypotheses. Therefore, we did not perform

any sample size calculations in advance. However, we wanted to have a large enough sample to increase the likelihood that the data set would include participants with different preferences and allow for exploratory analysis. The study took on average 14 minutes to complete, and participants received 2.38€, which corresponds to an hourly rate of 10.20€ and thus exceeds the minimum wage of 9.60€ in Germany at the time the study was conducted. A total of $N = 705$ German participants took part in our study. A total of 69 participants were excluded because they did not complete the questionnaire, their response time was particularly short, or they did not pass the attention checks. From the final sample ($N = 636$) a total of 265 identified as women, 362 as men, six as other/diverse, and three did not specify their gender. All participants were at least 18 years old with the following distribution: 191 were between 18 and 30, 192 were between 31 and 40, 111 were between 41 and 50, 101 were between 51 and 60, and 41 over 61 years old. In terms of education, 0.3 % had not finished high school, 55.8 % had finished school, and 44.2 % held a university degree. The technological affinity of the sample was $M = 4.22$ ($SD = 0.92$) out of 6 points. The sample's privacy concerns were out of 7 points $M = 5.6$ ($SD = 1.18$) for the subscale control, $M = 6.26$ ($SD = 1.01$) for the subscale awareness, and $M = 5.53$ ($SD = 1.22$) for the subscale collection.

3.2.4 Ethical Considerations. We took the same ethical precautions for the main study as for the pilot study. For more details see Section 3.1.4. Furthermore, we did not conduct video-calls in the main study. Participants were provided with contact details at the first page of the survey questionnaire (informed consent) to give them the opportunity to ask questions.

4 RESULTS

In the following, we present the results of our studies. First, we describe how participants imagine their PPA (RQ1) along the five stations. This is followed by the results on differences between user groups (RQ2). We present both the quantitative results of the main study and the qualitative ones that emerged from the thematic analysis of the pilot study. The codebook of the thematic analysis can be found in Appendix B.

4.1 RQ1: How do Users Imagine their PPA?

4.1.1 Features of the PPA. In Station 1, we asked participants to use card sorting to rank various features as to whether they desire them. Figure 3 provides an overview of which features participants of the main study would like to see in their PPA, which they consider to be nice to have, and which they do not need. The majority of the participants would like their PPA to notify them if an app accesses information that threatens their privacy (72.4 %; $N = 557$) and sets privacy settings for them (70.2 %; $N = 553$). The notification feature is ranked as the most important function of their PPA by 36.7 % of respondents (see Table 2). On the other hand, most respondents do not want features such as praise (53.3 %) and gamification elements (53.8 %). These wishes are also reflected in the results of the thematic analysis of the interviews conducted in the pilot study, in which participants distinguish between awareness-focused and support-focused aspects of their PPA. Among the awareness aspects, most participants feel it is important that their PPA keeps them informed, Participant (P) P07: *"that's basically the point of a privacy assistant for me, that I want to know when someone is maybe somehow or why influencing my privacy"*. This applies especially to critical situations. Thus, the PPA should create transparency and for some participants take on the function of a learning guide. Like P11 expresses *"Then I also always learn something through my PPA"*. Regarding the supportive aspects of their PPA, participants express the desire, that their PPA should support them by remembering privacy decisions made, reducing complexity, and providing situational support, e. g., when downloading an app.

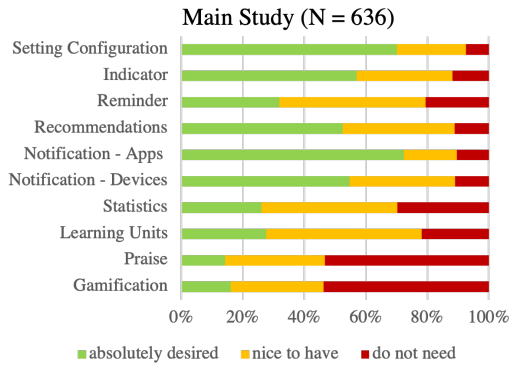

Figure 3: The figure shows the results of Station 1 (preferred features) from our main study.

Table 2: Results of Station 1: Number of participants who rated the feature as the most important. The percentage of the total sample ($N = 540$) is given in parentheses. For technical reasons, it was not possible to save the answer to this question for all participants, so the sample size here differs from the other questions.

	Main Study (N=540)
Setting configuration	151 (28.0 %)
Indicator	42 (7.8 %)
Reminder	8 (1.5 %)
Recommendations	55 (10.2 %)
Notification - apps	198 (36.7 %)
Notification - devices	35 (6.5 %)
Statistics	14 (2.6 %)
Learning units	15 (2.8 %)
Praise	12 (2.2 %)
Gamification	10 (1.9 %)

4.1.2 Preferences Learning of the PPA. An important question is how the PPA learns users' privacy preferences. An overview of the results can be found in Table 3. In Station 2, we asked participants to select the preference learning approach that most appealed to them. The option that the PPA asks questions (33.8 %; $N = 363$) was the most favored, followed by the option to choose a profile (19.3 %; $N = 363$). Automatic learning based on previous behavior was chosen by only a few (7.1 %; $N = 363$). The interviews of the pilot study

reveal that participants reject this option because their (previous) behavior does not necessarily reflect their privacy wishes. When determining preferences, it is important to some of the interview participants that they are not forced into a profile and that they have the opportunity to readjust their settings.

Table 3: Results of Station 2: Number of participants who chose the corresponding design as their preferred design for how the PPA should learn their privacy preferences. The percentage of the total sample (N = 636) is given in parentheses.

	Main Study (N=636)
Data	60 (9.4 %)
Automatically	45 (7.1 %)
Questions	215 (33.8 %)
Fictitious scenarios	88 (13.8 %)
Profile	123 (19.3 %)
Notifications	105 (16.5 %)

4.1.3 Level of User Involvement in the PPAs' Decisions. In Station 3, we asked participants to use a slider to set their preferred level of involvement in the PPA decisions between 1 (no automation) and 101 (full automation). No automation means that the PPA is in constant contact with the user, informs them about every decision and always involves them. Full automation means that the PPA runs in the background and the user does notice as little of the PPA as possible. Participants indicated that, on average, they would like to be moderately involved in their PPAs decisions (M = 54.02; SD = 30.19; N = 621). However, looking at the distribution of the answers, as shown in Figure 4, there seem to be two groups here: Participants who prefer to be more involved (low automation) in their PPAs decisions and participants with a desire for less involvement (high automation). A more detailed description of the two groups can be found in Appendix B. The thematic analysis of the interviews in the pilot study reveals that some conditions must be met for participants to accept automation of the PPA. These include the fundamental trust of the user in the PPA. Trust is also influenced by the transparency and the perceived reliability of the PPA. Furthermore, it is important to the interviewees to retain control over the PPA, but they are willing to accept an increase of automation over time, when the PPA has learned the preferences. Participants differentiate which aspects of the PPA they would like to be more and less automated. Especially in time-critical situations, e. g., downloading an app on the go, and for recurring decisions, the participants tend to want more automation. When determining privacy preferences and making important privacy-relevant decisions, participants prefer to be more involved.

4.1.4 Vendor of the PPA. In Station 4, participants were asked to assess the trustworthiness of potential PPA vendors and select their favorite one. The final vendor selected most often in the main study was a national hackers organization (28.1 %; N = 629) followed by a national university (26.9 %; N = 629) and least often Facebook (0.3 %; N = 629), whereby the national university was most often (92.7 %; N = 565) rated as trustworthy. For more detailed results see

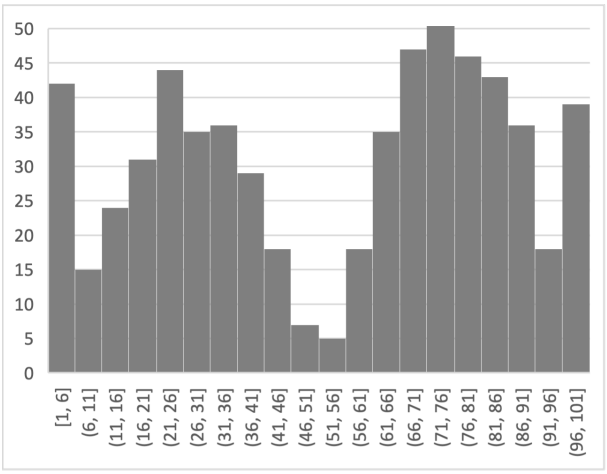

Figure 4: The figure shows the results of the main study from Station 3: Distribution of frequencies of desired involvement (1 - high involvement/no automation to 101 - low involvement/full automation).

Table 4: Results of Station 3: Average level of involvement that participants overall, the low automation/high involvement group, and the high automation/low involvement group, desire from their PPA.

	Main Study
Overall involvement	M = 54.02; SD = 30.20; N = 621
High involvement (<51)	M = 23.5; SD = 12.97; N = 277
Low involvement (≥51)	M = 78.5; SD = 12.6; N = 344

Appendix B. The thematic analysis of the interviews of the pilot study reveals that trustworthiness, along with competence, is the central criterion considered when deciding on a vendor. Factors influencing trust in a vendor are diverse and range from participants' gut feelings, which are influenced by the vendor's brand image, for example, to the vendor's perceived independence (e. g., from undemocratic governments). The vendors's business model (user data as a central element) and the general handling of data also play a role here.

4.1.5 Data Disclosure to the PPA. In Station 5, we wanted to find out what data users are willing to share with their PPA to ensure that it functions optimally. To do this, they were asked to rate items on a Likert scale from 1 (strongly disagree) to 7 (strongly agree). In order for the PPA to function optimally, participants are on average most willing to disclose the purpose for which they want to use the PPA (M = 3.93; SD = 1.032; N = 623) as well as the organizations about which they have privacy concerns (M = 3.86; SD = 1.123; N = 627). They are less likely to disclose information from their online social media account (M = 2.70; SD = 1.283; N = 617) and their identity to the PPA (M = 2.84; SD = 1.314; N = 626). For more detailed results, the reader is referred to Appendix B. The interviews show that participants express a general desire that their PPA uses

and collects as little data as possible - also because they are afraid of data misuse. Related to this, some participants do not want service connections through the PPA (e. g., the connection of their social media profile). Participants are not willing to disclose their data if they do not see the point or added value in it.

4.2 RQ2: How do Different User Groups Imagine their PPA?

To answer our RQ2, we chose an exploratory approach. To this end, we first performed cluster analyses [7]. For the analysis of the interval scaled data we used the ward method with squared Euclidean distance. For the analysis of the categorical variables we used a two-step cluster analysis with log-likelihood as distance measure. All variables included, however, we were not able to identify a satisfactory differentiated cluster. Therefore, we used graphical inspection of the results of the pilot and main study as a starting point for further analysis. These showed a bimodal data distribution for the involvement question, indicating two user groups. A binomial logistic regression was performed to determine the effect of age, privacy knowledge, motivation and concerns, and technology affinity and to predict the likelihood of preferring a PPA with high or low user involvement. The binomial logistic regression model was statistically significant, $\chi^2 = 54.87$, $p < .001$., resulting however in a low amount of explained variance [4], as shown by Nagelkerke's [41] $R^2 = .1$. We further analyzed the two groups: If we divide participants from the main study according to their predefined involvement level into a high/low automation (< 51 %; $N = 277$) and low/high automation (≥51 %; $N = 344$) group, we see that they differ significantly with $M = 23.55$ ($SD = 12.97$) in the high and $M = 78.55$ ($SD = 12.59$) in the low involvement group. To explore differences between these two groups, we ran t-test for unpaired samples for interval scaled data and Pearson chi-squared test for lower scaled data. An overview of all values of the significance test can be found in Appendix B. We found statistically significant differences among others in terms of age, technology affinity, motivation to protect their privacy, and privacy concerns of the users (see Table 10). No significant differences appeared between the two groups in terms of gender, highest education, knowledge to protect their privacy and preferred vendor of the PPA. Westin has classified users in terms of their privacy concerns and refers to users with low concerns as Unconcerned, with medium concerns as Pragmatists and with high concerns as Fundamentalists [29]. Our study results show that users who prefer a high-automation PPA report significantly lower privacy concerns, therefore we give this user group the name "Pragmatists" following Westin's classification. The users of the low-automation group, who show rather high privacy concerns, we call "Fundamentalists". In the following, we will describe these two user groups and their PPA designs, focusing only on aspects where the two groups differ significantly. An overview of the user characteristics and PPA design choices of the two groups is provided in Table 5.

4.2.1 User Group 1: Pragmatists. Pragmatists are typically under 30 or over 51 years old, tend to install new apps on their smartphones several times a month, and are less technology affine than Fundamentalists ($M = 4.135$; $SD = .92$). They typically show medium or low motivation to protect their privacy and report on average lower privacy concerns than "Fundamentalists" in all subscales of the IUIPC: control ($M = 5.47$; $SD = 1.15$), collection ($M = 5.33$; $SD = 1.21$), awareness ($M = 6.10$; $SD = 1.09$). As the main feature of the PPA, notification about app access is particularly popular among Pragmatists, but other features such as settings, recommendations, and the privacy indicator are also popular in this group (see Table 10). Among Pragmatists the most popular way for the PPA to learn users' preferences is through questions and some can imagine their PPA learning their preferences automatically. As mentioned above, Pragmatists want their PPA to be rather highly automated ($M = 78.55$; $SD = 12.59$). The the most frequently chosen vendor in the pragmatists group is a university. Pragmatists are significantly more willing to disclose information about their identity, personality traits, and their online social network profile to the PPA. No differences were found between the groups with regard to the willingness to share their age, their knowledge of privacy, the purpose of the PPA, and the organization about which they have privacy concerns.

4.2.2 User Group 2: Fundamentalists. Fundamentalists are typically between 31 and 50 years old, tend to install new apps on their smartphones less than once a month, and are more likely to be technology affine ($M = 4.33$; $SD = 0.92$). They typically show high motivation to protect their privacy and have comparatively high privacy concerns in all subscales: control ($M = 5.81$; $SD = 1.15$), collection ($M = 5.78$; $SD = 1.18$), awareness ($M = 6.43$; $SD = 0.86$). Fundamentalists particularly often want their PPA to inform them about app accesses as the main function (see Table 10). The most popular way for the PPA to learn users' preferences is through questions. While some Pragmatists can imagine the PPA learning their preferences automatically, this variant is not very popular among Fundamentalists. More popular here are the fictitious scenarios. As mentioned above, Fundamentalists want their PPA to be rather low automated ($M = 23.55$; $SD = 12.97$). Among Fundamentalists, a national hacker association is the most frequently chosen vendor. Fundamentalists are statistically significantly less willing to disclose information about their identity, personality traits and their online social network profile to their PPA.

5 DISCUSSION

In this section, we first summarize the findings in comparison with the results of related work. We will then present a design space for a need-sensitive PPA also providing concrete recommendations how to adress user needs in the PPA design.

5.1 RQ 1: How do Users Imagine their PPA?

Functions and Features: Our study shows that most participants want their PPA to create awareness of privacy-prone app access, and furthermore, to set privacy settings for them. This aligns with the findings of Colnago et al. [8], who stated that users have a desire for awareness of privacy violations and at the same time want the control to change this. Surprisingly, the desire for awareness through notifications related to app access for many, and to devices in the environment for only a part of the participants. An explanation could be, that the PPA for mobile app permissions as a study framing could have led to less focus on IoT devices as a potential privacy threat. Our results reveal that in line with Colnago et

Table 5: Differences between the user groups Pragmatists and Fundamentalists in terms of user characteristics and PPA design. Statistically significant differences are marked with *.

	Fundamentalists	Pragmatists
User characteristics	Age: 31-50 years* Technology affinity: comparatively high* Privacy concerns: comparatively high* High motivation to protect privacy* Rarely install new apps*	Age: under 30 and over 51 years* Technology affinity: comparatively low* Privacy concerns: rather low Low or medium motivation to protect privacy* Install new apps more often*
Preferred features	Setting configuration Notification-app	Setting configuration Notification-app
Preference learning	Questions	Questions or profile selection
Level of involvement	High*	Low*
Preferred vendor	Hacker association	National university
Data disclosure	Less willing to disclose information about their identity, personality traits and their online social network profile to their PPA*	More willing to disclose information about their identity, personality traits and their online social network profile to the PPA*

al.'s results [8] participants value educational aspects and perceive their PPA also as a learning guide. At the same time, however, they do not necessarily want learning units, gamification, and praise but would rather learn through context-related demonstration of their own behavior as well as situational presentation of alternative possibilities for action.

Preference Learning: Participants prefer that their PPA learns their preferences through questions. This confirms Lui's [34] approach of assigning users to a preference profile of a PPA using questions. Our study illustrates that participants do not want the PPA to automatically learn their behavior. In the pilot study, we learned that one reason is that participants find that their previous behavior does not reflect what they want. Also Colnago et al. [8] had already found out that for users the source of the recommendations of their PPA is crucial and that already existing user preferences are not considered optimal for this.

Level of User Involvement in the PPAs' Decisions: On average, participants want a medium to lower level of involvement. However, a closer look at the data reveals that there are two groups of users: Users who want a low level of involvement (Pragmatists) and users who want a high level of involvement (Fundamentalists), with a larger group of those who want a low level of involvement. Colnago et al. [8] have already shown that participants differ in their evaluation of the automation level of the PPA. Our results can complement these findings. We could see that the degree of involvement desired by the participants differs in different situations. Especially in the initial preference learning phase users prefer rather high involvement, likewise in critical situations. In recurring decision-making situations they want to be less involved. In addition, certain conditions, especially trust in the PPA, must be met for users before they allow automation.

Vendor of the PPA: Participants most frequently chose a national hacker association as the vendor for their PPA. The interviews show that the vendor plays a central role for the users, which is in line with previous research [8]. Competence and trustworthiness of the vendor influence the decision for a vendor.

Data Disclosure to the PPA: In general, study participants are more willing to share data with their PPA if they see a direct benefit to it, which is in line with previous research [15, 20]. In general, participants demand that their PPA be as data-sparse as possible so that it does not become a privacy threat itself. This is an major requirement for a PPA, which has not been considered in the literature so far. Hence, there is a need to develop methods to capture privacy preferences of users in a privacy-friendly way. That considered together with the desire of some of the participants for highly automated PPAs, reveals a certain trade-off: Users want to protect their privacy while having the convenience of automation.

5.2 RQ2: How do Different User Groups Imagine their PPA?

The pilot study already indicates that there are two different user groups that have different ideas of a PPA. The main study confirms this assumption. Following Westin's privacy classification, we call the first group of users the Fundamentalists, who have comparatively high privacy concerns [29]. The second group, we call Pragmatists, because they report rather medium privacy concerns. The two groups differ statistically significantly in a number of user characteristics (e. g., age, technology affinity) and in their ideas about the design of a PPA (e. g., level of automation, vendor). Classifying users into personas has also proven to be a helpful approach in the context of privacy for developing products that better meet user needs [46]. In the context of PPAs, personas have been successfully used to classify users according to their privacy preferences and to make appropriate privacy settings and recommendations [6, 33, 40]. With our findings on the two user groups corresponding to the Westin personas Pragmatists and Fundamentalists, we go a step further and propose to design PPAs according to the needs of these groups.

5.3 Design Space for a Need-Sensitive PPA

With our study, we aimed to understand what is important to users in the design of a PPA. Underneath the aspects expressed may lie basic psychological needs that users are trying to satisfy [59]. A need is according to Ryan and Deci *"an energizing state that, if satisfied, conduces toward health and well-being but, if not satisfied, contributes to pathology and ill-being"* [47, pg.74]. Hassenzahl et al. [18] follow up on the work of Ryan and Deci [47] and Sheldon et al. [50] and propose seven needs that they consider most important in the context of experience with technology (user experience). These include beside autonomy, competence, relatedness, security, meaning, stimulation, and popularity [18]. Zimmermann and Gerber [59] confirm that users aim to fulfill these needs by using digital applications. While Zimmermann and Gerber [59] show that meeting these needs sometimes overweighs privacy concerns and prevents the use of privacy-friendly alternatives, Kraus et al. [28] reveal that some of the needs - namely autonomy, competence, meaning, and stimulation - can also act as a motivator for security and privacy actions on smartphones. Since a PPA is an application that is intended to promote privacy actions and provide users with a positive experience, we will take a closer look at these needs in the context of a PPA. Based on our results, we summarize the design space we studied for the PPA and show how different design elements can address different user needs. We highlight how these design elements were evaluated by our participants and provide recommendations for the development of a PPA. For this purpose, we refer to the needs proposed by Hassenzahl et al. [18], which we elaborate in the following for the PPA design space:

Autonomy describes the feeling of living according to one's own ideas [18]. For the PPA design, this means the users' feeling of living according to their own privacy preferences. The PPA could support this by setting preferences for users, a feature that was requested by most of the study participants. It is important that users can trust the PPA to act in their best interest. To establish a reliable relationship, our study participants demand that the PPA is transparent about its actions and give them final control to make adjustments. For a PPA to act in the user's interest, it must learn their preference correctly. There are several ways to do this, which we discussed in Station 2. Our results suggest that participant control is particularly important here. This means that the PPA should not necessarily determine preferences automatically, but involve users by asking specific questions or example scenarios. To consider the user need for control in the design of the PPA we recommend the following:

- *Implement privacy settings as a main feature.* As a main feature, the PPA should make privacy settings for users to allow them to live according to their own privacy preferences.
- *Increase the users' trust in the PPA through control and transparency.* Users want the possibility to see what actions the PPA has taken and to adjust them if necessary. This can be implemented in the form of a dashboard, for example.
- *Involve user in the preference learning process:* Users want to understand how the PPA learns their privacy preferences and make sure these are learned correctly. Hence, they want to be involved in the learning process. This can be implemented by using questions to learn the user preferences rather than an automated approach.

Competence is the feeling of being capable and effective [18]. On the one hand, this can mean that users can effectively implement their privacy preferences with the help of the PPA, and on the other hand, they can acquire new privacy competencies through the PPA. The first can happen, for example, through the PPA's recommendations on how privacy preferences can be implemented. This is a feature that many of our study participants rated as desired. When designing this feature, it is important to consider different user types we identified in our data (see Section 4.2) in order not to limit the experience of competence. Pragmatists are characterized by a tendency to have a low affinity for technology and a low motivation to deal with privacy. Here, it could be useful to address the most important settings and to formulate the recommendations in a simple and easy-to-understand manner in order to avoid overwhelming them. The fundamentalists, on the other hand, are more technology-savvy and motivated to deal with privacy. In this case, it may be useful to provide detailed recommendations with technical details in order to enhance the experience of competence. Privacy skills in general can be promoted through the inclusion of learning units. Also, revealing the user behavior through statistics and corresponding recommendations for action can encourage users to reflect and adjust their behavior. These design elements are especially useful for users who see their PPA as a learning companion, as was formulated in our pilot study. To increase the privacy competence of the users, we make the following recommendations for the PPA design:

- *Consider user types when designing recommendations.* The design of recommendations provided by the PPA should take into account the different technical affinities and motivations of users to deal with privacy.
- *Design the PPA as a learning companion for interested users.* A part of the users can imagine the PPA as a learning companion that actively supports them to reflect and adapt their privacy behavior. This can be implemented through statistics that show the user their privacy behavior and suitable recommendations for behavioral changes. The companion should also not need too much attention, e.g. through gamification aspects.

Security relates to the feeling of having pleasant habits and routines [18]. Here, the PPA design is on the one hand about being able to implement the privacy preferences as comfortably as possible. This can be done, for example, by using targeted automation. For example, many study participants can imagine the PPA taking over decisions for them in time-critical situations or those that recur. At the same time, the results of our pilot study show that the PPA's actions must not disrupt familiar routines or the user experience when using other applications. One approach here could be for the PPA to make transparent not only its actions but also possible consequences for the use of other apps. To satisfy the users' need for security, we recommend the following:

- *Allow different levels of automation for different aspects of the PPA.* The desired level of automation varies for users in different situations or use cases. While in time-critical situations and for recurring decisions, the PPA should act as automated as possible, most users want little automation in the first contact with their PPA and for important decisions.

- *Note that the PPA's actions do not interfere with the user experience of other apps.* This wish can be realized, for example, if the PPA transparently shows the user the consequences of its actions. For example, prohibiting location sharing for a navigation app can lead to restrictions, but for other apps it only protects the users' privacy.
- *Minimize data collection of the the PPA and be transparent about its purpose.* Users express concerns that the PPA as such becomes a privacy threat with the data it collects about them. Therefore, they want the PPA to use and collect as little data as possible and not share data.

Meaning is the feeling of experiencing meaningful moments, consciously, personal development or gaining new insights [18]. For the PPA, this can mean making their own privacy behavior transparent to users. For example, in the form of statistics that show how often a user is exposed to a privacy risk. In order to encourage personal development, the PPA can provide the user with concrete, small-step, and individualized options for changing behavior.

- *Avoid overwhelming the user.* Too many notifications or too much information can overwhelm users and lead to fatigue. This can be avoided by the PPA giving an appropriate number of notifications and focusing on information that is particularly relevant to the user. How many and which information users want can also be determined for each user when installing the PPA.
- *Provide the user with concrete and manageable recommendations for action.* To encourage personal development and strengthen their self-efficacy, the PPA should provide concrete and manageable recommendations for action. For example, the PPA can suggest privacy-harming apps that the user does not use to be removed from the smartphone.

Stimulation describes the feeling of discovering new things and getting enough stimulation [18]. In the case of the PPA, this can mean that users are informed about existing privacy threats, gain knowledge about privacy in general or their privacy behavior and are encouraged to reflect and adapt their own behavior. One way to implement this is to provide notifications when an app makes accesses that endanger privacy. This is a function that the majority of the study participants would like to see and rate as the most important function. Stimulation can also be generated through the use of gamification elements, but the majority of the study participants rated this as not needed. Stimulation can also be influenced by the degree of automation of the PPA. If the PPA runs fully automatically in the background and neither involves the user in decision-making nor actively informs them - which is desired by some of the participants - this can mean lower stimulation. Conversely, the PPA can generate targeted stimulation in the user through notifications and information. Here, however, it is important to find an appropriate measure that does not overwhelm or causes fatigue.

- *Implement notifications as a main feature.* Notifications about privacy-threatening app access is an often desired feature that can be implemented as a targeted and helpful stimulation.
- *Take into account different needs for stimulation.* There are users who want to see as little as possible of their PPA and can therefore quickly be overwhelmed or annoyed by stimulation elements such as gamification or notifications. These different needs for stimulation must be taken into account. This can be implemented, for example, by designing the PPA specifically for the user needs of the user types that we have identified in our data.

Relatedness and Popularity: These two needs proposed by Hassenzahl et al.[18] are important in the design of technology, but they appear only in the margin in our data, which is why we discuss them only briefly. *Relatedness* describes the feeling of having regular close contact with other people who care about one [18]. In the PPA design, this can be implemented, for example, through privacy recommendations from friends or challenges with friends. Our study participants do not express a need for gamification elements in the PPA. In general, the need for relatedness was not mentioned much in our participant responses. It would be interesting to see if it plays a role in other use cases or with specific target groups. For example, the issue could become more relevant when parents use a PPA to set privacy preferences for their children. Furthermore, it could be that, e. g., adolescents, who are not represented in our sample, are more open to gamification elements in a PPA. *Popularity* refers to the feeling of being liked and respected and influencing other people with one's own behavior. This need could even be restricted by a PPA, for example, if the PPA makes suggestions for alternative apps such as messenger, which then excludes the user from their social group. When designing the PPA, it is therefore important to ensure that people with a strong need for popularity are not put at a disadvantage.

6 LIMITATIONS AND FUTURE WORK

In our study, we focused on one use case ("Mobile App Permission") in order to avoid overwhelming the study participants. However, this limits the applicability of our results to other scenarios, such as IoT or web browsers. Nevertheless, our findings offer a starting point for further studies in this area, e. g., future studies could use a similar study design again for other contexts. To create an atmosphere in which participants were inspired to design a PPA, we used many different methods, such as card sorting and ranking. With this setting, we were able to gain deep insights in our pilot study. Nevertheless, the statistical analysis of the data of the main study showed major limitations. In addition to Likert items, we used a combination of different participative, interactive methods from the HCI context such as card sorting or ranking to inspire our participants in their design process. However, this also led to categorical, i.e., nominal, data and limits the feasibility for some statistical procedures, such as cluster analyses. For future research, we suggest that the user perception of the PPA should be measured with standardized methods and scales in order to perform more in-depth statistical analyses. Finally, we would like to point out that the sample of our main study, although large, only included participants from one country and was not representative for the whole population of Internet users. Therefore, the results can only be generalized to a limited extent and further surveys with representative samples are necessary.

7 CONCLUSION

We investigate how (1) users in general and (2) different user groups imagine their personal privacy assistant (PPA). We start by deriving five essential aspects from the literature that need to be taken into account when designing PPAs. We conducted an online user study with N = 636 participants. We assess participant understanding of the study material and gather qualitative insights with a pilot study in which we interview 12 participants. We find that the main feature that participants desire from their PPA is that it sets privacy preferences for them and notifies them of privacy-infringing app access. The PPA should learn their privacy preferences in a transparent process, e. g., by asking questions. The level of desired user involvement in the PPAs decisions can vary in different contexts. For example, for repetitive decisions, participants tend to want to be less involved. Our studies show that there are two possible user groups regarding the PPA design, which differ significantly in their user characteristics (e. g., privacy concerns) and requirements for the PPA (e. g., level of desired involvement). Our findings offer a holistic picture on the user perspective on PPAs and can serve as a starting point for further research and as a basis for the design of PPAs. In the discussion we show how different elements from the design space for PPAs can fulfill psychological needs of the users. Based on this, we give concrete recommendations for the design of the PPA to fulfill user needs and contribute to a positive user experience.

ACKNOWLEDGMENTS

This work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, grant number 251805230/GRK 2050) and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] Yuvraj Agarwal and Malcolm Hall. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services - MobiSys '13*, page 97, Taipei, Taiwan, 2013. ACM Press. http://dl.acm.org/citation.cfm?doid=2462456.2464460.

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796, 2015.

[3] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information, November 2019.

[4] Klaus Backhaus, Bernd Erichson, and Rolf Weiber. *Fortgeschrittene multivariate Analysemethoden: eine anwendungsorientierte Einführung*. Springer-Verlag, 2015.

[5] Paritosh Bahirat, Yangyang He, Abhilash Menon, and Bart Knijnenburg. A data-driven approach to developing iot privacy-setting interfaces. In *23rd International Conference on Intelligent User Interfaces*, IUI 2018, pages 165–176. ACM Press, 2018. http://dx.doi.org/10.1145/3172944.3172982.

[6] Tom Biselli, Enno Steinbrink, Franziska Herbert, Gina M Schmidbauer-Wolf, and Christian Reuter. On the challenges of developing a concise questionnaire to identify privacy personas. *Proceedings on Privacy Enhancing Technologies*, 4:645–669, 2022.

[7] Jürgen Bortz and Christof Schuster. *Statistik für Human-und Sozialwissenschaftler: Limitierte Sonderausgabe*. Springer-Verlag, 2011.

[8] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery. https://doi.org/10.1145/3313831.3376389.

[9] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, 2018.

[10] Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, and Mahadev Satyanarayanan. Assisting Users in a World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1387–1396, Honolulu, HI, USA, July 2017. IEEE.

[11] Geert de Haan. Hci design methods: where next? from user-centred to creative design and beyond. In *Proceedings of the European Conference on Cognitive Ergonomics 2015*, pages 1–8, 2015.

[12] Lujun Fang and Kristen LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web - WWW '10*, page 351, Raleigh, North Carolina, USA, 2010. ACM Press.

[13] Thomas Franke, Christiane Attig, and Daniel Wessel. 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):456–467, 2019.

[14] Nina Gerber, Paul Gerber, Hannah Drews, Elisa Kirchner, Noah Schlegel, Tim Schmidt, and Lena Scholz. FoxIT: enhancing mobile users' privacy behavior by increasing knowledge and awareness. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust - STAST '17*, pages 53–63, Orlando, Florida, 2018. ACM Press.

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

[16] Clickworker GmbH. Ai training data and other data management services, 2005-2022. Retrieved on February 02, 2022 from https://www.clickworker.com/.

[17] Thomas Gross. Validity and reliability of the scale internet users' information privacy concerns (iuipc). *Proceedings on Privacy Enhancing Technologies*, 2021:235 – 258, 2021.

[18] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. Needs, affect, and interactive products–facets of user experience. *Interacting with computers*, 22(5):353–362, 2010.

[19] Yangyang He. Recommending privacy settings for IoT. In *Proceedings of the 24th International Conference on Intelligent User Interfaces Companion - IUI '19*, pages 157–158, Marina del Ray, California, 2019. ACM Press.

[20] Franziska Herbert, Gina Maria Schmidbauer-Wolf, and Christian Reuter. Who should get my private data in which case? evidence in the wild. In *Mensch und Computer 2021*, pages 281–293. 2021.

[21] Ron Hirschprung, Eran Toch, Frank Bolton, and Oded Maimon. A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, 61:443–453, 2016.

[22] IBM. SPSS Software, Version: 28.0.1.0, 2022.

[23] BSEN ISO and BRITISH STANDARD. Ergonomics of human-system interaction. *British Standards Institution*, 2010.

[24] Mounika Kasaraneni and Johnson P Thomas. A self–learning personal privacy assistant. In *International Conference on Advanced Information Networking and Applications*, pages 276–287. Springer, 2020.

[25] Roeland HP Kegel. The personal information security assistant. In *2015 IEEE 23rd International Requirements Engineering Conference (RE)*, pages 393–397. IEEE, 2015.

[26] Saskia M Kelders, Robin N Kok, Hans C Ossebaard, and Julia EWC Van Gemert-Pijnen. Persuasive system design does matter: a systematic review of adherence to web-based interventions. *Journal of medical Internet research*, 14(6):e2104, 2012.

[27] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[28] Lydia Kraus, Ina Wechsung, and Sebastian Möller. Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, 34:34–45, 2017.

[29] Ponnurangam Kumaraguru and Lorrie Faith Cranor. *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, 2005.

[30] A Can Kurtan and Pınar Yolum. Assisting humans in privacy management: an agent-based approach. *Autonomous Agents and Multi-Agent Systems*, 35(1):1–33, 2021.

[31] Marc Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In Gaetano Borriello and Lars Erik Holmquist, editors, *UbiComp 2002: Ubiquitous Computing*, volume 2498, pages 237–245. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[32] D.J. Leiner. Sosci survey (version 2.5. 00-i), 2014. Computer Software, available at: https://www.soscisurvey.de.

[33] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th*

Symposium On Usable Privacy and Security ({SOUPS} 2014), pages 199–212, 2014.
[34] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security*, pages 27–41, 2016.
[35] Bin Liu, Jialiu Lin, and Norman Sadeh. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help? In *Proceedings of the 23rd international conference on World wide web*, pages 201–212, 2014.
[36] Bojana Lobe, David Morgan, and Kim A Hoffman. Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods*, 19:1609406920937875, 2020.
[37] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühläuser. "i don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, NordiCHI '20, pages 1–11, New York, USA, 2020. ACM.
[38] Michal Jakob, Zbyněk Moler, Zbynek Michal Pechoucek, Roman Vaculín. Intelligent Content-based Privacy Assistant for Facebook. In *2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, volume 1, pages 499–500. IEEE, 2011.
[39] Tehila Minkus and Nasir Memon. Leveraging personalization to facilitate privacy. *Available at SSRN 2448026*, 2014.
[40] Jonathan Mugan, Tarun Sharma, and Norman Sadeh. Understandable learning of privacy preferences through default personas and suggestions. *Institute for Software Research Technical Report CMU-ISR-11-112. Carnegie Mellon University, Pittsburgh, PA*, 2011.
[41] Nico JD Nagelkerke et al. A note on a general definition of the coefficient of determination. *Biometrika*, 78(3):691–692, 1991.
[42] Primal Pappachan, Martin Degeling, Roberto Yus, Anupam Das, Sruti Bhagavatula, William Melicher, Pardis Emami Naeini, Shikun Zhang, Lujo Bauer, Alfred Kobsa, Sharad Mehrotra, Norman Sadeh, and Nalini Venkatasubramanian. Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences. In *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 193–198, Atlanta, GA, USA, June 2017. IEEE.
[43] Hannah Quay-de la Vallee, Paige Selby, and Shriram Krishnamurthi. On a (Per)Mission: Building Privacy Into the App Marketplace. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM'16*, pages 63–72, Vienna, Austria, 2016. ACM Press.
[44] Frederic Raber, David Ziemann, Antonio Krueger, C Weir, and M Mazurek. The "retailio" privacy wizard: assisting users with privacy settings for intelligent retail stores. In *EuroUSEC '18: 3rd European Workshop on Usable Security. EuroUSEC European Workshop on Usable Security (EuroUSEC-18), 3rd, located at IEEE Conference on Security & Privacy, April 23*, volume 18, pages 23–23, 2018.
[45] Bahman Rashidi, Carol Fung, and Tam Vu. Dude, ask the experts!: Android resource access permission recommendation with RecDroid. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 296–304, Ottawa, ON, Canada, May 2015. IEEE.
[46] Manuel Rudolph, Svenja Polst, and Joerg Doerr. Enabling users to specify correct privacy requirements. In *International Working Conference on Requirements Engineering: Foundation for Software Quality*, pages 39–54. Springer, 2019.
[47] Richard M Ryan and Edward L Deci. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, 55(1):68, 2000.
[48] Norman Sadeh, Bin Liu, Anupam Das, Martin Degeling, and Florian Schaub. Personalized privacy assistant, March 23 2021. US Patent 10,956,586.
[49] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. Informing the Design of Privacy-Empowering Tools for the Connected Home. *arXiv:2001.09077 [cs]*, pages 1–14, January 2020. arXiv: 2001.09077.
[50] Kennon M Sheldon, Andrew J Elliot, Youngmee Kim, and Tim Kasser. What is satisfying about satisfying events? testing 10 candidate psychological needs. *Journal of personality and social psychology*, 80(2):325, 2001.
[51] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, 2021.
[52] Alina Stöver, Nina Gerber, Sushma Kaushik, Max Mühlhäuser, and Karola Marky. Investigating simple privacy indicators for supporting users when installing new mobile apps. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–7, 2021.
[53] Alina Stöver, Felix Kretschmer, Christin Cornel, and Karola Marky. Work in progress: How i met my privacy assistant–a user-centric workshop. *Mensch und Computer 2020-Workshopband*, 2020.
[54] Onuralp Ulusoy and Pinar Yolum. Panola: A personal assistant for supporting users in preserving privacy. *ACM Transactions on Internet Technology (TOIT)*, 22(1):1–32, 2021.
[55] Userstudymaterial. Ppa-study-survey, 2022. Study material available at: https://github.com/Userstudymaterial/PPA-Study-Survey/blob/main/Survey%20-%20Pre%20and%20Main%20Study.pdf.
[56] VERBI Software, Berlin, Germany. MAXQDA 2020 [computer software], 2020.
[57] Alan F Westin. Privacy and freedom. *Washington and Lee Law Review*, 25(1):166, 1968.
[58] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 1077–1093, San Jose, CA, USA, May 2017. IEEE.
[59] Sina Zimmermann and Nina Gerber. Why do people use digital applications? a qualitative analysis of usage goals and psychological need fulfillment. *i-com*, 18(3):271–285, 2019.
[60] Zoom Video Communications, Inc. Zoom Video Communications Software, Version: 5.9.1, 2022.

A APPENDIX A - STUDY MATERIAL

In this section, we provide materials used within our pilot and main study.

A.1 Survey Pilot and Main Study

Notes: The questionnaire was translated from the original language. For these submissions, the design choice images and some explanatory descriptions for the participants have been shortened. The study material is available here [55].

- **Informed Consent**
- **Preliminary Questions:** Technology Affinity Scale[13], Demographics (age, gender, education, smartphone usage, app installation frequency, motivation to protect privacy, privacy knowledge)
- **Introduction:** Many people use their smartphone every day, on which they have installed many apps that make their everyday life easier or simply give them pleasure - social network apps, flashlight apps, etc. Often we don't know exactly what else these apps do in the background, what data they collect about us, what happens to this data or what permissions they have. And, who of us, when installing an app, reads through all the terms of use or manually goes into the privacy settings to adjust the settings the way he:she would like. This is where the privacy assistant comes into play. This is also an app on the smartphone. And it knows what is important to you and can then take over settings for you, or alert you when an app is doing something that is not in your best interest, or help you make decisions regarding your privacy. There are many options for how exactly such a privacy assistant looks like. Your task is to design a privacy assistant that suits your preferences at a total of five stations.
- **Station 1.1:** Which functions should the PPA have? First of all, we want to find out what exactly your PPA should be able to do. There are several ways to do this. Please assign the different options to a category using drag and drop. [Images of these 10 design choices: *Setting Configuration; Indicator; Reminder; Recommendations; Notification - Apps; Notification-Devices; Statistics; Learning Units; Praise; Gamification*]
- **Station 1.2:** Which function is most important to you? Please put the blue boxes in order by dragging and dropping them onto the fields with the numbers. [Presentation of the design choice categorized as important in Station 1.1.]

- **Station 2:** How should the PPA learn your privacy preferences? This station is about how your PPA should learn what is important to you. To do this, it can determine a profile of you. There are several options here as well. Please take a close look at the options listed below and then select the one that suits you best by clicking on it. [Images of these 6 design choices: *Data; Automatically; Questions; Fictitious Scenarios; Profile; Notifications*]
- **Station 3:** How should the PPA communicate with you? This station is about how much your PPA communicates with you and involves you. Please adjust the slider according to your preference. [Display of slide: *No Automation - the PPA is in constant contact with you, informs you about every decision and always involves you; Full Automation - The PPA runs in the background and you notice as little of it as possible*]
- **Station 4.1:** Who should provide the PPA? To use your PPA, it must be developed by a vendor. Please indicate to what extent you would trust the following vendors to provide your PPA. [Choice: rather trustworthy, rather untrustworthy, don't know: *Google, Apple, National hacker association, General Public Licence, National University, Facebook, National Government, Samsung, Huawai, National Telecommunication Provider, International Telecommunication Provider, 2121 Atelier (PPA Provider), Others*]
- **Station 4.2:** Now please choose a vendor which should ideally provide your PPA. [Presentation of the vendors categorized as rather trustworthy in Station 4.1.]
- **Station 5:** Which data are you willing to disclose to your PPA? For your PPA to work well, it needs certain data from you. Previous research has shown that the following data can be used to determine as accurate a profile of your preferences as possible and that the privacy assistant can support you well. What data would you be willing to disclose to your PPA? [Likert Scale: absolutely disagree - absolutely agree, don't know: *Age, Identity, Personality traits, Knowledge of data protection, purpose of the PPA, Organizations where you have privacy concerns, Information from your OSN profile*]
- **Final Questions:** Internet Users' Information Privacy Concerns (IUIPC) 8 scale [17].

B APPENDIX B - FURTHER RESULTS

In this section, we provide further results from our pilot and main study.

B.1 Results Station 4 and 5

Table 6: The table shows the results of the main study of Station 4 - Number of participants in %, who rate the corresponding vendor as rather trustworthy, rather untrustworthy or don't know

	Main Study			
	Rather trustworthy	Rather untrustworthy	Don't know	Final provider
Google	28	68	5	3
Apple	35	59	6	7
National hacker association	60	21	19	28
General Public Licence (GNU)	33	30	63	5
National university	82	6	11	27
Facebook	10	88	3	0
National government	61	34	6	13
Samsung	33	60	6	3
Huawei	13	81	7	1
National telecommunication provider	49	46	6	7
International telecommunication provider	39	54	7	2
2121 Atelier (PPA provider)	24	19	57	3
Others	na	na	na	1

Table 7: The table shows the results of the main study of Station 5 - participants' assessment of whether they are willing to disclose the respective data to their PPAs on a Likert scale ranging from 1 (don't agree) to 7 (absolutely agree)

	Main Study		
	M	*SD*	*N*
Age	3.80	1.20	625
Identity	2.84	1.31	626
Personality traits	3.05	1.20	620
Knowledge of data protection	3.78	1.07	622
Purpose of the PPA	3.93	1.03	623
Organizations where user has privacy concerns	3.86	1.12	627
Information from OSN profile	2.70	1.28	617

B.2 Results Group Differences

Table 8: The table shows the results of the t-tests examining the group differences between pragmatists and fundamentalists using the data from main study.

Aspect	User group	*N*	*M*	*SD*	*T*	*d*
Technology affinity	Pragmatists	344	4.14	0.92	2.65**	0.21
	Fundamentalists	277	4.33	0.92		
IUIPC control	Pragmatists	344	5.47	1.16	3.67***	0.3
	Fundamentalists	277	5.81	1.15		
IUIPC awareness*	Pragmatists	343	6.10	1,09	4.76***	0.38
	Fundamentalists	277	6.47	0.86		
IUIPC collection	Pragmatists	344	5.33	1,21	4.60***	0.37
	Fundamentalists	277	5.78	1.18		
Level of automation	Pragmatists	344	78.55	12.59	53.40***	4.31
	Fundamentalists	277	23.55	12.97		
Data disclosure: Age*	Pragmatists	339	3.88	1.12	1.51***	0.13
	Fundamentalists	271	3.73	1.27		
Data disclosure: Identity*	Pragmatists	339	3.02	1.25	3.55***	0.29
	Fundamentalists	272	2.64	1.35		
Data disclosure: Personality traits	Pragmatists	335	3.21	1.16	3.53***	0.29
	Fundamentalists	270	2.87	1.22		
Data disclosure: Privacy knowledge*	Pragmatists	336	3.84	0.98	1.07	n.a.
	Fundamentalists	271	3.75	1.13		
Data disclosure: Purpose of PPA	Pragmatists	335	3.95	0.98	0.15	n.a.
	Fundamentalists	273	3.93	1.10		
Data disclosure: Critical organizations	Pragmatists	339	3.82	1.10	1.05	n.a.
	Fundamentalists	273	3.92	1.15		
Data disclosure: Data from OSN	Pragmatists	334	2.89	1.25	4.15***	0.34
	Fundamentalists	268	2.46	1.27		

Table 9: The table shows the results of the Chi square tests of independence examining the group differences between pragmatists and fundamentalists using the data from main study.

Aspects	Overall sample	Pragmatists	Fundamentalists	Chi square tests of independence
Age in years n (%)				
<30	186 (30.0)	118 (34.3)	68 (24.5)	$\chi^2(4) = 11.64; p = .02; \phi = 0.14$
31-40	190 (30.6)	101 (29.4)	89 (32.1)	
41-50	108 (17.4)	47 (13.7)	61 (22.0)	
51-60	97 (15.6)	56 (16.3)	41 (14.8)	
61-70	40 (6.4)	22 (6.4)	18 (6.5)	
Gender (%)				
female	353 (56.8)	196 (57.0)	157 (56.7)	$\chi^2(4) = 1.45; p = .70$
male	260 (41.9)	142 (41.3)	118 (42.6)	
others	5 (0.8)	4 (1.2)	1 (0.4)	
n.a.	3 (0.5)	2 (0.6)	1 (0.4)	
New app installation (%)				
less than once/month	322 (51.9)	197 (57.3)	125 (45.1)	$\chi^2(1) = 9.06; p = .02; \phi = 0.12$
at least one/month	299 (48.1)	147 (42.7)	152 (54.9)	
Privacy knowledge (%)				
low	119 (19.2)	73 (21.2)	46 (16.6)	$\chi^2(2) = 2.15; p = .34$
medium	447 (72.0)	242 (70.3)	205 (74.0)	
high	55 (8.9)	29 (8.4)	26 (9.4)	
Privacy motivation (%)				
low	42 (6.8)	31 (9.0)	11 (4.0)	$\chi^2(2) = 26.02; p < .000; \phi = 0.20$
medium	363 (58.5)	222 (64.5)	141 (50.9)	
high	216 (34.8)	91 (26.5)	125 (45.1)	
Preference learning PPA (%)				
data	59 (9.5)	36 (10.5)	23 (8.3)	$\chi^2(5) = 28.10; p < .000; \phi = 0.21$
fictitious scenarios	87 (14.0)	46 (13.4)	41 (14.8)	
notifications	101 (16.3)	43 (12.5)	58 (20.9)	
questionnaire	210 (33.8)	108 (31.4)	102 (36.8)	
automatically	45 (7.2)	39 (11.3)	6 (2.2)	
profile	119 (19.2)	72 (20.9)	47 (17.0)	

Table 10: The table shows the results from main study Station 1: Number of people (in %) who rated each feature as the most important for their PPAs, split by user group of Fundamentalists and Pragmatists.

	Fundamentalists ($N = 246$)	Pragmatists ($N = 281$)
Setting configuration	28.0 %	27.4 %
Indicator	5.3 %	10.0 %
Reminder	0.0 %	2.5 %
Recommendations	8.9 %	11.7 %
Notification - apps	44.7 %	29.5 %
Notification - devices	4.1 %	8.9 %
Statistics	2.0 %	3.6 %
Learning units	2.0 %	2.8 %
Praise	2.8 %	1.8 %
Gamification	2.0 %	1.8 %

B.3 Code Book Thematic Analysis (Pilot Study)

Table 11: The table shows the code book with themes and categories, which resulted from the thematic analysis of the pilot study.

Theme	Categories
Awareness-related requirements for PPA	Privacy behavior must be allowed to adapt Creating transparency Giving an outside perspective Being a learning companion Creating awareness of habits Pointing out change Showing possibilities for change Inform
Support-related requirements for PPA	Knows user preferences very well Should remember user decisions Gives situational support Requires little involvement with PPA Supports by complexity reduction Makes intelligent assessment Should make decisions
Requirements for preference learning	Simplicity Close to everyday life Concrete/non-abstract Empathy possible Avoid excessive demands Readjustment must be possible Transparency Not forced into profile Possibility of reflection Right of co-determination Previous behavior does not reflect desired behavior
Conditions for acceptance of automation	Reliability Consent must be given Trust Control Transparency Behavior must remain changeable Adaptability must be guaranteed
Areas where automation is desired	Time critical situations Recurring decisions

Table 12: The table shows the code book with themes and categories, which resulted from the thematic analysis of the pilot study.

Theme	Categories
Areas where automation is not desired	Preference learning Getting to know Important decisions Profile building
Why do users not disclose data	Fear of data misuse General desire for data economy See no added value Vendors not trustworthy Do not want to connect services
Factors influencing trust in vendors	Personal connection/positive previous experience Brand Image Gut feeling Intention of the vendor External control Business model Data practices User focus Prior experience with vendor privacy Independence/controllability of the vendor Demographics/democracy of the vendor
Concerns about the PPA	Bystander conflicts Overload UX of other apps disturbed Vendor has interest in data PPA interferes too much with privacy PPA encourages smartphone consumption Personality profile generation
Factors influencing trust in PPA	(Data) Security Reliability Control transparency Trust in vendor
Factors influenced by trust in PPA	Acceptance of PPA Desired features Level of automation Data willing to disclose