Work in Progress: How I met my Privacy Assistant – A User-Centric Workshop

Alina Stöver
stoever@psychologie.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Felix Kretschmer
felix.kretschmer@stud.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Christin Cornel
christin.cornel@stud.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

Karola Marky
marky@tk.tu-darmstadt.de
Technical University of Darmstadt
Darmstadt, Germany

ABSTRACT

Privacy Assistants (PAs) are a promising method to support users in making and communicating privacy-related decisions. In this work in progress paper, we present a study design to investigate users perspective on PAs in the context of mobile apps in an explorative user-centric workshop. The participants are asked to provide 1) which information they are comfortable sharing with their PA, 2) how the PA learns this information, 3) how the PA should assist and how it should communicate with the participants, and 4) which entity should provide the PA. Participants are encouraged to think aloud during the workshop and are interviewed as debriefing. The initial results of a pilot study indicate that there may be a great variety of requirements and ideas of a PA between users.

CCS CONCEPTS

• Security and privacy → Privacy protections; **• Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Privacy; Privacy Assistant; Workshop

1 INTRODUCTION

Three in four (78%) global citizens are concerned about their online privacy [2]. At the same time, users also express a lack of control over their personal information online [2]. A promising way to mitigate these concerns and facilitate control are so-called *Privacy Assistants (PAs)* [3, 6]. PAs can support users in making privacy decisions and communicating privacy intentions. Different possibilities for realizing PAs have been demonstrated in specific domains, such as Online Social Networks [12, 23], the Internet of Things [6, 9], and mobile apps [3, 34].

In this work-in-progress study, we first developed a concept for a PA. In particular, our PA aims to support users in matching the permissions of mobile apps to their privacy preferences. Next, we designed a user workshop. The goal of our workshop is to explore the user's perspective on the PA and the user's requirements for different aspects of the PA. In four workshop stations, the participants get the opportunity to create their personal PA to support protecting their privacy when interacting with mobile apps. During the workshop, we encouraged participants to think-aloud [4] and interviewed them to gain a deeper understanding of: Which information are users comfortable sharing with the PA? How should the PA learn about the user? How should the PA assist the user and how should it communicate with the user? And finally, which entity will provide the PA?

We report first results from a pilot study (N = 2), giving first insights on the user perspectives on different aspects of interaction with a PA. The results indicate that there may be a great variety of requirements and ideas of a PA between users. Finally, we discuss the methodological implementation of the workshop and give an outlook on how further data collection can proceed. Furthermore, we show how other researchers can build on this work in progress.

2 RELATED WORK

Research on Privacy Assistants (PA) can be clustered into four different areas: Privacy Assistants for 1) Websites, 2) Online Social Media, 3) Internet of Things devices, and 4) mobile apps. This section will give an overview of different approaches within these categories.

2.1 Website Privacy Assistants

To avoid the unwanted storage of information (e.g. tracking cookies), users have to locate a website's privacy policy, read it, and configure the setting according to their preferences. However, doing this for each visited website places a big burden on the user. To mitigate this problem, PAs were designed to support users with reading and comprehending these policies [5, 8, 16]. The main function of these PAs is summarizing privacy policies and showing users their most relevant aspects. A different approach was developed by the German telecommunication agency Deutsche Telekom [11]. They deployed a data cockpit for their website, to provide their costumers with an interface to gain information about the company, data usage, and their contracts, as well as data management settings.

MuC'20 Workshops, Magdeburg, Deutschland
© Proceedings of the Mensch und Computer 2020 Workshop on «6. Usable Security und Privacy Workshop». Copyright held by the owner/author(s).
https://doi.org/10.18420/muc2020-ws119-005

2.2 Online Social Networks Privacy Assistants

Online Social Networks (OSNs) are a considerable threat to user privacy as their main purpose is sharing information. In this context, Wisniewski et al. showed that users prefer achieving a level of privacy that matches their preferences rather than sharing as much as possible [37]. However, the choice of privacy settings and deciding which information should be shared can be difficult [21]. Thus, many users struggle in managing their privacy settings. To mitigate this problem Fang et al. developed a framework for a PA that automatically adjusts privacy settings [12]. They built a prototype that asked users whether they would be willing to share their personal information, e.g. their birthday, with a selected set of friends. Based on this information the PA was able to predict a user's privacy preferences. Another way to protect users from oversharing their data is a PA specifically developed for the OSN Facebook [23]. When interacting with this PA users are asked to define rules to determine which recipients can see status updates. If a user posts a status update, the PA highlights privacy-sensitive parts, like locations and provides a list of friends with whom the status update can be shared. This enables users to select an audience for their status update based on its content.

2.3 Internet of Things Privacy Assistants

Internet of Things (IoT) devices are everyday devices with computing and networking capabilities, such as smartwatches, smart speakers, or smart fridges. IoT devices can be used to continuously monitor their users and, in case of smart homes, also their housemates and guests [22]. This comes with the potential of various privacy threats. However, many users lack concerns about privacy risks [20], as well as knowledge about data collection and storage [6], or are overwhelmed by the number of privacy decisions [6]. This suggests the need for IoT PAs but due to the heterogeneity of IoT devices, different approaches might be needed. Colnago et al. described three possible types of IoT PAs: 1) PAs, which inform users about data collection, 2) PAs, which provide recommendations for information disclosure, and 3) PAs, which automatically act on behalf of the user [6]. Past research on IoT PAs focused also on public spaces. For instance, Pappachan et al. developed a framework for a PA that manages privacy preferences in smart buildings [25]. Langheinrich describes a framework for a PA, which informs the users about the data collection and provides the possibility to change settings [19]. Das et al. developed an app to inform users of nearby cameras and give them the opportunity to obscure their face [9]. Raber et al. addressed the problem of data collection by smart retail stores, like Amazon Go, by building a privacy manager that can help users with their privacy settings [29]. Further papers deal with data collection within smart homes. Hereby, He proposes a prototype for a privacy settings interface that allows users to configure the settings of multiple smart assistants [15]. Seymore further extended this idea and developed a PA that not only informs users about data collection of their IoT devices and gives the option to set a firewall to prevent data leakage but also gives lessons about network privacy [31].

2.4 App Privacy Assistants

Several research projects are concerned with privacy in the context of smartphone apps. The cause of this lies in the fact that smartphones are commonly used devices and that apps often collect various sensitive user data, like the users location or identity information. These data is not only gathered for the purpose of app functionality, but it is also often used for targeted advertising and sold off to third parties [13]. It is therefore vital to support users with managing their data as many do not read End User License Agreements before installing an app [32] and are therefore unaware of the specific information requested by the apps. Different approaches to mitigate this problem include PAs, which notify users when data is collected [1, 3, 30], PAs, which automatically set permission settings [34, 36] and PAs, which give recommendations for app settings either in the form of ratings [1, 14, 27] or in the form of a personalized set of recommendations [3].

2.5 Research Gap

The approaches described above evaluated one part or specific concept of a PA, or focus on very specific aspects, such as personalized recommendations [18], information about permission purposes [3], or gamification [14]. Therefore, in this study, we build upon this findings and introduce the PA Workshop as a method to explore how users would design different aspects of a their personal PA.

3 CONCEPT OF A PRIVACY ASSISTANT AND RESEARCH QUESTIONS

The basis for the user workshop is a concept of a PA. A PA can support users in different contexts where the user wants to enforce privacy preferences (e.g. IoT, Smart Home devices). The PA concept presented in the following is a general one. For our study, we used the use case app permission. Therefore, we understand a PA as a program that learns about the privacy preferences of the user regarding different app permissions, implements them, and might also notify the user. In our concept, the user provides input to the PA (e.g., privacy preferences) and receives the output generated by the PA (e.g., settings). The PA in turn enforces the user preferences against all entities that allow the user to adjust privacy settings (e.g., IoT devices, OSNs). This means that the PA passes the user's preferences as input to the privacy settings but also receives output from the settings, e.g. if new settings are available. In addition, the PA is connected to a provider. There can also be exchanges between the PA and provider of the PA, for instance, the provider can inform the PA about changes in the law.

We divide the use of the PA into the three stages of 1) input, 2) process, and 3) output (see Fig. 1). This idea is based on work by Xiao and Benbasat who applied and investigated this division in the field of advice-giving systems (AGS) [39]. They defined the input stage "where users' preferences or needs are elicited". In our concept the PA in the stage *Input User* receives all the information it needs from the user. This can be demographic data, the user's level of expertise in the area of data protection, or information from social media accounts. Especially social media postings are a valuable source of information, as it was shown that a person's privacy measures and therefore their privacy concerns can be inferred from this kind of data [28]. However, it is unclear what kind of data users

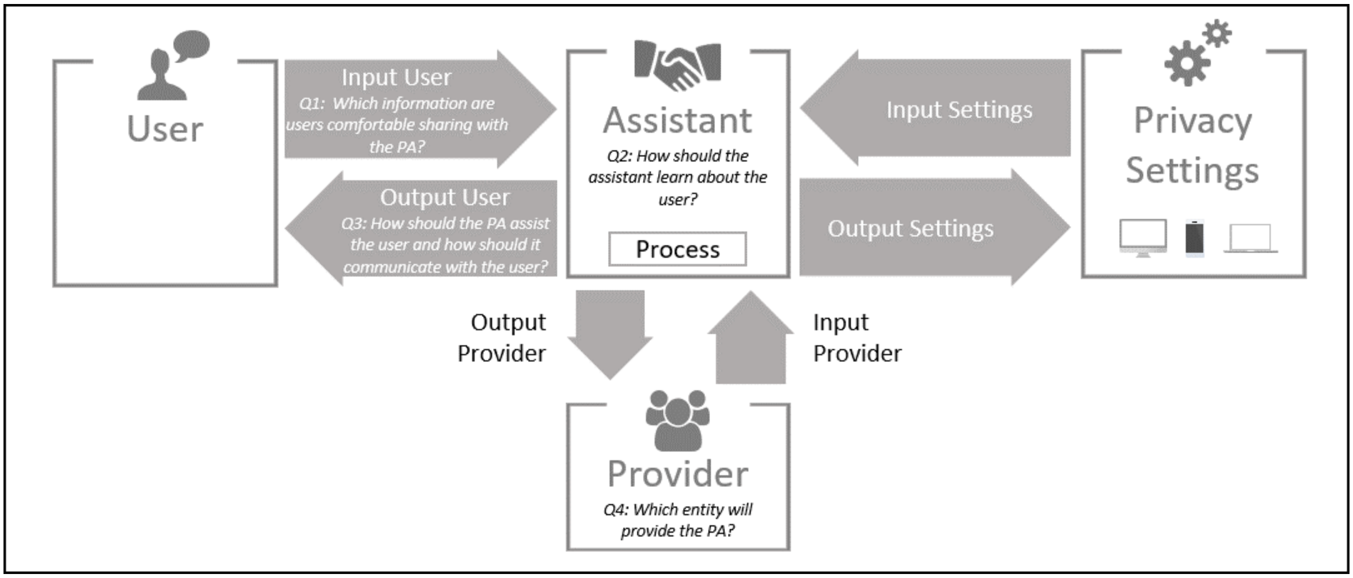

User
Input User
Q1: Which information are users comfortable sharing with the PA?
Output User
Q3: How should the PA assist the user and how should it communicate with the user?
Assistant
Q2: How should the assistant learn about the user?
Process
Input Settings
Output Settings
Privacy Settings
Output Provider
Input Provider
Provider
Q4: Which entity will provide the PA?

Figure 1: Model of the communication from a PA to the neighbouring entities

are comfortable providing to the PA, as the tendency to provide personal information is not a unidimensional construct [17]. This means that people differ in their disclosure behavior depending on the type of requested information. This leads to the question

> **Q1:** Which information are users comfortable sharing with the PA?

In the context of advice-giving systems, the "process stage is where advice is generated based on users' preferences or needs." [39]. In our context, the *Process Stage* means that the PA processes the intentions of the user and transfers them into privacy settings (of devices, apps, websites). In this study, we focus on the interaction between the user and PA and therefore are interested in the following question

> **Q2:** How should the PA learn about the user?

For advice-giving systems, "the Output stage is where systems present the generated advice to users." [39] In our concept, the question of communication of the PA with the user is central in the *Output Stage*. This includes 1) the interface or design of the PA, 2) what information the PA communicates to the user 3) how often, and 4) in what way the communication occurs. In our study, we examine the user perspective on different variants of these four aspects to answer the following question:

> **Q3:** How should the PA assist the user and how should it communicate with the user?

Behind every PA is a provider. The choice here ranges from device or software manufacturers (e.g., Apple, Google), to research institutions (e.g., a university), to non-governmental organizations (e.g., the Chaos Computer Club), and public authorities (e.g. a ministry). With our last question, we would like to shed light on the user perspective on:

> **Q4:** Who will provide the PA from the users point of view?

4 METHOD

To investigate the user perspective on different aspects of a PA and shed light on the previously formulated questions, we conducted a workshop study combined with an interview. With our study design, we aimed to create a trustworthy and open atmosphere to achieve a holistic and detailed reception of the user perspective. Open answers were implemented to address the creativity of the user. In a written introduction, the concept of a privacy assistant for smartphone apps was explained to the participants and a problem-based scenario was presented in which the support of a PA would be helpful. In four stations (see Fig. 2), participants were asked to create their personal PA. They were guided through the four stations by a workshop assistant and encouraged to express their thoughts out loud [4]. In order not to influence the respondents in the decision-making process, communication was reduced to a minimum. After a demographic questionnaire, finally, the participants summarized and discussed their thoughts on their personal PAs in a semi-structured interview.

4.1 Procedure

The procedure of our workshop was as follows:

4.1.1 Station 1: Which information are users comfortable sharing with the PA?. In the first station, a questionnaire was used to determine the data the user is willing to disclose to the PA. Based on that, the PA can create a privacy profile. The items were created, based on literature research on factors for previous PAs. The feature awareness of privacy controls, as well as sharing tendencies in OSNs, are partially related to privacy management strategies and can be used to create privacy profiles of the users [38]. Also, the knowledge about privacy and the motivation can be used to assign users to privacy profiles[10]. Users' personality traits, as well as demographics, were used to suggest accurate personalized privacy settings in the context of OSNs [24].

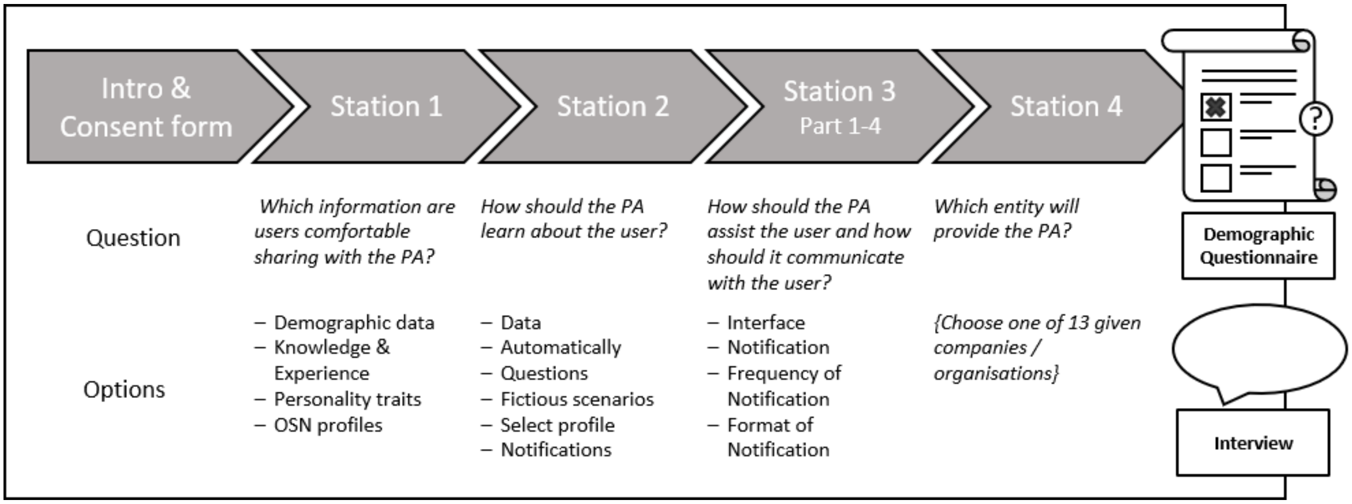

Intro & Consent form
Station 1
Station 2
Station 3 Part 1-4
Station 4
Question
Which information are users comfortable sharing with the PA?
How should the PA learn about the user?
How should the PA assist the user and how should it communicate with the user?
Which entity will provide the PA?
Demographic Questionnaire
Options
– Demographic data
– Knowledge & Experience
– Personality traits
– OSN profiles
– Data
– Automatically
– Questions
– Fictious scenarios
– Select profile
– Notifications
– Interface
– Notification
– Frequency of Notification
– Format of Notification
{Choose one of 13 given companies / organisations}
Interview

Figure 2: Procedure of the user workshop

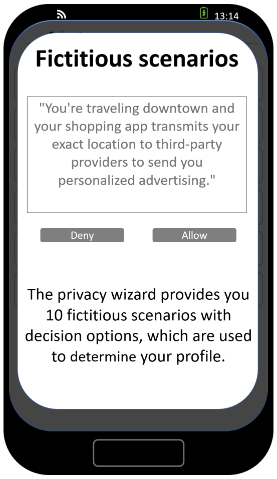
We used the following eleven items to assess the extent to which participants are willing to disclose the data to the PA. Using a 4-point Likert scale (disagree absolutely to agree completely), we assess the extent to which participants are willing to disclose the following data to the PA: demographic variables, identity, e-mail address, age, knowledge of data protection, previous experience with privacy violations, personality traits, and information from OSN profiles.

Furthermore, there was a text field for qualitative answers to add further sources of information.

While realistic scenarios offer an opportunity to capture context-based privacy behavior without distortion [33], an exemplary notification is less abstract. Conalgo et al. showed that users differed in the degree of desired automation of PA recommendations [6] and unlike an automated approach, are choosing a profile to determine preferences commonly used in mobile applications. Thus, in the second station, the participants explored ways how the PA could learn about their privacy preferences and how it could create a privacy profile. Participants could choose between the following six options or create their own version (example see Fig. 3):

4.1.2 Station 2: How should the PA learn about the user? While realistic scenarios offer an opportunity to capture context-based privacy behavior without distortion [33], an exemplary notification is less abstract. Conalgo et al. showed that users differ in the degree of desired automation of PA recommendations[7] and unlike an automated approach, choosing a profile to determine preferences is commonly used in mobile applications. Thus, in the second station, the participants explored ways how the PA could learn about their privacy preferences and how it could create a privacy profile. Participants could choose between six different options or create their own version (example see figure3):

- *Data:* The PA determines the profile based on the information provided in Station 1.
- *Automatically:* The PA automatically determines the profile based on the existing permissions for the user's apps.



Fictitious scenarios

"You're traveling downtown and your shopping app transmits your exact location to third-party providers to send you personalized advertising."

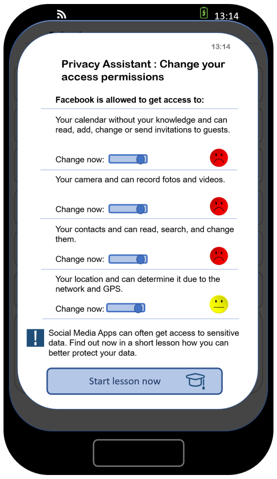
The privacy wizard provides you 10 fictitious scenarios with decision options, which are used to determine your profile.

Figure 3: Example station 2

- *Questions:* The PA determines the profile based on questions regarding personal settings.
- *Fictitious scenarios:* The PA provides ten fictitious scenarios with decision options, which are used to determine the user's profile.
- *Select profile:* The PA presents three profiles to choose from (Fundamentalist, Pragmatist, Unconcerned) [35].
- *Notifications:* The PA sends ten exemplary notifications with decision options to determine the profile.

4.1.3 Station 3: How should the PA assist the user and how should it communicate with the user? Station 3 included four parts: 1) interface, 2) type of notification, 3) frequency of notification, and 4) the format of notification. An example is given by Fig. 4).

Interface. In the first part of Station 3, the participants were asked to determine their preferred interface of a PA. The various design



Privacy Assistant : Change your access permissions

Facebook is allowed to get access to:

Your calendar without your knowledge and can read, add, change or send invitations to guests.

Change now:

Your camera and can record fotos and videos.

Change now:

Your contacts and can read, search, and change them.

Change now:

Your location and can determine it due to the network and GPS.

Change now:

Social Media Apps can often get access to sensitive data. Find out now in a short lesson how you can better protect your data.

Figure 4: Example station 3

implications were drawn up on the basis of Gerber et al. [14]. The goal is to determine whether different gamification elements are preferred over a simplified presentation of the PA recommendations. The participants could choose from a selection of four interfaces:

(1) *Online ranking list:* Users can earn points by completing challenges, for example changing three questionable access permissions of applications. The earned points are displayed in an online ranking list together with the points of other users of the PA.
(2) *Avatar:* Similar to the online ranking list, users can earn points by completing challenges. The points can be spent to customize an avatar.
(3) *Achievements:* Specific achievements could be earned for completing challenges.
(4) *Information only:* An overview of all apps, containing the information about the access permissions of the respective apps.

Notification. Considering the notification, the participants could choose aspects in which they wish a notification from the PA. These aspects are:

- *Privacy threats:* Potential threats to the user's privacy
- *Preference violations:* about access rights of apps that contradict the user's preferences
- *App permission:* notifications about permissions of all apps
- *App permission + privacy lesson:* notifications about permissions of all apps with an offering of a lesson on how to better protect privacy.

Frequency of Notification. While push notifications can increase mobile app engagement, they can result in the opposite effect, if they are used too frequently [26]. Therefore, the following options for notification frequency were provided:

- *several times per day*
- *once per day*
- *several times per week*
- *once per week*
- *once per month*
- *never*

Format of Notification. The participants could choose from three notification formats:

- *full screen*
- *half screen*
- *notification bar*

4.1.4 Station 4: Which entity will provide the PA?. In the fourth station, 13 different manufacturers who could possibly produce the PA were presented to the participant (including a short description). Since the mission statement of a provider always allows possible conclusions to be drawn about further data processing and intentions, a broad selection of providers with different features was made. Therefore, transparency as well as the possibility to choose the source of the PA recommendation, are desired by users [7]. The selection consisted of Google, Apple, Chaos Computer Club, GNU General Public License, a university, Facebook, the German Government, Android, Samsung, Huawei, Telekom, Vodafone, and 2121 Atelier Inc. First, the participants categorized them as trustworthy or not trustworthy. Then, the participant chose a manufacturer that offers the PA and explained their choice.

4.1.5 Final Interview. Finally, a semi-structured interview was conducted to clarify ambiguities or incomplete answers and gain more detailed information on the cause of the decision made. This ensured that the precise meaning of the think-aloud-comments was not distorted by interpretation along with the consideration of factors that might have been disregarded. It was also an opportunity for the participant to view the PA in context, reconsider decisions already made, and address the priority of different features. In addition, a ten-point scale was used to assess the likelihood of using and recommending the self-developed PA to check the accuracy of the information given and the discrepancy between the attitude and behavior intention.

4.1.6 Data collection. The study was initially planned as an offline laboratory study and has already been tested as such. Later the concept was transferred into an online study, that should meet the following criteria:

- *Accessibility:* In principle, participation in the study should be possible for all persons, regardless of previous technical experience.
- *Positive Atmosphere:* A pleasant and trusting situation should be created in which the participants feel comfortable.
- *Creativity:* The study design should be interactive and allow room for the participant's creativity to maintain motivation.

The offline version of the study took place in a laboratory. All materials were printed on paper and could be attached to a pinboard by the participants. In the online study, the materials were presented as a survey. We used the provider *soscisurvey.de.* During the whole process, the participants and the interviewing person participated in a video conference service. We used the German Research Network available under *www.conf.dfn.de.* In both variants -offline and online- the conversations were audio-recorded and transcribed for analysis.

Table 1: Demographic data of the participants

Demographics	P1	P2
Age	31	20
Gender	male	female
Education	university degree	high school
Profession	business engineer	law student
Operating System	Android	Android
Data protection knowledge	advanced	advanced
Motivation	medium	high
Privacy concerns	medium	high

4.2 Data Analysis

We started by transcribing the audio recordings of the study into written form. For the purpose of this work-in-progress study, single-case-analysis of the transcripts was performed. Qualitative content analysis is planned for the analysis of further interviews.

4.3 Recruitment and Participants

In the preliminary study, two participants were recruited from the author's personal environment. Participant 1 (P1) participated in the offline version of the study, participant 2 (P2) in the online version. Table 1 shows the demographic data of the participants.

4.4 Ethical Considerations

The study follows the guidelines of the ethics committee of our institution. 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. Our study, furthermore, complied with national privacy regulations and the European General Data Protection Regulation (GDPR).

5 PRELIMINARY RESULTS

In this section, we report results from our pilot study (N = 2), giving first insights on the user perspectives on different aspects of a PA. First, we give an overview of the personal PAs that the participants have created in the course of the study. Then, we detail the results of the different stations of the study, providing participant comments when meaningful.

5.1 Participants' Final Privacy Assistant

Two people (P1 and P2) created their personal PA while they went through the four stations of the workshop. Their final choices are shown in Table 2. Both participants also gave a final statement about their personal PA, in which they formulated their understanding of the PA and emphasized what is important to them.

For P1, the PA is an app *"that simply analyzes which apps with which settings I already have on my phone and (...) notifies me if there's an anomaly in it, or if I download something new, it gives me a hint or even makes the settings completely for me."*. The participant also pointed out that *"it works as automatically as possible and that I don't have to spend so much time with it and can still feel secure.* Every now and then he wants to receive a notice from his PA to check if *"it is still alive?"*. P1 also states that it is important to him that the PA evolves and adapts to new knowledge or changed behavior and does not force him *"into a rigid profile of 2 years ago."*

For P2, on the other hand, it is important that the PA *"always indicates as soon as a new change or a request for a private matter occurs."* She wants to have a say in *"whether the PA should allow anything"*. The actions of the PA should be as conspicuous as possible *"should be displayed on my whole display"*. P2 goes on to say that it's important to her that the PA *"shows me which app wants something and that it shows me what exactly that is and that I can definitely change that. And that I am warned"*. It's also important to her *"that it's displayed neutrally and that I'm not being pushed into anything."* A *"creatively designed"* PA, she would find *"just confusing"*.

Table 2: Participants' final PAs

	P1	P2
Station 1	9 of 11	1 of 11
Station 2	fictitious scenarios	data
Station 3		
Part 1: Interface	avatar	information only
Part 2: Notification	privacy threats	app permission + privacy lesson
Part 3: Frequency	several times / day	several times / day
Part 4: Format	half screen	full screen
Station 4	Chaos Computer Club	university

5.2 Station 1: Which information are users comfortable sharing with the PA?

P1 would give the PA access to 9 of 11 types of information excluding email-address and phone number. The choice is justified by saying that the PA needs this information *"to do its job. [...] with the things, [...] - where it seemed strange to me - I said: no, not that."*. P2 only allows the PA access to her email-address and says *"actually I don't want to give away any of my data"*.

5.3 Station 2: How should the PA learn about the user?

P1 opts for*fictitious scenarios* because *"I can easily be asked how I would act in a certain situation"*. Also, they are not as rigid and boring as a questionnaire. Furthermore, he suggests that the PA should rather ask for scenarios that it has not yet been able to learn from past behavior.

P2 is unsure whether the indirect methods really select the correct settings and therefore opts for the variant that the PA takes the data from station 1. *"Therefore I would probably rather take the second picture, where I then accept exactly what I have specified."*

5.4 Station 3: How should the PA assist the user and how should it communicate with the user?

Part 1 - Interface. P1 rates the possibility that the PA includes achievements or rankings as positive. But *"this is not the first thing I want to see when I open the app"*. That is why he chooses the Avatar. *"I think if there's like my avatar up there, with my name and stuff, it feels like that's my assistant"*.

P2 selects *"information only"*: *"I think it looks neutral."* She rates the avatar as *"a little creepy"*. And about the achievements she says: *"Your achievements sound very commendable, for yourself somehow. But I don't know if that would fit in with a privacy assistant telling me what I've done well."*

Part 2 - Information. P1 decides to be notified when a vulnerability occurs because *"that would be the most important thing"* and *"not too often"*.

P2 chooses to be notified about permissions of all apps with an offering of a voluntary lesson on how to better protect her privacy.

Part 3 - Frequency. P1 indicates to be informed by the PA several times a day and specifies that he wants to be informed immediately in case of a threat without getting *"totally bombed."*

P2 also wants to be informed several times a day. In fact, *"as soon as there's any question of what to access."*.

Part 4 - Format. P1 prefers the "Half Screen". Because *"especially in case of danger, I think it's good if there is an explanation."*.

P2 thinks *"it is good if it is eye-catching and you notice it as much as possible"* and therefore chooses the whole screen.

5.5 Station 4: Which entity will provide the PA?

P1 says that it is *"always important for him that it is not a provider who would trade the data commercially on the other side. In other words, a provider that uses a privacy manager to cannibalize its own business model elsewhere. I would rather not trust that provider."*. He chooses the Chaos Computer Club as the provider because *"it is more likely to position itself as a consumer protector, which means as extremely critical. [...] They are even more critical than I am. And that's why this might be a good source to give me some guidelines on how I should behave."*

P2 chooses the university as the provider and explains her choice by saying that she would probably take something *"that seems trustworthy to me, and if I was going to study at university now, I would probably take a university."*

6 DISCUSSION

The aim of our pilot study was to create a basis for a discussion on the further development of the study design. Furthermore, the results of the two interviews can provide possible first indications of how users envision a PA. Since the sample is very small (N = 2), we will not discuss the results in detail here, but rather give an overview and a possible general direction. Finally, the methodological implementation will be discussed.

6.1 Discussion of the Results

The PAs developed by the participants in the study differ greatly in terms of which information participants are willing to share with the PA (Q1), how it should learn about them (Q2), how the PA should assist, and how should it communicate (Q3). It should be noted that both participants report a different level of privacy concerns and motivation to protect their privacy. These might be a hint that different user types have different ideas about what actions a PA should perform and how it should communicate with them. It may be useful to design PAs for a specific user group with similar requirements or think about how different user needs can be integrated in a PA.

6.2 Discussion of the Method

Our proposed method should make it possible to explore how users imagine their personal PA. For this purpose, the participants designed their PA in a workshop. With the help of think-aloud techniques and an interview, an insight into their perspective and decisions was captured. With our study design, we tried to create a balance between an open and concrete approach. On the one hand, we wanted to explore the user's view of a PA with an open mind. On the other hand, the questions and tasks should not be too abstract, so that the participants knew what they should relate to. The fact that there is still a need for adjustment here is particularly evident in the first station, where one participant initially states that she has almost no intention of disclosing personal data to the PA. This could be an indicator that participants find it difficult to estimate which data a PA needs in order to be functional. As a consequence, we will check all stations of the workshop to what extent an inexperienced participant can give a realistic assessment.

With the design of the study, we wanted to create a positive atmosphere in which participants feel encouraged to get creative with the design of their personal PA. In the offline study, the participant had both visual and haptic stimuli as well as a spatial dimension through the paper materials he could place on a pinboard. In addition, personal contact enabled the workshop assistant to create an atmosphere of trust. With the transfer to online studies, we wanted to continue to meet these requirements. This raises the question of how successful this has been and what other options are possible to implement the study design online. A possible indicator that the study design needs to be adjusted is the fact that the participant in the offline study answered in much more detail than the person in the person in the online study. Especially in times of the corona pandemic, the question arises on how innovative online studies can be designed that at the same time, ensure both the accessibility of the study and the privacy of the participants.

7 OUTLOOK

With our workshop approach, we provide a method to explore how users imagine their personal PA for app permissions. This study design can serve as a basis for further research, such as PAs for other contexts or with a focus on a certain aspect. We plan to implement the findings from the discussion on this work in progress paper as far as possible in the study design. Subsequently, a sample of N = 20 - 30 will be collected. The responses will be considered both quantitatively (number of options selected) and qualitatively by means of content analysis. With this study, we hope to provide valuable insights on users' perspective and their wishes for a PA.

ACKNOWLEDGMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050.

REFERENCES

[1] Yuvraj Agarwal and Malcolm Hall. 2013. 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*. ACM Press, Taipei, Taiwan, 97. https://doi.org/10.1145/2462456.2464460

[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2020. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[3] Florian Schaub Hazim Almuhimedi Shikun Zhang Norman Sadeh Alessandro Acquisti. and Yuvraj Agarwal Bin Liu, Mads Schaarup Andersen. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security.*

[4] Ted Boren and Judith Ramey. 2000. Thinking Aloud: Reconciling Theory and Practice. *IEEE transactions on professional communication* 43, 3 (2000), 261–278. https://doi.org/10.1109/47.867942

[5] Cheng Chang, Huaxin Li, Yichi Zhang, Suguo Du, Hui Cao, and Haojin Zhu. 2019. Automated and Personalized Privacy Policy Extraction Under GDPR Consideration. In *Wireless Algorithms, Systems, and Applications*, Edoardo S. Biagioni, Yao Zheng, and Siyao Cheng (Eds.). Vol. 11604. Springer International Publishing, Cham, 43–54. https://doi.org/10.1007/978-3-030-23597-0_4

[6] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. 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* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376389

[7] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. 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.* 1–13.

[8] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)* 13, 2 (June 2006), 135–178. https://doi.org/10.1145/1165734.1165735

[9] Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, and Mahadev Satyanarayanan. 2017. 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)*. IEEE, Honolulu, HI, USA, 1387–1396. https://doi.org/10.1109/CVPRW.2017.181

[10] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* 5228–5239.

[11] Gerald Eichler, Claudia Pohlink, and Wolfgang Kurz. 2020. The Telecommunication Data Cockpit – Full Control for the Household Community. In *Innovations for Community Services*, Siddharth Swarup Rautaray, Gerald Eichler, Christian Erfurth, and Günter Fahrnberger (Eds.). Vol. 1139. Springer International Publishing, Cham, 3–22. https://doi.org/10.1007/978-3-030-37484-6_1

[12] Lujun Fang and Kristen LeFevre. 2010. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web - WWW '10*. ACM Press, Raleigh, North Carolina, USA, 351. https://doi.org/10.1145/1772690.1772727

[13] Federal Trade Comission. 2017. Understanding Mobile Apps. https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

[14] Nina Gerber, Paul Gerber, Hannah Drews, Elisa Kirchner, Noah Schlegel, Tim Schmidt, and Lena Scholz. 2018. 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*. ACM Press, Orlando, Florida, 53–63. https://doi.org/10.1145/3167996.3167999

[15] Yangyang He. 2019. Recommending privacy settings for IoT. In *Proceedings of the 24th International Conference on Intelligent User Interfaces Companion - IUI '19*. ACM Press, Marina del Ray, California, 157–158. https://doi.org/10.1145/3308557.3308732

[16] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[17] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. 2013. Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies* 71, 12 (2013), 1144 – 1162. https://doi.org/10.1016/j.ijhcs.2013.06.003

[18] Bart P Knijnenburg, Martijn C Willemsen, and Stefan Hirtbach. 2010. Receiving recommendations and providing feedback: The user-experience of a recommender system. In *International Conference on Electronic Commerce and Web Technologies.* Springer, 207–216.

[19] Marc Langheinrich. 2002. A Privacy Awareness System for Ubiquitous Computing Environments. In *UbiComp 2002: Ubiquitous Computing*, Gaetano Borriello and Lars Erik Holmquist (Eds.). Vol. 2498. Springer Berlin Heidelberg, Berlin, Heidelberg, 237–245. https://doi.org/10.1007/3-540-45809-3_19

[20] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[21] Mary Madden. 2012. Privacy management on social media sites. *Pew Internet Report* (2012), 1–20.

[22] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühläuser. 2020. "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the Nordic conference on Human-Computer Interaction (NordiCHI '20)*. ACM, New York, USA.

[23] Michal Jakob, Zbyněk Moler, Zbynek Michal Pechoucek, Roman Vaculín. 2011. Intelligent Content-based Privacy Assistant for Facebook. In *International Conferences on Web Intelligence and Intelligent Agent Technology.*

[24] Tehila Minkus and Nasir Memon. 2014. Leveraging personalization to facilitate privacy. *Available at SSRN 2448026* (2014).

[25] 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. 2017. 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)*. IEEE, Atlanta, GA, USA, 193–198. https://doi.org/10.1109/ICDCSW.2017.52

[26] X. Pham, T. Nguyen, W. Hwang, and G. Chen. 2016. Effects of Push Notifications on Learner Engagement in a Mobile Learning App. In *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*. 90–94.

[27] Hannah Quay-de la Vallee, Paige Selby, and Shriram Krishnamurthi. 2016. 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*. ACM Press, Vienna, Austria, 63–72. https://doi.org/10.1145/2994459.2994466

[28] Frederic Raber and Antonio Krüger. 2018. Privacy perceiver: Using social network posts to derive users' privacy measures. In *Adjunct Publication of the 26th Conference on User Modeling, Adaptation and Personalization.* 227–232.

[29] Frederic Raber, David Ziemann, Antonio Krueger, C Weir, and M Mazurek. 2018. 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.*

[30] Bahman Rashidi, Carol Fung, and Tam Vu. 2015. Dude, ask the experts!: Android resource access permission recommendation with RecDroid. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, Ottawa, ON, Canada, 296–304. https://doi.org/10.1109/INM.2015.7140304

[31] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. *arXiv:2001.09077 [cs]* (Jan. 2020). https://doi.org/10.1145/3313831.3376264 arXiv: 2001.09077.

[32] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. ACM Press, Toronto, Ontario, Canada, 2347–2356. https://doi.org/10.1145/2556288.2557421

[33] Ali Sunyaev, Tobias Dehling, and Manuel Schmidt-Kraepelin. 2018. *Verbraucherorientierter Datenschutz Identifizierung von Verbraucherarchetypen zur effektiven Kommunikation von Datenschutzpraktiken.* 163–179. https://doi.org/10.15501/978-3-86336-920-0_8

[34] Hua-Zhe Tan, Wei Zhao, and Hai-Hua Shen. 2018. A Context-Perceptual Privacy Protection Approach on Android Devices. In *2018 IEEE International Conference on Communications (ICC)*. IEEE, Kansas City, MO, 1–7. https://doi.org/10.1109/ICC.2018.8422188

[35] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[36] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 1077–1093. https://doi.org/10.1109/SP.2017.51

[37] Pamela Wisniewski, A.K.M. Najmul Islam, Bart P. Knijnenburg, and Sameer Patil. 2015. Give Social Network Users the Privacy They Want. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1427–1441. https://doi.org/10.1145/2675133.2675256

[38] Pamela J Wisniewski, Bart P Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies* 98 (2017), 95–108.

[39] Ruijing Zhao, Izak Benbasat, and Hasan Cavusoglu. 2019. DO USERS ALWAYS WANT TO KNOW MORE? INVESTIGATING THE RELATIONSHIP BETWEEN SYSTEM TRANSPARENCY AND USERS'TRUST IN ADVICE-GIVING SYSTEMS. In *Proceedings of the 27th European Conference on Information Systems (ECIS)*.