The Influence of Transparency and Control on the Willingness of Data Sharing in Adaptive Mobile Apps

FLORIAN BEMMANN, LMU Munich, Germany
MAXIMILIANE WINDL, LMU Munich, Germany
JONAS ERBE, LMU Munich, Germany
SVEN MAYER, LMU Munich, Germany
HEINRICH HUSSMANN, LMU Munich, Germany

Today, adaptive mobile applications use mobile sensing and user tracking, allowing for adaptation to the users' context and needs. This raises several privacy concerns. Privacy dashboards provide transparency and sharing control; however, their impact on the users' behavior is unclear. To shed light on the effects of (a) transparency and (b) control features, we developed a mobile sensing privacy dashboard and evaluated it in the wild (N=227). We found that the pure presentation of raw logging data is rather deterring, and users tend to use the app less, but offering the user control over the data collection can compensate for that. Users used the control features rarely and, as such, did not affect the data collocation. Our work informs the design of future privacy-enhancing interfaces in applications relying on passively collected mobile sensing data. Moreover, our results encourage the adoption of privacy dashboards in the applications and relieve developers from concerns about the negative influences of transparency information on the quality of collected data.

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

Additional Key Words and Phrases: mobile sensing, privacy, reflection, data collection

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

1 INTRODUCTION

Using ubiquitous and mobile technology, developers track various kinds of user behavior data, e.g., location [38], physiological data [30], and mobile behavior [35]. These tracking features make it possible to build adaptive and intelligent user interfaces that provide the user with information right when needed [23]. On the other hand, the concerns of users about privacy in mobile sensing apps are often disregarded, and user-friendly solutions to provide transparency about data usage are rare cf. [12]. As a result, most users are unaware of the kinds of data used [43] and the actions performed with the collected information [37, 45]. This leads to privacy concerns [20, 32], which may lead to people not using an application. In mobile sensing research studies, where an app is

Authors' addresses: Florian Bemmann, LMU Munich, Frauenlobstr. 7a, Munich, 80337, Germany, florian.bemmann@ifi.lmu.de; Maximiliane Windl, LMU Munich, Frauenlobstr. 7a, Munich, 80337, Germany, maximiliane.windl@ifi.lmu.de; Jonas Erbe, LMU Munich, Frauenlobstr. 7a, Munich, 80337, Germany, XXX@ifi.lmu.de; Sven Mayer, LMU Munich, Frauenlobstr. 7a, Munich, 80337, Germany, info@sven-mayer.com; Heinrich Hussmann, LMU Munich, Frauenlobstr. 7a, Munich, Germany, 80539, hussmann@ifi.lmu.de.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
2573-0142/2022/9-ART189 $15.00
https://doi.org/10.1145/3546724

deployed in the wild to collect user data, these concerns led to much lower consent rates than in traditional studies [20, 22, 32]. Previous research proposed the concept of "consent as a process" to tackle these issues, including making the logging process transparent and giving the users control over their data [13].

Privacy dashboards are one way to incorporate transparency and control into the apps [14]. While research on the effects of privacy dashboards indicates positive results [46], other studies revealed none [18] or even contradictory effects [16]. A promising direction is supplementing transparency with control which has already been shown to mitigate the adverse side effects of transparency [10, 14]. For example, increased transparency decreased trust and willingness to share data [17, 34]. However, those studies were either conducted in the domain of actively donated data [14], conducted as vignette studies [18, 20] or did not evaluate transparency and control independently [18, 46]. Thus, developers of mobile sensing applications in industry and research cannot build on insights on the effects of a privacy dashboard incorporating both features. Overall, the literature showed that privacy dashboards are promising but need a well-informed design to avoid adverse effects [10].

In the following, we address how privacy dashboards can help users be informed and how they help users gain control over their data. Both questions are crucial for developers as we do not know how these two factors influence usage rates of passive sensing-based apps (i.e., study participation rates), whether they manipulate the users' real-world behavior, and which effects arise on the resulting data. Therefore, we built a privacy dashboard for a mobile sensing app. The dashboard addresses both questions with one distinct set of features for each question. While the *Transparency Features* visualize the logged data in the privacy dashboard, the *Control Features* allow the users to stop or pause the logging or delete already logged information post-hoc. To understand how both features impact the usage, we ran a 2×2 in-the-wild study (N=227). We compare variants of a mobile sensing app in a between-groups design with 1) no privacy dashboard (baseline), 2) a privacy dashboard with only *Transparency Features*, 3) only *Control Features*, and 4) both types of features.

As a result of our in-the-wild study, we contribute a detailed analysis of the effects of the factors "transparency" and "control" on the app usage rates across the entire process, from advertising the app over the installation and permission granting steps to dropout rates. Our results show that transparency features should not be incorporated alone but instead be combined with the ability to control the data logging. Nevertheless, the effects on the resulting log data are negligible. The sole presence of the control features appears to give users a good amount of trust in the app, and as a consequence, they use them very rarely. This is promising for application developers of mobile sensing apps in both industry and research since privacy, user perception, and adoption rates of their systems can be improved without affecting the quality of collected data.

2 RELATED WORK

In the following, we first reflect on privacy in mobile sensing apps. Next, we define privacy dashboards and explain how they are designed before reporting on literature about the effects of transparency and control in privacy-enhancing technologies. Finally, we summarize the related work and explain how our study fills a significant gap in the literature.

2.1 Privacy in Mobile Sensing Applications

Various theories explain how and why users behave privacy-wise. The Privacy Calculus Theory [29] states that users weigh the risks and benefits of disclosing their data to come to a decision. For example, the perceived social benefits outweigh the risk of data privacy issues for social media apps. The relation between willingness to be profiled and the desire for transparency features is

described by the Personalization-Privacy Paradox [2]: Users who value transparency features are less willing to be tracked and profiled. Karwatzki et al. [18] justify this with those people being "privacy fundamentalists," which means that they are careful with their data in general and value privacy more. Moreover, the Privacy Paradox states that users are generally concerned about their privacy; however, this is not reflected in their behavior [1, 26].

Klasnja et al. [21] interviewed participants of a personal context-sensing study on their privacy concerns. They found that people were primarily concerned about higher-level features derived from data than the raw data itself. For example, the ability to derive one's home address was rated more critical than the continuous GPS data collection. As a remedy, they suggest explanations of what an app is doing in the background, alongside features offering transparency and control on what data is recorded.

According to Harari et al. [13], privacy should be incorporated into the entire process of self-tracking systems. Hence, transparency must be facilitated during each stage, opt-in should be adopted as the default setting, and control should be provided throughout each stage. Harari et al. [13] thereby distinguish between the two general privacy concepts of offering (1) transparency and (2) control. The demand for control resulted from a vignette study on the willingness to use passive mobile data collection technologies by Keusch et al. [20], where participants commented on a lack of control over their data. In our study, we follow up on Harari et al.'s [13] distinction and analyze the effect of the two concepts.

2.2 Transparency and Control in Privacy Dashboards

In this section, we introduce privacy dashboards as a means to tackle the privacy issues and implement the privacy tool suggestions derived from the previous section. We first define privacy dashboards, describe existing privacy dashboard projects, and finally give an overview of work on transparency and control in privacy dashboards.

The privacy dashboard is a common privacy design pattern [8]. Other privacy design patterns are, for example, the *Personal Data Table* and *Privacy Policy Icons* [41]. Privacy dashboards make users aware of the data services have collected about them. They should provide successive summaries of the collected data and give an easily understandable overview [8, 55]. For this, they can use demonstrative examples, predictive models, visualizations, or statistics. Additionally, a privacy dashboard can provide control options and privacy settings to empower users to control the processing and collection of future data, cf. [8, 55]. Especially actions like deletion and correction of data are highlighted. Finally, privacy dashboards should give an overview rather than presenting every detail of possibly thousands of data items [41].

Privacy dashboards are spreading in practice, for example, the Google Privacy Dashboard[1], and have become subject to research. They were examined as a European General Data Protection Regulation (GDPR)[2] compliant alternative to consent forms [5]. They were studied as tools to give users a sense of what data is collected and inform the user instead of listing every detail [2, 18]. Raschke et al. [31] implemented a comprehensive privacy dashboard that adapts the newsfeed concept from social media. The dashboard incorporates transparency and control features so that users can view the collected data and learn about the purpose by obtaining information about involved processors, requesting rectification or erasure of each data item in the timeline, or reviewing and withdrawing the consent for each individual data type.

Privacy dashboards are a tool to implement the principles of *notice and choice* [36, 51], often through features that provide transparency and control [39]. Transparency and control have

[1] https://myaccount.google.com/dashboard, last accessed 25th of July 2022
[2] https://gdpr.eu/what-is-gdpr, last accessed 25th of July 2022

Table 1. Studies on the effects of transparency (T) and control (C) in privacy dashboards, their context, methodology, and findings. Most studies were conducted with vignette or survey methodologies, while evaluations of real behavior are rare.

Paper	T	C	Finding	Context	Method
Keusch 2019 [20]	✗	✓	An option to switch off data collection would significantly increase the willingness to participate	mobile sensing studies	vignette study
Tsai 2011 [46]	✓	✗	Transparent privacy information policies increase the usage of the service and even justify higher prices	online purchasing	between-subject lab experiment
Elevelt 2019 [9]	✗	✓	74% of the participants continued sharing their GPS data although they could have opted out	smartphone sensing	Longitudinal diary study with sensing (enabled by default, opt out possible)
Awad 2006 [2]	✓	✗	Acceptance of tracking and effects of transparency vary with personality	personalization in online shops	survey
Karwatzki 2017 [18]	✓	✗	Transparency has no positive effect on willingness to disclose information	personalization of event finding online service	evaluation of screenshots in 2x2 design
Farke 2021 [10]	✓	✓	Transparency reduces concerns, control features are used rarely	Google Privacy Dashboard	interview after guided usage
Herder 2020 [14]	✓	✓	Control and transparency on raw data increase trust, while transparency on derived data decreased trust but increases concerns	online purchasing	vignette study with assessment of behavior intention
Schnorf 2014 [39]	✓	✓	Depending on the user predisposition, transparency can also raise anxiety	inferred user interests	survey
van Kleek 2017 [47]	✓	✗	Transparency on what happens with their data increases user confidence when deciding for an app	mobile app choice	prototype study

long been studied in the context of mobile systems. Permission popups force mobile apps to provide transparency and control about what data an app can access [11]. However, the context is limited [48]. Permission popups lack appropriate information and contain hardly understandable terms, making it hard for users to grasp the implications of granting permission [19]. Also, the amount of information conveyed to the user leaves space for improvement [4, 11]. In contrast, interfaces that provide more detailed information on what happens with the data increase user confidence [47]. In the web context, similar issues are proliferated. Privacy policies are long and hard to understand and, thus, often ignored [28]. In addition, they fail to provide sufficient transparency to the user [4]. Here, consent popups may even be designed to nudge users towards illegal configurations [27].

Permission popups offer transparency and control before the data logging happens. In contrast, privacy dashboards take effect afterward. The retrospective approach has the advantage that the user can be informed about what has actually been logged. Transparency and control features, incorporated through privacy dashboards, have shown positive effects: The Google privacy dashboard [10] and a dashboard for online shopping [14] increased user trust. However, this is only valid for raw data: In the study of Herder and van Maaren [14], showing derived data increased perceived privacy risk and reduced user trust. Perceived risks and trust may lead to fewer people using a service, not sharing required data, or dropping out early. For example, in vignette studies, participants indicated to prefer using a service that provides transparency over the logged data [2, 20, 46] or an option to switch off the data collection [20]. However, while control features show a positive effect, they are only seldomly used. In the studies by Farke and Elevelt only a quarter of the participants involved had already used or indicated a willingness to use such features in the future [9, 10].

While the previously reported studies in the contexts of webshops, surveys, and personalization of online services agree that the provision of decision-relevant information is positive [54], the literature is contradictory in the context of sensing data [18]. Here, transparency increases privacy

concerns resulting in less data disclosure [17]. This inverse impact of transparency features can also be found in studies on personalized advertisements [49] and inferred user interests [39]. Also, the reaction to transparency features depends on the user's privacy predisposition [39]. To give an overview, we show studies evaluating the effects of transparency and control with their context, methodology, and findings in Table 1.

3 RESEARCH QUESTIONS

Incorporating privacy-enhancing features that provide transparency (e.g., [2, 20, 46]) and control (e.g., [20]) have positively affected users' trust and privacy concerns. Furthermore, vignette studies indicated positive effects on the usage of such services [18, 20]. However, it is unclear whether those effects hold in a real application, especially in the light of the Privacy Paradox that indicates discrepancies between behavioral intentions and real-world behavior, cf. [1, 26]. Further, most research has been conducted in the context of online shops or personalized adaptive services and was fueled by data actively provided to the system by its user. In contrast, only a few works exist in mobile passive sensing applications, where data is collected without the user's active involvement. And if so, studies used vignette methodologies and only assessed user intention via self-reports instead of actual behavior. Yet, to the best of our knowledge, no study measured the effects on participation rates and app usage, the resulting data (i.e., gaps), the privacy concerns, and trust in mobile sensing apps equipped with a privacy dashboard while treating transparency and control features as two independent factors. To address this gap, we define the following research questions:

RQ1 How do transparency and control in a privacy dashboard affect the number of users adopting and dropping out of a passive mobile sensing app?

RQ2 How do transparency and control in a privacy dashboard affect the awareness of and knowledge about the data logging?

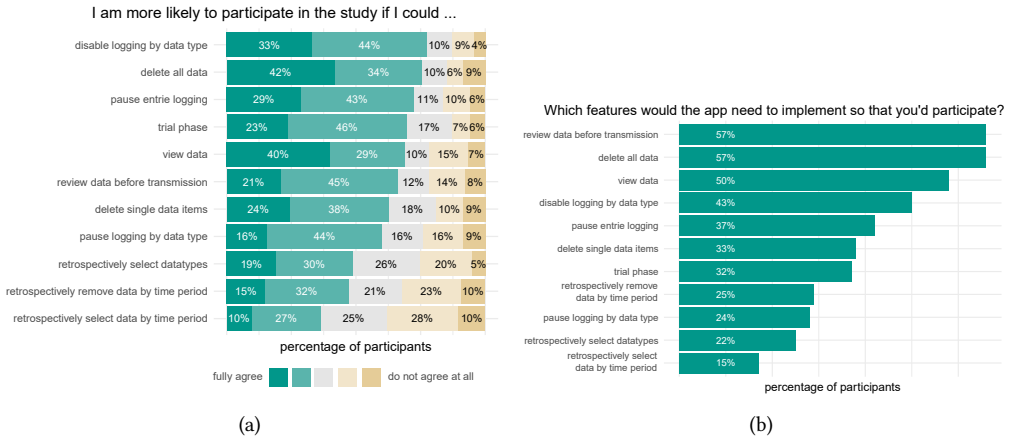
RQ3 How do transparency and control in a privacy dashboard induce behavior change and self-reflection and thus the logged data of a passive mobile sensing app?

RQ4 How do transparency and control in a privacy dashboard affect a passive mobile sensing system user's privacy concerns and trust?

We compared four privacy dashboard variants to investigate these research questions: Transparency and control, either transparency or control, and a baseline variant without both. This 2x2 factorial design allowed us to evaluate the effects of transparency and control independently. In addition, we deployed the privacy dashboard as part of a passive mobile sensing app in the wild ($N = 227$) to overcome the limitations of related work that often relied on vignette studies. In the beginning, we did not tell participants that the privacy dashboard was the study's primary objective to be able to measure natural, unbiased behavior. We started with a preliminary survey to operationalize transparency and control and decide which features to implement in the dashboard.

4 PRELIMINARY SURVEY

We first assessed which transparency and control features are important to users to inform the development of our privacy dashboard. Then, we aimed to incorporate only essential features to not overwhelm the users. We conducted a survey (N=118) to determine which transparency and control features are most important for users. Therefore, we presented our participants with a vignette of a hypothetical mobile sensing scenario and asked how likely they were to participate in that study. The design of the vignette study, including the questions, is adopted from Keusch et al. [20]. The participants rated a set of privacy dashboard transparency and control features on a 5-point Likert scale for their likeliness to increase their willingness to participate. We collected the presented features from related work by constructing a list of features these papers used to implement



(a) (b)

Fig. 1. Results of our preliminary survey to inform the privacy dashboard design. We implemented all features where the majority of the participants fully agreed or rather agreed that it would increase their likelihood to participate (a).

transparency or control in their privacy dashboards [20, 31]. We further asked them to select a minimal set of features that they would like to have in a hypothetical mobile sensing application. Finally, we incorporated all features desired by most of the users into our privacy dashboard design.

4.1 Participants

The sample consisted mainly of students (62%) and employees of IT companies (20%). Their mean age was 27 years (SD = 8.4). The following insights are based on 115 participants (3 participants stated in the first question that they would participate in the vignette study in any case, and thus we could not ask them about features to improve their participation likelihood).

4.2 Results

Detailed control features were the most desired. Disabling data logging ranked high in both questions, whereas fine-grained control (disabling single data types, 77% agreed) was more desired than disabling the full logging (72% agreed). They also desired the option to delete all data (76% agreed) and single data types (60% agreed). Further, the transparency features to view the recorded data (69% agreed), and a trial phase (70% agreed) were rated to increase participation likelihood. Participants rated retrospective features as less critical. Less than half of the participants stated that retrospectively deleting data of specific periods (47% agreed), exclusively allowing data of specific periods (37% agreed), or removing data of single data types (49% agreed) would increase their likelihood of participating.

5 STUDY

We conducted the study with the PhoneStudy app[3] and added a privacy dashboard to understand the impact of transparency and control. We evaluated the mobile sensing privacy dashboard in a 2×2 factorial study design, with the presence of (a) Transparency and (b) Control features as the independent variables. Thus, each participant was assigned to one of the following four conditions:

[3] https://phonestudy.org/, last accessed 25th of July 2022

- *Baseline*: The mobile sensing app without any possibility to view logged data or control the logging
- *Transparency Features*: The app with a privacy dashboard that allows users to view the data but not delete or pause data entries (Figure 2 1-4)
- *Control Features*: The app with control features where users can pause the data logging (Figure 2 5-7)
- *Both*: The app with both a dashboard to view data and control features to pause logging and delete data entries (Figure 2 1-8).

This modular design allowed us to turn single features on and off depending on a user's study condition. Following our research questions, we can hence study the behavior of users who were exposed to one of the two factors independently and compare how our dependent variables behave. Hence, in contrast to studies from related work, we can evaluate the effects of transparency and control features individually.

5.1 Apparatus

The PhoneStudy app collects the sensing data, incorporates the privacy dashboard, and implements study management features such as prompting questionnaires when desired by the researcher. It was available for Android (version 6 or above) and was distributed as an APK file. We implemented the privacy dashboard as a web app built with the React JavaScript Framework to make it as reusable as possible for other applications. For this study, it was seamlessly integrated into the sensing app using an Android WebView. WebViews allow direct communication between its JavaScript environment and the native Android code[4], such as displaying and deleting data from within the dashboard. The control features to pause the data collection were implemented via a native Android screen. The sensing app communicated with a central server to control the study flow and gather the data. This also allowed the distribution of the questionnaires at specific study stages via push notifications. The questionnaires were implemented in the online survey platform SoSci Survey[5]. Thus, we could run our study completely remotely.

We made the following design decisions for the privacy dashboard: 1) We only show raw data but no aggregations and interpretations. Raw data is the first step in every data processing workflow and is thus present in every mobile sensing application. Furthermore, the effects of aggregations and interpretations are highly dependent on their precise design and implementation. Since we wanted to keep our results generalizable and independent of one specific application case, we forward such analyses to future work. 2) Informed by the results of the preliminary survey, we implemented all features, where the majority of the participants fully or rather agreed that they would increase their likelihood to participate. We list the resulting set of features in Table 2. 3) The privacy dashboard has two main screens. A *view data* screen that mainly implements the *Transparency Features* and a *settings* screen that contains most control features. Figure 2 shows a visualization of the structure, and Table 2 explains how the agreed-on features are incorporated. 4) The timeline concept of the *view data* screen is informed by the privacy dashboard of Raschke et al. [31]. Each data item is listed in chronological order, beginning with the newest. In contrast to theirs, our dashboard is optimized for smartphone screens, i.e., controls to configure filters like time range, data type, etc., are hidden in menus. While deleting data is supported in the according study condition as well, we did not include features to rectify erroneous data. Multiple items of the same type in a row are

[4] https://developer.android.com/reference/android/webkit/WebView, last accessed: 25th of July 2022
[5] https://www.soscisurvey.de, last accessed: 25th of July 2022

Table 2. In this table we show the features derived from our preliminary survey and requirement analysis (left column) and matches it to how each feature is implemented in the dashboard (column *Implementation*). The three rightmost columns denote in which of the experimental conditions each feature is present: Transparent Features (T), Control Features (C), and Both (B).

Feature	**Implementation**	*T*	*C*	*B*
Disable logging by data type	In the *Settings* screen **(5)** one can disable the logging via data type specific toggles.	✗	✓	✓
Delete all data	Is already implemented in a dedicated tab to fulfill the privacy regulations.	✓	✓	✓
Pause entire logging	In the *Settings* screen all toggles can be turned off, and a pause duration in hours can be specified **(6)**.	✗	✓	✓
Trial phase	The first data items are uploaded after 24 hours, thus one can uninstall the app within the first day without data being transmitted.	✓	✓	✓
View data	In the *View Data* tab a timeline visualizes all logged data items **(1)**. Additionally a detail view **(2)** which is accessible via a context menu **(8)**, raw data view **(3)**, and explanations **(4)** about what can be inferred from the data are provided. The timeline can be filtered by datatype and timerange **(9)**.	✓	✗	✓
Review data before transmission	Data is uploaded only after 24 hours, thus one has time to view and withdraw before transmission by deleting all data of the current filter selection **(7)** or single data items via an item's context menu **(8)**.	✗	✗	✓
Pause logging by data type	The toggles in the *Settings* screen allow to set a pause duration **(6)**.	✗	✓	✓

collapsed (e.g., "9 more app usages") but can be expanded on demand. In general, all views follow Google's design standard *Material Design*[6].

5.2 Procedure

We used convenience sampling to recruit our participants (via email lists, social media, and Slack). The advertisement contained only a little information. We merely advertised it as a study on smartphone usage in daily life. For further information, the ad referred to an onboarding questionnaire to reduce the risk of a hidden selection bias by privacy disposition (DTVP) [18]. If people drop out in the onboarding questionnaire instead of the study ad, we could count them. When opening the onboarding questionnaire, users were randomly assigned to one of the four study conditions. Then the study details (e.g., mobile sensing app has to be installed, data is logged, study duration) were introduced to the potential participants. In addition, for the non-baseline condition, we advertised the respective privacy features prominently. Via this onboarding procedure, we could retrace how the transparency and control features already influenced the decision to install the mobile sensing app. Thus, monitoring the "interest in the study." The participants could download the app via a QR Code or a link. In the non-baseline condition, the setup process started with an intro slider where the respective privacy features were again advertised. Afterward, participants had to walk through a four-step setup process to accept the app's privacy policy and grant the necessary system permissions. The app then summarized the study procedure. Finally, the app prompted a link to the pre-study questionnaire (see Section 5.3.1 for the instruments).

Participants should then keep the app on their phone for seven days while data was passively logged in the background. Our app logged smartphone behavior (i.e., opening and closing apps), connectivity status (i.e., wifi and Bluetooth status), and high-level activity data (like walking, biking, or running[7]). After two days, the app reminded the participants about the transparency and control

[6] https://material.io/design, last accessed 25th of July 2022

[7] Retrieved via the Google Awareness API activity recognition, https://developers.google.com/awareness/android-api/snapshot-get-data#get_the_current_activity, last accessed 25th of July 2022

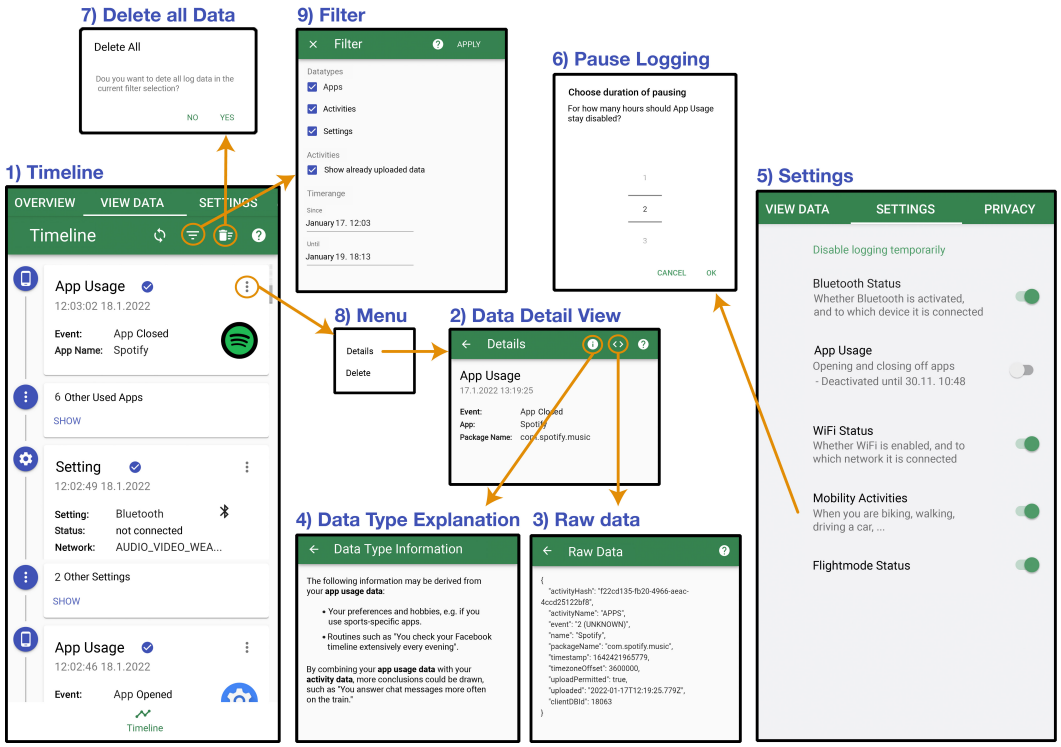


Fig. 2. The UI of our privacy dashboard is structured into two main components: The timeline view (1-4) that offers transparency, and the settings features (5-7) that implement control over the data logging.

features via a notification. After seven days, the app prompted the post-study questionnaire via a notification (see Section 5.3.3 for the instruments). At the end of that questionnaire, participants chose their compensation, and the study was finished. We compensated participants for their participation with either 15€ via PayPal or a respective amount of study points that can be credited at our university[8]. We visualize the study procedure in Figure 3. According to the ethics approval procedures at our faculty, we assessed our study with the ethics committee's questionnaire. As a result, we concluded that it was not ethically questionable and forwarded the completed questionnaire to the ethics committee.

5.3 Measurements and Logs

The collected data consists of three parts: 1) a pre-study questionnaire in the app, 2) the app usage data, and 3) a post-study questionnaire. We chose this study design to observe changes in behavior and knowledge. Moreover, some measurements need to be collected before to get unbiased insights (e.g., the prior privacy experience), and others can only be collected after using the dashboard (e.g., behavior change and self-reflection).

5.3.1 Pre-Study Questionnaire. After installing the app, the pre-study questionnaire was prompted via a notification which took approximately 5 minutes to complete. There we assessed participants'

[8]The participation in the study is still anonymous, and data required for compensation and study credits is kept independent of the study sensing data and questionnaire answers.

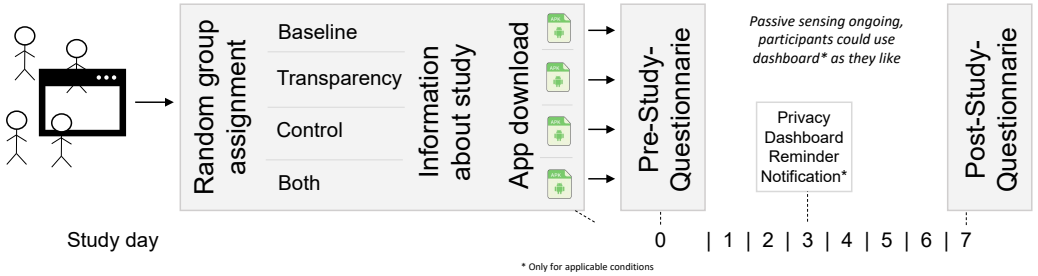


Fig. 3. A flowchart visualizing the procedure of our study. Potential participants were recruited with a sparse study description (i.e. not mentioning that a mobile sensing app is involved). When they clicked on the onboarding link which was realized with an online questionnaire tool, they were immediately randomly assigned to one of the four study conditions. Afterward, the full information about the study was presented, mentioning the privacy dashboard in the applicable conditions, and the condition-specific Android app could be downloaded. After the installation participants had to fill out the pre-study questionnaire, on day seven the post-study questionnaire.

prior privacy experience and how good they were informed about what data was logged during the study and what happened with their data:

- Prior privacy experience: Contributing to RQ4, we used the construct collection of Degirmenci et al. [6], which consists of adaptions of the items about prior privacy experience from Xu, Gupta et al. [52], computer anxiety by Stewart and Segars [44], perceived control by Xu, Teo et al. [53], and app permission concerns by Smith et al. [42] (see Table 6).
- Knowledge about data logging: A set of self-constructed items constituting a data logging quiz. It consists of 12 statements about logging, e.g., " The PhoneStudy app is logging my precise location (GPS coordinates)." The participants had to rate each item whether it was true, false, or they did not know. We use this information to answer RQ2 (see Table 7).
- Knowledge of how data is processed: Also corresponding to RQ2, we constructed another set of items constituting a data processing quiz. It consists of 10 statements on where the data is processed (e.g., "The collected data is never leaving my smartphone"), who has access (e.g., "My collected data is accessible for everybody on the internet") or anonymization (e.g., "The collected data is anonymous, i.e., cannot be connected to my real-world identity"). Equivalent to the items on knowledge about data logging, participants had to rate whether each statement was true, false, or they did not know (Table 7).

5.3.2 App Usage Logging. The PhoneStudy app tracks its usage to determine how participants used the privacy dashboard and control features. We track lifecycle events of the PhoneStudy app screens and detailed usage of the privacy dashboard (which log items were visible, if the detail view was clicked, if a filter was applied). Furthermore, usages of the control features were logged (e.g., which data items were deleted, when the logging was paused). Among others, we need this information to investigate RQ3, as the usage of control features directly affects the resulting log data.

5.3.3 Post-Study Questionnaire. At the end of the study period, another questionnaire was prompted via a notification. Here we assessed whether the privacy perception and knowledge about data logging and processing changed during the study, how the control features were used (if present), which effects the app usage had on the participants, and whether the app was usable in general. The

post-study questionnaire took approximately 8 minutes and ended with the choice of compensation. In detail, the questionnaire inquired about the following factors:

- Prior privacy experience (repetition, cf. Section 5.3.1)
- Knowledge about data logging (repetition, cf. Section 5.3.1)
- Knowledge of how the data is processed (repetition, cf. Section 5.3.1)
- Data deletion behavior (condition *Control* only): Freetext and slider items on how many data items participants deleted in total, how many of which data types, why they did it, and in which situations (RQ3) (see Table 3).
- Logging pausing behavior: Freetext and slider items on how often the logging was paused in total, how often for which data types, why they did it, and in which situations (RQ3) (see Table 3).
- Behavior change and self-reflection: Four self-constructed items, inspired by the Technology-Supported Reflection Inventory of Bentvelzen et al. [3], on how the app usage affected smartphone usage, real-world behavior, and self insights. Additionally, a free text item on what changed and why (RQ3) (see Table 9).
- Logging awareness: Four self-constructed items on how aware participants were of the logging, whether this awareness influenced them, and if yes, what and why (RQ2) (see Table 10).
- Usability and other comments: Finally, we assessed the UEQ item groups on attractivity, perspicuity, and stimulation. [40]. Furthermore, participants could enter any comments or remarks on the app and study in a free text field (see Table 11).

5.4 Data Analysis

The Android app sends its log data to our central server, where the data of all users is collected. The questionnaire data, which we initially stored at a university server, is also imported here. The raw data is not exported to the researchers' local computers for privacy and security reasons but instead analyzed on the server. Therefore we use an RStudio Server[9] instance running the statistics language R[10] at version 4.1.3. We provide the preprocessing script files and the aggregated data in a Jupyter Notebook: https://github.com/mimuc/mobilehci22-transparency-and-control.

6 RESULTS

In the following, we present the results of our evaluation of the privacy dashboard's transparency and control features in the wild. Each of the following subsections corresponds to one of our research questions: We show how transparency and control features affect the app installation rate, usage, and dropout (RQ1); evaluate which effects on privacy concerns and trust are raised by both aspects (RQ4); how aware users are about the logging and whether the knowledge about the logging differs (RQ3); and whether induced behavior change and self-reflection could be noticed, thus the resulting data is influenced by the two factors (RQ2).

6.1 Mobile Sensing App Usage

In this section, we show which influence the experimental conditions had on how many participants installed our mobile sensing app, how long they kept it on their phones, and how much they actively used the app with its respective privacy features. These objectives correspond to RQ1.

In total, 1286 potential users opened the onboarding questionnaire through our study advertisement. Already here, they were equally assigned to the four experimental conditions. Of those, 17.7%

[9] https://www.rstudio.com/products/rstudio/#rstudio-server, last accessed: 25th of July 2022
[10] https://www.r-project.org/, last accessed: 25th of July 2022

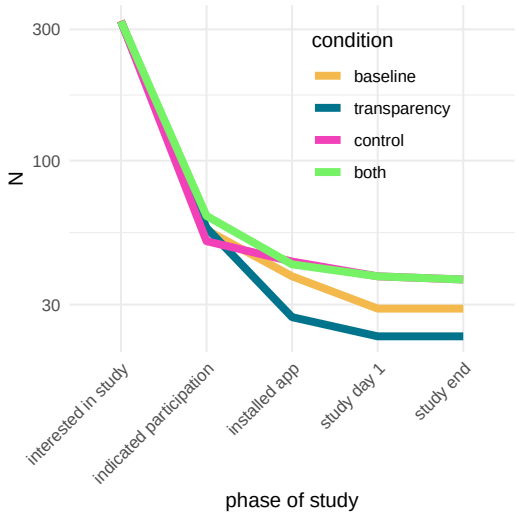


Fig. 4. Participation rates throughout our mobile sensing study. Users with the control features were significantly more likely to install the app, whereas users with the transparency features were significantly less likely to do so.

(227) finished the onboarding questionnaire and indicated a willingness to install the app, roughly equally across the conditions ($\chi^2(3) = 1.607$, $p = .658$). Of those who indicated a willingness, 66.1% actually installed the app and granted the required system permissions. There was a significant difference between users who indicated participation and those who installed the app ($\chi^2(3) = 16.557$, $p = .0009$). Post hoc comparisons revealed that users with the *Control Features* installed the app, significantly more often (84.3%), while significantly fewer users with *Transparency Features* did so (47.4%). After having installed the app the dropout was comparatively low. 85.3% of those who installed the app kept it for at least one day ($\chi^2(3) = 3.674$, $p = .299$), 84.0% for 7 days (until end of the study) ($\chi^2(3) = 1.390$, $p = .708$).

Dashboard Usage: Factor Transparency. Throughout the 7-days study, the users who had the possibility to view their data in the privacy dashboard (*Transparency Features* and *Both*) did so on average 14.60 times. A Mann-Whitney U Test ($W = 631.5$, $p = .430$) showed no differences between

Table 3. The number of participants throughout each study stage. The relative values relate to the stage before, i.e. report how many users continued since the previous stage.

	Baseline		*Transparency*		*Control*		*Both*		**Total**	
Study Phase	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Interest in Study	322	100.0%	321	100.0%	322	100.0%	321	100.0%	1286	100.0%
Indicated Participation	56	17.4%	57	17.8%	51	15.8%	63	19.6%	227	17.7%
App Installed	38	67.9%	27	47.4%	43	84.3%	42	66.7%	150	66.1%
Study Day One	29	76.3%	23	85.2%	38	88.4%	38	90.5%	128	85.3%
Study End	29	100.0%	23	100.0%	37	97.4%	37	97.4%	126	98.4%

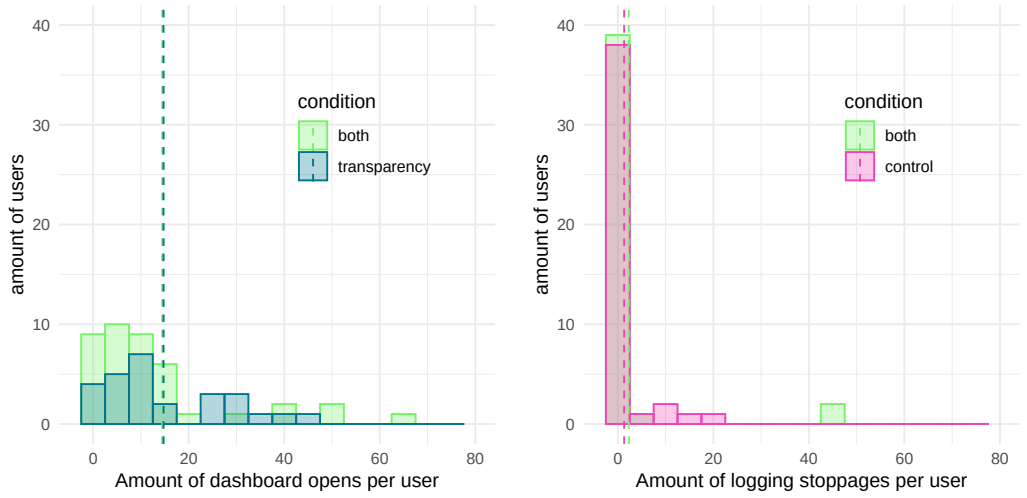


Fig. 5. Histograms visualizing the average usage frequency of the provided privacy features per user. The dashed lines shows the group mean. Users with the factor transparency (a) used the privacy dashboard on average 14.74 (*Transparency Features*) resp. 14.45 (*Both*) times. The features of factor control (b) in contrast were used very rarely, on average 1.33 times (*Control Features*) resp. 2.29 times (*Both*).

the conditions ($M_{Transparency}$ = 14.74, M_{Both} = 14.45). The distribution of usage frequencies (visualized in Figure 5) is common, with a peak at around ten times, a set of more frequent users that opened the dashboard between 20 and 50 times, and a few outliers with up to 80 usages. Due to the data not being normally distributed according to a Levene test, we used the nonparametric Mann-Whitney U test instead of a standard t-test.

Dashboard Usage: Factor Control. Those who had the option to control the logging, i.e., turning the logging of specific data features off or deleting data entries, made only rarely use of that. The average user paused the logging of one datatype 1.8 times ($M_{Control}$ = 1.33, M_{both} = 2.29; Mann-Whitney U Test: W = 960, p = .395). The frequency distribution shows that the majority of the users did not use that feature at all (74 out of 85 users in *Control Features* and *Both*, resp. 87.06%).

Participants in the condition *Both* additionally could delete data entries from within the dashboard. This feature was used even more rarely by only 3 out of 42 users. In total, 15 data entries were deleted.

6.2 Logging Awareness and Knowledge

We assess how much the participants know about (1) what happens with their data and (2) what data is logged during the study to answer RQ2. Therefore, we used items designed as a data logging quiz and data processing quiz that had to be answered in the pre-study and post-study questionnaires.

6.2.1 Data Understanding. The data understanding quiz assessed knowledge on what happens with the data that the participants' app collects during the study, i.e., who has access to it, where it is processed, and where it is stored. The participants had to check for each of the ten statements whether they were right or wrong. For each correctly rated statement, one gained 1 point; otherwise,

Table 4. Participants answered two groups of quiz-like items to assess their knowledge of (1) what happens with their data, and (2) what data is logged. While the latter did not show differences between the conditions, we noticed significantly higher knowledge of what happens with the data among participants that were using either the transparency or control features.

	Baseline	*Transparency*	*Control*	*Both*
Data Understanding - What happens with my data?				
Pre-Study Questionnaire [0;10]	6.55	7.91	6.54	8.08
Post-Study Questionnaire [0;10]	6.63	7.13	7.21	8.44
Difference Before/After [-10;10]	+0.296	−0.818	+0.559	+0.333
Logging Knowledge - What is logged?				
Pre-Study Questionnaire [0;12]	5.72	6.27	6.05	5.83
Post-Study Questionnaire [0;12]	6.26	6.61	6.5	6.56
Difference Before/After [-12;12]	+0.704	+0.182	+0.529	+0.788

0. Thus, each participant reached a score between 0 and 10. We performed a Shapiro–Wilk test which showed that the data is not a normal distribution; thus, we used the nonparametric Aligned Rank Transformation (ART) ANOVA [50].

We first assessed the pre-study questionnaire. Here, users of *Both* and *Transparency Features* scored on average higher than those of *Baseline* and *Control Features* (see Table 4). The ART ANOVA shows a statistical significance for the main factor Transparency. However, there was no statistically significant difference for the main factor Control, nor was there an interaction effect, see Table 5.

After using the app for seven days (post-study questionnaire), users of the *Transparency Features* had a lower mean score than before (-0.818), while the other conditions on average increased (*Baseline*: +0.296, *Control Features*: +0.559, *Both*: +0.333), see Table 4. The ART ANOVA showed again a statistically significant difference for the main factor Transparency; however, not for Control or an interaction effect, see Table 5.

Important for app developers is if the app – the transparency and control features – impacts the user understanding. Therefore, we run a third ART ANOVA on the change in score (differences *start* − *end*). Here, the ANOVA could not reveal any difference; see Table 5.

6.2.2 Logging Knowledge. Similarly, as with the data processing quiz, we assessed how much the participants knew about what the app was logging in the data logging quiz. Here we let them rate 12 items about the logging of data types (e.g., is GPS location logged raw? Are phone calls recorded?). The scores were, in general, lower than for the data understanding items, especially since the scale had a higher range (0 to 12). We could neither find any significant differences between the conditions in both pre-study- and post-study questionnaires nor significant effects between the factors, see Table 5.

Comparing the scores before and after the seven-day study we found a slight improvement over all conditions, again with *Transparency Features* users showing the lowest (+0.182). *Both* shows the highest increase (+0.788), closely followed by the *Baseline* (+0.704). *Control Features* users increased their logging knowledge by, on average, 0.529 points. We could not find any statistically significant effects using an ART ANOVA [50]; see Table 5.

Table 5. The two-way F-statistics.

	Analysis of variance (ANOVA) using ART [50]							
			Transparency		Control		T × C	
	dfn	*dfd*	*F*	*p*	*F*	*p*	*F*	*p*
Data Understanding - Pre	1	120	18.606	<.001	0.031	.861	0.699	.792
Data Understanding - Post	1	114	12.818	<.001	2.693	.104	0.153	.697
Data Understanding - Differences	1	112	3.135	.079	1.707	.194	0.506	.478
Logging Knowledge - Pre	1	120	0.211	.647	0.213	.645	0.822	.366
Logging Knowledge - Post	1	114	0.096	.758	0.131	.718	0.412	.522
Logging Knowledge - Differences	1	112	0.101	.751	0.341	.560	1.733	.191
I learned new things about myself	1	111	0.137	.712	0.030	.863	1.543	.217
I learned new things about my behavior	1	111	0.001	.978	0.227	.634	3.590	.061
I have changed my smartphone usage	1	111	0.475	.492	0.957	.330	0.169	.682
I have changed my behavior	1	111	0.677	.412	0.879	.351	0.025	.874
Perceived control	1	117	2.598	.11	9.358	.003	2.679	.104
App permission concern	1	117	0.004	.949	3.709	.057	1.14	.288
Perceived surveillance	1	117	0.374	.542	1.928	.168	2.85	.094
Perceived intrusion	1	117	0.824	.366	3.41	.067	9.441	.003
Permission Acceptance	1	117	1.114	.293	3.18	.077	1.89	.172
UEQ Score	1	111	0.399	.529	0.521	.472	0.748	.389

6.3 Behaviour Change and Self-Reflection

The items on behavior change and self-reflection correspond to RQ3. We included four items inspired by the Technology Supported Reflection Inventory (TSRI) in the post-study questionnaire [3] to assess self-reflection and learning effects (*learnings about myself* and *learnings about my behavior*) and behavior change (*change in smartphone usage* and *change of behavior*) induced by our privacy dashboard. Slightly more users of the conditions *Transparency Features* and *Control Features* agreed that they had learned something about themselves and their behavior; however, there are no statistically significant differences, see Table 5. Moreover, no differences are visible between changes in smartphone behavior and real-world behavior change, see Figure 6 and Table 5. Furthermore, the free-text responses did not reveal differences regarding transparency and control features. Although users mentioned gaining insights during the usage (e.g., that they are using their smartphone too much, high social media usage, or unlock it unnecessarily often) and reported behavior changes (more conscious phone usage, reduction of screen time, and unlocks), we found no relation to the presence of transparency and control features. The sole presence of the logging app had more effect than the privacy dashboard.

Bayes Factor estimates returned values for BF_{0+} below 1/3, which according to the classification scheme by Jeffreys [33], provides moderate evidence for H_0. This means that the data is more than three times more likely to occur for a system where the factors Transparency and Control have no effect than for one where the privacy dashboard triggers learning effects and behavior change. For all four measurements, except for *learnings about my behavior* BF_{0+} is below 0.1. This donates strong evidence that H_0 (no influence) is 10 times more likely (*learnings about myself*: $BF_{0+} = .089$, *learnings about my behavior*: $BF_{0+} = .196$, *change of smartphone usage*: $BF_{0+} = .085$, *change of behavior*: $BF_{0+} = .085$).

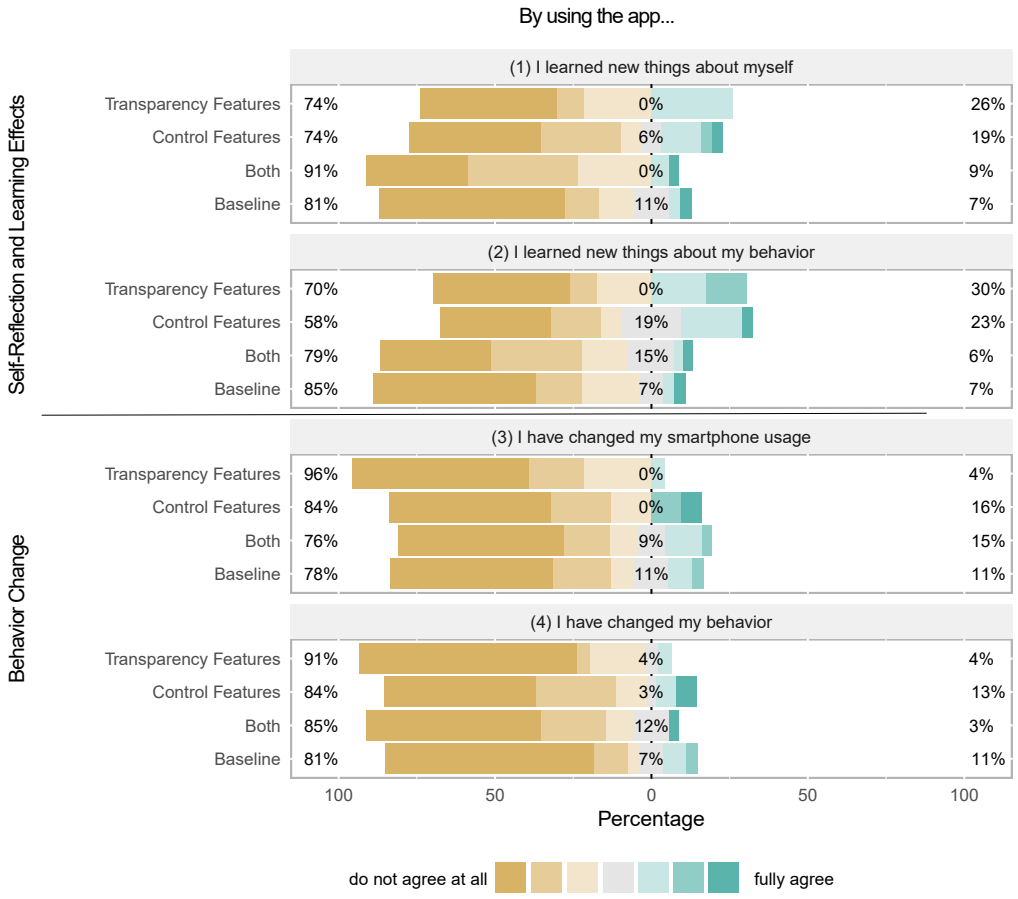


Fig. 6. Users of the conditions *Transparency Features* and *Control Features* reported slightly higher learnings about themselves and their behavior. However, none of the effects was significant, and no effect could be observed regarding self-reported behavior changes induced by our privacy dashboard.

6.4 Privacy Concerns and User Experience

According to RQ4, we evaluated privacy concerns about the usage of our app at the end of the seven days of app usage. Therefore we used the item collection by Degirmenci [6], which is tailored to the use of mobile devices. It is structured into five subscales. We tested the effects of the factors transparency and control via two-way ANOVA tests for normally distributed data, the nonparametric ART ANOVA otherwise. The results are plotted in Figure 7.

The factor control showed a significant positive effect on the ratings about perceived control, see Table 5. Users of the condition *Control Features* reported the highest scores for perceived control ($M_{Control}$ = 21.0, scale range: [5;35]), followed by the condition *Both* (M_{Both} = 20.5) and *Baseline* ($M_{Baseline}$ = 19.1). Users of the condition *Transparency Features* scored lowest ($M_{Transparency}$ = 14.6). In the ratings for **app permission concern**, slightly lower scores were reported for the conditions *Control Features* and *Both*; however, the factor control does not reach the significance level of

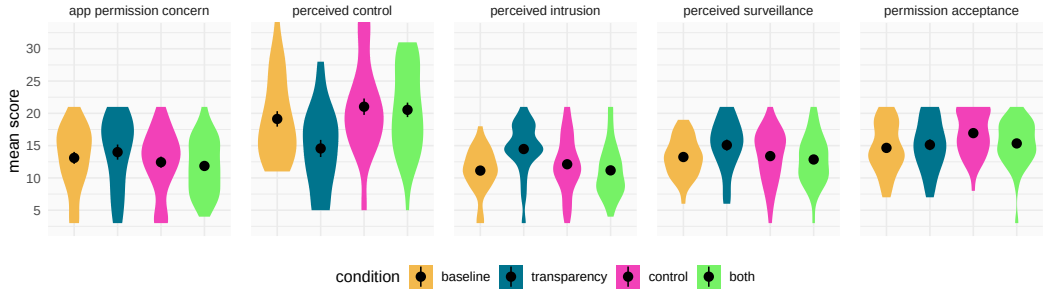


Fig. 7. Scores of the items on prior privacy experience [6]. Users that were offered transparency features were in general most concerned, even more than those who did not have the privacy dashboard at all. Control features could to some extent mitigate those concerns, and the both conditions scored equally and for some items better than the baseline condition without any privacy dashboard features.

$p < .05$. For the **perceived surveillance** scale, the condition *Transparency Features* reports slightly higher values; however, again not significant. **Perceived intrusion** also shows the highest scores for users of the condition *Transparency Features*, followed by *Control Features*, which scored above average. Although the individual factors do not reach significance, we found significant interaction effects. The **permission acceptance** is highest in the condition *Control Features*, with the other conditions ranging equally. None of the factors was statistically significant.

UEQ scores for Attractiveness, Perspicuity and Stimulation were rather bad, according to the benchmark intervals of Schrepp et al. [40]. The condition *Control Features* scored highest ($M_{Control} = 0.555$), followed by *Both* ($M_{Both} = 0.334$) and *Transparency Features* ($M_{Transparency} = 0.311$). The baseline condition without any transparency or control features received the lowest scores ($M_{Baseline} = 0.288$). However, we could not reveal that the factors are statistically significantly different, see Table 5.

7 DISCUSSION

RQ1: How do transparency and control in a privacy dashboard affect the number of users adopting and dropping out of a passive mobile sensing app? Our results show that transparency and control have different effects. While transparency led to fewer users actually installing the mobile sensing app, control, in contrast, increased the number of users. The dropout, later on, seems not to be affected.

The observed app usage rates across the study phases are common for mobile sensing studies. The literature agrees that once a potential participant has agreed to participate, it is unlikely that they quit their participation early [15, 25]. The low conversion rate of 10% is also common. For example, Kreuter et al. [22] report a revocation of 88% in a comparable mobile sensing study. The *Control Features* having the highest participation rate and best concern and trust rates in opposite to *Transparency Features* aligns with the literature. We can confirm the finding of Schnorf et al. [39] that control does not lead to less trust. Also, we support the recent work by Farke et al. [10]. They studied the "Google Privacy Dashboard" and emphasized the importance of control. Transparency features alone rather deter the users. They become aware of what is logged, which - without control features - might make them feel like their data is not in their hands anymore. From a trust and concern perspective, this is even worse than not providing any transparency. We argue that in the *Baseline* condition, the users instead experience a sense of security due to unknowingness, which seems to be better than knowing what happens in detail but being unable to control it. However,

it is interesting that the biggest difference between the groups, with significant effects for both factors control and transparency, did not occur while using the app with the users' data but during the onboarding phase. This means that the main difference was not made by whether the users could view, delete and pause their data, but by the advertisement of the privacy-enhancing features in the onboarding process. This aligns with the usage statistics of the control features: The sole presence of control features made users feel better protected, although they only rarely made use of them. Therefore, we conclude that the screenshots during onboarding presenting the transparency features, including demo data, made the difference. We argue that they have better conveyed what is logged than the sole privacy declaration.

RQ2: How do transparency and control in a privacy dashboard affect the awareness of and knowledge about the data logging? We found that transparency is the influencing factor: Users with this factor could better recall the information. In contrast, users without it caught up during the one-week app usage. While the knowledge increased for both factors, it increased the least for transparency. The awareness of and knowledge about what data is logged, however, was not affected by transparency nor control. During the first assessment in the pre-study questionnaire, both the knowledge about what data is logged and what happens with the data had the lowest scores in the condition *Baseline*, i.e., when no privacy-enhancing features were available. The reason might again be the screenshots with demo data, i.e., the control features in the onboarding process, which as a side effect, seem to convey what the app is doing. However, during the one-week usage period of our mobile sensing app, the scores in *Transparency Features* behaved significantly differently. They decreased for the data understanding items, while all other conditions increased, and reported the lowest increase of all conditions for the logging knowledge items. The reason for the low improvement of the logging knowledge scores might be caused by the presentation: The control features screen in the conditions *Control Features* and *Both* provided an overview over all logged datatypes, whereas the main view in condition *Transparency Features* consists of a timeline view. As a result, rarely logged data types (e.g., Bluetooth settings changes) were likely not seen by users who used the dashboard rarely and did not scroll down much. In future systems, we recommend not only providing a strictly chronological order (timeline view) but also a grouped view where at least one entry of each data type is presented prominently. We suspect self-reflection effects regarding the increase of the data understanding scores, which were present in all conditions except *Transparency Features*. For example, since changing logging settings and deleting data requires an active decision, we suspect that this might have made people think more about what the app does.

RQ3: How do transparency and control in a privacy dashboard induce behavior change and self-reflection and thus the logged data of a passive mobile sensing app? After having used the app, we asked the participants about the learning effects and behavioral changes induced by the app. If they at least rather agreed on having learned something or changed their behavior, we further asked them to describe the effect. Interestingly equal self-insights and behavioral changes were mentioned across the study conditions. We conclude that not the presentation of the data led to those effects but the sheer presence of the mobile sensing app. Thus, it does not make a difference whether a privacy dashboard is included or not. Our Bayes factor analysis further supports that an effect by the privacy dashboard itself is very unlikely. The control features implemented in the dashboard, i.e., pausing the logging and deleting logged data, were used only rarely. Besides a few users who used those features regularly, the vast majority did not make use of pause or delete features at all. Concluding on **RQ3**, we did not find any indicators that the log data is influenced by a privacy dashboard incorporating transparency and control significantly. However, we are aware that self-reported measurements, as we used them to assess self-reflection and behavior change, do

not provide full evidence. We encourage future research to conduct studies that measure actual behavior in the wild.

RQ4: How do transparency and control in a privacy dashboard affect a passive mobile sensing system user's privacy concerns and trust? We found that the factor control showed significantly higher scores in perceived control which is not surprising and confirms the effectiveness of the control features, albeit not used frequently. The app permission concern shows a similar (inverse) trend; users who had the option to control the logging might, thus, be more willing to grant the app permissions. The results of the permission acceptance items behave accordingly, supporting this conclusion. Furthermore, we found high scores in perceived surveillance and intrusion in the condition *Transparency Features*, but not in *Both*. This aligns with our findings from the app usage and dropout rates: *Transparency Features* should always be accompanied by the ability to control the logging.

7.1 Future Work

In the future, we recommend that more focused investigations would need to be conducted to obtain detailed insights on behavior change induced by privacy dashboards. We did the first step by investigating RQ3. However, measuring behavior change in in-the-wild studies is difficult and self-report scales as we used it can be biased [7].

Our privacy dashboard presented only raw data to the users. We deliberately omitted any aggregated or inferred data to keep our study setting generalizable and neutral. However, nearly every real-world application does some processing to use the data. Following the "consent as a process" approach [13] and guidelines for privacy in big data systems [24], the data processing steps following the raw data collection should be incorporated into privacy dashboards. Therefore, dedicated research becomes necessary that studies the effects of aggregated and derived data in privacy dashboards. Current research is contradictory. Here, Herder et al. [14] report increased trust and decreased perceived risks by derived data, while Rudnicka et al. [34] hypothesize that transparency about the derived data might make people less fearful.

Privacy perception is a very individual construct. The studies of Schnorf et al. [39] distinguished different groups of users by their privacy-related predisposition. Also, Awad et al. [2] reported that the relation between transparency and the resulting effect depends on the user: People who desire transparency are less willing to be profiled. Thus, for them, trust decreases, and concerns increase with the provision of transparency than for people who have a weaker desire for privacy. Future privacy dashboards could make use of this and adapt to their user. Therefore, researchers could extend our RQ4 and investigate different kinds of privacy dashboards depending on the individual user's predisposition towards privacy perceptions.

8 CONCLUSION

In this work, we investigated how (a) *Transparency Features* and (b) *Control Features* of privacy dashboards affect app usage, users, and the collected data in mobile sensing applications. Our in-the-wild study with independent groups confirmed the opinion of current literature that transparency alone can be counterproductive. Privacy dashboards should also incorporate control features to allow users to control what happens with their data. Our quantitative analyses on usage rates and privacy perceptions underline the importance of control features in the mobile sensing context. We found a significantly higher app installation rate of 88.4% compared to 47.4% for *Transparency Features*. Despite the ability to delete data and pause the logging anytime, users made only rare use of it. Thus, developers of mobile sensing apps in the industry and researchers deploying mobile sensing technology for data collection do not have to fear significant gaps in the data.

REFERENCES

[1] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security Privacy* 3, 1 (2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[2] Naveen Farag Awad and M. S. Krishnan. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly* 30, 1 (2006), 13–28. https://doi.org/10.2307/25148715

[3] Marit Bentvelzen, Jasmin Niess, Mikołaj P Woźniak, and Paweł W Woźniak. 2021. The Development and Validation of the Technology-Supported Reflection Inventory. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–8. https://doi.org/10.1145/3411764.3445673

[4] Jan Hendrik Betzing, Matthias Tietz, Jan vom Brocke, and Jörg Becker. 2020. The impact of transparency on mobile privacy decision making. *Electronic Markets* 30, 3 (2020), 607–625. https://doi.org/10.1007/s12525-019-00332-3

[5] Christoph Bier, Kay Kühne, and Jürgen Beyerer. 2016. PrivacyInsight: the next generation privacy dashboard. In *Annual Privacy Forum*. Springer, 135–152. https://doi.org/10.1007/978-3-319-44760-5_9

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

[7] Stewart I Donaldson and Elisa J Grant-Vallone. 2002. Understanding self-report bias in organizational behavior research. *Journal of business and Psychology* 17, 2 (2002), 245–260. https://doi.org/10.1023/A:1019637632584

[8] Nick Doty and Mohit Gupta. 2013. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. (2013). https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.385.6907

[9] Anne Elevelt, Peter Lugtig, and Vera Toepoel. 2019. Doing a time use survey on smartphones only: What factors predict nonresponse at different stages of the survey process?. In *Survey Research Methods*, Vol. 13. 195–213. https://doi.org/10.18148/srm/2019.v13i2.7385

[10] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*. 483–500. https://doi.org/10.48550/arXiv.2105.14066

[11] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14. https://doi.org/10.1145/2335356.2335360

[12] Paul Gerber, Melanie Volkamer, and Karen Renaud. 2015. Usability versus Privacy Instead of Usable Privacy: Google's Balancing Act between Usability and Privacy. *SIGCAS Comput. Soc.* 45, 1 (feb 2015), 16–21. https://doi.org/10.1145/2738210.2738214

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

[14] Eelco Herder and Olaf van Maaren. 2020. Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk. In *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization* (Genoa, Italy) *(UMAP '20 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 169–174. https://doi.org/10.1145/3386392.3399557

[15] Annette Jäckle, Jonathan Burton, Mick P Couper, and Carli Lessof. 2019. Participation in a mobile app survey to collect expenditure data as part of a large-scale probability household panel: Coverage and participation rates and biases. In *Survey Research Methods*, Vol. 13. 23–44. https://doi.org/10.18148/srm/2019.v1i1.7297

[16] Milena Janic, Jan Pieter Wijbenga, and Thijs Veugen. 2013. Transparency enhancing tools (TETs): an overview. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 18–25. https://doi.org/10.1109/STAST.2013.11

[17] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2011. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research* 37, 5 (2011), 858–873. https://doi.org/10.1086/656423

[18] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, and Daniel Veit. 2017. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems* 34, 2 (2017), 369–400. https://doi.org/10.1080/07421222.2017.1334467

[19] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6

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

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

[22] Frauke Kreuter, Georg-Christoph Haas, Florian Keusch, Sebastian Bähr, and Mark Trappmann. 2020. Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review* 38, 5 (2020), 533–549. https://doi.org/10.1177/0894439318816389

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

[24] Sandra C Matz, Ruth E Appel, and Michal Kosinski. 2020. Privacy in the age of psychological targeting. *Current opinion in psychology* 31 (2020), 116–121. https://doi.org/10.1016/j.copsyc.2019.08.010

[25] Lemay Michael. 2009. *Understanding the Mechanism of Panel Attrition.* https://www.proquest.com/openview/d71fed70218da25ab000364c88aa5053/

[26] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[27] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13. https://doi.org/10.1145/3313831.3376321

[28] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

[29] Iryna Pentina, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior* 65 (2016), 409–419. https://doi.org/10.1016/j.chb.2016.09.005

[30] Sarah Prange, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In *Human-Computer Interaction – INTERACT 2021*. Springer International Publishing, Cham, 339–360. https://doi.org/10.1007/978-3-030-85610-6_20

[31] Philip Raschke, Axel Küpper, Olha Drozd, and Sabrina Kirrane. 2017. Designing a GDPR-compliant and usable privacy dashboard. In *IFIP international summer school on privacy and identity management*. Springer, 221–236. https://doi.org/10.1007/978-3-319-92925-5_14

[32] Melanie Revilla, Mick Couper, and Carlos Ochoa. 2019. Willingness of Online Panelists to Perform Additional Tasks. *methods, data, analyses* 13, 2 (2019), 29. https://doi.org/10.12758/mda.2018.01

[33] Christian P Robert, Nicolas Chopin, and Judith Rousseau. 2009. Harold Jeffreys's theory of probability revisited. *Statist. Sci.* 24, 2 (2009), 141–172. https://doi.org/10.1214/09-STS284

[34] Anna Małgorzata Rudnicka. 2020. *Disclosure of personal data in citizen science settings.* Ph. D. Dissertation. UCL (University College London). https://discovery.ucl.ac.uk/id/eprint/10099010/

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

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

[37] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 1–17. https://doi.org/10.5555/3235866.3235868

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

[39] Sebastian Schnorf, Martin Ortlieb, and Nikhil Sharma. 2014. Trust, transparency & control in inferred user interest models. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. 2449–2454. https://doi.org/10.1145/2559206.2581141

[40] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2014. Applying the user experience questionnaire (UEQ) in different evaluation scenarios. In *International Conference of Design, User Experience, and Usability*. Springer, 383–392. https://doi.org/10.1007/978-3-319-07668-3_37

[41] Johanneke Siljee. 2015. Privacy Transparency Patterns. In *Proceedings of the 20th European Conference on Pattern Languages of Programs* (Kaufbeuren, Germany) *(EuroPLoP '15)*. Association for Computing Machinery, New York, NY, USA, Article 52, 11 pages. https://doi.org/10.1145/2855321.2855374

[42] H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4 (2011), 989–1015. http://www.jstor.org/stable/41409970

[43] Emily Stark, Ryan Sleevi, Rijad Muminovic, Devon O'Brien, Eran Messeri, Adrienne Porter Felt, Brendan McMillion, and Parisa Tabriz. 2019. Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate. In *2019 IEEE Symposium on Security and Privacy (SP)*. 211–226. https://doi.org/10.1109/SP.2019.00027

[44] Kathy A Stewart and Albert H Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information systems research* 13, 1 (2002), 36–49. https://doi.org/10.1287/isre.13.1.36.97

[45] Eric Struse, Julian Seifert, Sebastian Üllenbeck, Enrico Rukzio, and Christopher Wolf. 2012. PermissionWatcher: Creating user awareness of application permissions in mobile systems. In *International Joint Conference on Ambient Intelligence*. Springer, 65–80. https://doi.org/10.1007/978-3-642-34898-3_5

[46] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research* 22, 2 (2011), 254–268. https://doi.org/10.1287/isre.1090.0260

[47] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. 2017. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 5208–5220. https://doi.org/10.1145/3025453.3025556

[48] Daniel Votipka, Seth M Rabin, Kristopher Micinski, Thomas Gilray, Michelle L Mazurek, and Jeffrey S Foster. 2018. User comfort with android background resource accesses in different contexts. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 235–250. https://doi.org/10.5555/3291228.3291247

[49] Sunil Wattal, Rahul Telang, Tridas Mukhopadhyay, and Peter Boatwright. 2012. What's in a "name"? Impact of use of customer information in e-mail advertisements. *Information Systems Research* 23, 3-part-1 (2012), 679–697. https://doi.org/10.1287/isre.1110.0384

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

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

[52] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John Carroll. 2012. Measuring mobile users' concerns for information privacy. (2012), 2278–2293. https://doi.org/10.1.1.668.3794

[53] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research* 23, 4 (2012), 1342–1363. https://doi.org/10.1287/isre.1120.0416

[54] J Christopher Zimmer, Riza Arsal, Mohammad Al-Marzouq, Dewayne Moore, and Varun Grover. 2010. Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems* 48, 2 (2010), 395–406. https://doi.org/10.1016/j.dss.2009.10.003

[55] Christian Zimmermann, Rafael Accorsi, and Günter Müller. 2014. Privacy dashboards: reconciling data-driven business models and privacy. In *2014 Ninth International Conference on Availability, Reliability and Security*. IEEE, 152–157. https://doi.org/10.1109/ARES.2014.27

A QUESTIONNAIRE ITEMS

In the following we list the instruments that we used in the pre-study-survey and post-study-survey. They were used in german language and were translated into English for these tables.

Table 6. Items of the instrument assessing *prior privacy experience*

Instrument	Source	Question/Statement	Scale	Items
prior privacy experience	adaptation of the collection of Degirmenci et al. [6], which consists of adaptions of the items about prior privacy experience from Xu, Gupta et al. [52], computer anxiety by Stewart and Segars [44], perceived control by Xu, Teo et al. [53], and app permission concerns by Smith et al. [42]	Please rate the level of control you have over your personal information on a scale of 1-7, where (1) means no control and (7) means full control.	7-point Likert (no control - full control)	How much control do you think you have over your personal information shared with the PhoneStudy app?
				How much control do you think you have over the amount of personal data collected by the PhoneStudy app?
				Overall, how much control do you think you have over your personal information that you have shared with the PhoneStudy app?
				How much control do you think you have over who can have access to your personal information?
				How much control do you think you have over how your personal information isused by the PhoneStudy app?
		Please rate your concerns about your personal information on a scale of 1-7, where (1) means "strongly disagree" and (7) means "strongly agree". When I installed the PhoneStudy app on my mobile device...	7-point Likert (disagree at all - totally agree about)	it bothered me when I was asked to accept the app permissions
				I thought twice before accepting the app permissions
				bothered me accepting the app permissions
		Please rate how much you feel monitored by the PhoneStudy app on a scale of 1-7, where (1) means "strongly disagree" and (7) "strongly agree". Since I accepted the PhoneStudy app permissions…	7-point Likert (disagree at all - totally agree about)	I believe that my smartphone is at least temporarily monitored by the PhoneStudy app
				I am concerned that the PhoneStudy app is collecting too much information about me
				I am concerned that the PhoneStudy app is monitoring my activity on my smartphone
		Please rate how much PhoneStudy interferes with your privacy on a scale of 1-7, where (1) means "strongly disagree" and (7) "strongly agree". Due to the installation of the PhoneStudy app…	7-point Likert (disagree at all - totally agree about)	I have the feeling that other people know more about me than I would like
				information about me that I consider private is more readily available to others than I would like
				Is there information outside of my smartphone that can be used to invade my privacy
		For each of the following app permission requests, indicate the degree to which you have accepted those permissions.	7-point Likert (not at all agree - totally agree)	Confirm privacy policy
				Access usage statistics
				Location (for activity detection)

Table 7. Items of the data-logging- and data-understanding quiz

Instrument	Source	Question/Statement	Scale	Items
data logging quiz	self-constructed	Are the following statements about the PhoneStudy app correct? The PhoneStudy app captures...	no, yes, I don't know	my exact location (GPS coordinates)
				my activity, e.g., when I ride a bike or run
				which apps I use
				how many messages I send in messenger apps (e.g., WhatsApp).
				when I unlock my phone
				when to turn airplane mode on or off
				when I created a new contact in the address book
				how many photos i take
				Sensor data of the smartphone (e.g., acceleration and movement)
				whether I have headphones connected to the smartphone
				the name of connected Bluetooth devices (e.g., Apple AirPods)
				The device type of connected Bluetooth devices (e.g., headphones)
data understanding quiz	self-constructed	Please indicate whether each of the following statements is true or false. These dates...	no, yes, I don't know	don't leave my smartphone
				are collected on a server
				are accessible to everyone on the internet
				are accessible to PhoneStudy scientists
				are accessible to all LMU scientists
				are anonymous, ie cannot be assigned to my identity (name, e-mail address, ...).
				are only recorded while I have the PhoneStudy app open
				I can delete individual data from the last 24 hours in the app
				I can delete individual data in the app at any time
				I can view all recorded data in the app at any time

Table 8. Items used to assess the usage of control features. Detailed questions on logging pause- or delete actions (marked with *) were only asked if the corresponding question on whether the action happened at all was answered with *yes*.

Instrument	Source	Question/Statement	Scale	Items
usage of control features	self-constructed	Have you used the option to delete data in the app? Approximately how many entries have you deleted?*	yes, no freetext	
		What types of data have you deleted, roughly how often? It's all about comparing amounts between data types, not absolute numbers*	freetext	app usage activities settings
		Why did you delete data?*	freetext	
		In what situations have you deleted data?*	freetext	
		Have you used the option to temporarily pause data recording? How many times do you think you paused the data recording?*	yes, no freetext	
		Which types of data do you estimate how often have you paused? It's all about comparing amounts between data types, not absolute numbers*	freetext	app usage activities settings
		Why did you pause the data recording?* In which situations did you pause the data recording?*	freetext freetext	

Table 9. Items of the instrument used to assess behavior change induced by our privacy dashboard.

Instrument	Source	Question/Statement	Scale	Items
behavior change	adaptation of the Technology Supported Reflection Inventory [3]	How much do you agree with the following statements? By using the PhoneStudy app...	7-point Likert scale (don't agree at all - fully agree)	I learned new things about myself I learned new things about my behavior I have changed my smartphone usage I changed my behavior
	self-constructed	If you learned something about yourself or your behavior by using the PhoneStudy app, what is it?	freetext	
		If you have changed your behavior or smartphone usage by using the PhoneStudy app, what has changed and why?		

Table 10. Items used to assess participants' awareness of the passive data logging happening in the background.

Instrument	Source	Question/Statement	Scale	Items
logging awareness	self-constructed	To what extent do you agree with the following statements?	7-point Likert scale (I do not agree - totally agree)	While using my smartphone, I was aware that the PhoneStudy app was recording data in the background
				In everyday life I was aware that the PhoneStudy app was recording data in the background
				The awareness that the PhoneStudy app was recording data in the background has changed my behavior on the smartphone
				The awareness that the PhoneStudy app was recording data in the background changed my behavior in everyday life
		If your behavior has changed, how?	freetext	

Table 11. Items to assess the usability of our Android app.

Instrument	Source	Question/Statement	Scale	Items
usability	UEQ subscales on attractivity, perspicuity and stimulation [40]	Please give your assessment of the PhoneStudy app. Make decisions as spontaneously as possible. It's important that you don't think too much about the terms so that your immediate judgment comes through. Please always tick one answer, even if you are unsure about a pair of terms or think that they do not fit the product very well. There is no "right" or "wrong" answer. Your personal opinion counts!	7-point Likert scale	unpleasant - pleasing
				incomprehensible - understandable
				easy to learn - hard to learn
				precious - inferior
				boring - exciting
				not interesting - interesting
				good - bad
				complicated - easy
				repulsive - attractive
				unpleasant - enjoyable
				activating - soporific
				clear - confusing
				attractive - unattractive
				friendly - unsympathetic
	self-constructed	Do you have any other feedback about the PhoneStudy app or this study?	freetext	