From Design Requirements to Effective Privacy Notifications: Empowering Users of Online Services to Make Informed Decisions

Patrick Murmann & Farzaneh Karegar


To link to this article: https://doi.org/10.1080/10447318.2021.1913859
From Design Requirements to Effective Privacy Notifications: Empowering Users of Online Services to Make Informed Decisions

Patrick Murmann and Farzaneh Karegar

Department of Mathematics and Computer Science, Karlstad University, Karlstad, Sweden

ABSTRACT

Privacy notifications issued by Transparency-Enhancing Tools (TETs) constitute a conceptual means of informing users of online data services about how their personal data are processed. We elicit a set of design requirements that reflect the particularities of privacy notifications received on mobile phones. Pursuing the principles of human-centered design, we evaluate the efficacy of a prototypical implementation for the context of personal health tracking in an iterative lab study. Our findings show that privacy notifications have the potential to facilitate usable transparency and informed decision-making in terms of improving privacy in the designated usage context. The feedback obtained during the evaluation of the prototype lends itself to a refined set of design requirements. We discuss these requirements as building blocks that can help designers create usable artifacts that accommodate the needs of users of mobile health services.

1. Introduction

The EU General Data Protection Regulation (European Parliament and the Council of the European Union, 2016) (GDPR) stipulates data subject rights as regards obtaining transparency about how one’s personal data will be and have been processed (Art. 12–14). Moreover, the Regulation stipulates the legal right to access, rectify, erase, object to, or restrict the processing of one’s personal data (Art. 15 et seq.). Likewise, data subjects have the right to withdraw their consent at any time, and to move their data to another service. Despite these legal requirements, few usable tools exist to aid data subjects in making informed decisions about when and how to exercise their rights (Murmann & Fischer-Hübner, 2017).

Transparency-Enhancing Tools (TETs) are technological artifacts that facilitate transparency, and can therefore help improve a data subject’s privacy. TETs that depend on the proactive engagement of users have e.g. explored the visualization of disclosed personal data (Karegar et al., 2016; Kolter et al., 2010). Conversely, TETs that rely on delivering notifications to facilitate awareness are often employed in the context of location-based services (see e.g. Hsieh et al. 2007; Sadeh et al. 2009). However, formal specifications for designers who seek to create usable TETs are lacking. While we consider obtaining transparency about the processing of one’s personal to be a valuable faculty in terms of satisfying legal compliance, we furthermore consider it to be a prerequisite for informed decision-making. Data subjects can intervene in the processing of their personal data by exercising their right of intervenability (Hansen, 2012; Meis & Heisel, 2016). In this context, obtaining clarity and insight about the status quo is a necessary condition for exerting influence on the process. Hence, transparency and intervenability go conceptually hand in hand. TETs will have to facilitate both principles to actually empower data subjects in terms of helping them improve their privacy.

In previous work (Murmann, 2018), we have proposed privacy notifications as a conceptual means to facilitate customized transparency of how personal data have been and will be processed. Privacy notification draw on various interaction paradigms established for the ecosystem of mobile phones, which in turn reflect behavioral patterns exhibited by the users of these devices. A recurring pattern is the habit of consuming relevant information in the form of contextualized messages rather than querying respective sources on one’s own (Murmann, 2019). Reflecting individual usage behavior and preferences for transparency, privacy notification pose an interesting candidate for leveraging the merits of a device that is as omnipresent as a mobile phone. Semi-permanent companions to many users, contemporary smart phones constitute epicenters of everyday communication. Mobile phones increasingly serve as monitoring devices and control hubs in domains such as home automation (Asadullah & Raza, 2016) and personal informatics (Rooksby et al., 2014).

Due to the lack of design requirements in the literature, the objective of this paper is to collect and validate a set of formal requirements that enable the design of TETs that operate on the basis of privacy notifications and that demonstrably reflect the needs of users of their users. We choose mobile health (mhealth) as our usage context because of its increasing prevalence and relatedness to the ecosystem of...
mobile phones. Wearable mhealth devices permeate many social strata Statista19shipment,Statista19connected,Statista19Europe, which will account for projected penetration rates of 5–10% for many European countries in 2022 (Tractica, 2020a, 2020b, 2020c, 2020d). A sub field of mhealth, personal health tracking and self-quantification have grown to be omnipresent, socio-cultural phenomena. Affordable wearables allow for monitoring and annotating a wealth of personal data, such as one’s physiology, sensitivities, and geographic location (ENISA, 2011; Wolf, 2009). According to the GDPR, many of these types of data qualify as “data concerning health” (Art. 4 (15)), which warrants special care in terms of processing (Art. 9). Hence, the temporal, spatial, and situational linkage of such data and any inferences drawn from their processing can have a considerable impact on the privacy of the data subjects concerned (Lowens et al., 2017).

To achieve our objective, we elicit the requirements from the literature and present the prototypical design of a TET for the context of personal health tracking. We then conduct an iterative qualitative lab study to evaluate the prototype as well as the requirements it embodies. Whereas the elicitation of the requirements draws on the existing body of knowledge, the design and evaluation implements characteristics of human-centered and participatory design (International Organization for Standardization, 2010) in that we rely on the feedback of representatives of the target audience. Pursuing an iterative design process, we integrate the feedback into the design of the prototype until we reach a demonstrable level of maturity. In this manner, we seek to facilitate progressive development and improvement of the prototype, as well as the requirements used to implement it. Finally, we present a refined set of design requirements that reflect the underlying objective.

As a stepping stone toward addressing the aforementioned objective, we seek to answer the following research question:

How can privacy notifications be designed such that they effectively inform users about their intervenability rights, and help them make informed follow-up decisions to improve their privacy?

We investigate how an information system can visualize intelligible information by means of privacy notifications such that they enable recipients to make informed decisions. The investigation is reflected by means of design requirements, the manifestation of these requirements in the prototype, and their evaluation in the course of the user study. The study targeted active, former, and prospective users of mhealth services ($n = 16$), and elicited qualitative feedback to evaluate the prototype in the course of three iterations.

We contribute to the body of knowledge by providing a proof of concept in the form of a prototypical implementation of a TET that facilitates usable transparency by harnessing privacy notifications. The evaluation of the prototype yields a set of design requirements that not only reflect the theory derived from the literature, but that have matured due to critical reflection by representatives of the target audience.

The rest of this paper is structured as follows: Section 2 provides an overview of the literature that is related to various dimensions of privacy notifications. Section 3 describes the methodology we employed to address our research question, including the elicitation of the requirements and the design and implementation of the user study. Section 4 reports the results we obtained from the user study, subdivided into three iterations of implementing and evaluating the prototype. Section 5 presents a comprehensive list of the revised set of design requirements. We also discuss each requirement against the backdrop of principles established in the literature. Section 6 discusses the results with respect to our research objective, and Section 7 concludes the paper.

2. Background and related work

We commence this section by discussing conceptual facets related to privacy notifications. We then concretize these notions in terms of presenting privacy-improving information and helping users intervene in the processing of their personal data, which mirrors the phases Presentation and Intervention of the interaction model presented in Section 3.1. We consider work on criteria related to privacy notices as a means to help users improve their privacy (Section 2.1). Furthermore, we consider privacy nudges (Section 2.2), a concept aiming to leverage what and how information is displayed to nudge users toward improving their privacy. We conclude by touching on studies that make recommendations of how to mitigate real-world issues discovered in the context of intervenability (Section 2.3).

2.1. Guidelines for privacy notifications

In the literature, “privacy notice” constitutes an umbrella term pertaining to information related to the transparency of the processing of personal data. The purpose of privacy notices is to raise awareness and promote informed decision-making based on the information thus conveyed. Ultimately, privacy notices aim to protect the privacy of a data subject. To motivate the design requirements for our prototypical implementation (Section 5), we touch on sources related to design principles, guidelines and concrete requirements pertaining to both ex ante and ex post transparency. The groups of authors referenced here either draw on normative and systematic elicitation of their findings (Bravo-Lillo et al. (2011), Schaub et al. (2017), Murmann and Fischer-Hübner (2017), Murmann (2019), and Data Protection Working Party (2016)), or on user studies that elicit or evaluate respective outcomes (Thomas et al. (2014), Cruzes and Jaatun (2015), Bravo-Lillo et al. (2011), and Schaub et al. (2017) present classification systems structured as legal and human-centered requirements, an analysis of the design space, and a discussion of the factors related to user interaction. Many facets of their respective taxonomies have carried over to privacy notifications, especially to the presentational aspects thereof. This is reflected in the requirements in Section 5.2. However, like the majority of the work published on privacy notices, these authors discuss transparency strictly through the lens of ex ante transparency (Murmann & Fischer-Hübner, 2017). Ex ante transparency pertains to how personal data will be processed in the future. Ex post transparency, i. e.
information on how personal data have been processed, is not considered. In terms of implications that arise for the design of TETs, the interaction phases associated with ex ante transparency are synchronous in that information display and decision-making are tightly coupled. For example, signing up for a data service or installing an app in response to obtaining clarity about the processing of personal data constitute self-contained, transactional contexts. Transparency obtained in the course of the transaction may have an immediate effect on the decision-making process. Conversely, ex post transparency typically reflects a decoupled relationship between the original cause that triggered a notification, and the asynchronous information displayed thereupon (Murmann, 2019). Users may not remember whether and why they made individual decisions in the past. They may therefore struggle to relate information presented to them in the present to the corresponding causes in the past. This necessitates contextualizing information and motivates design requirements related to linking past events to decision-making taking place in the present (see Contextual cues in Section 5.2.1).

Patrick and Kenny (2003) derive design guidelines from legal requirements by discussing the notion of click-through notifications to facilitate comprehension, consciousness, control and consent. Conceptually, the phases of comprehension, consciousness and control can be seen as a control loop that models ex post transparency as well as ex ante transparency. Moreover, the concept of push and pull notices proposed by the Article 29 Working Party (Data Protection Working Party, 2016) include just-in-time notices, which facilitate ad hoc privacy information for users of data services at the moment they are relevant for them. Both concepts have motivated privacy notifications as a means of transparency delivered asynchronously in response to an event (Murmann, 2018). Receiving notifications about a particular event is as subjective as the means employed to deliver the notification in question. Hence, both factors, what and how, are reflected in the design requirements of privacy notifications as functions of customization (Section 5.1).

Thomas et al. (2014) address privacy requirements by analyzing qualitative data from empirical studies related to privacy concerns of end users. Their elicitation process is based on analyzing privacy threats and associated harms to inductively derive requirements that arise due to gaps in the current system requirements of an information system. The approach we pursue in this paper is similar in that it builds on an initial set of requirements. However, our approach is deductive in that the qualitative evaluation of these requirements serves the purpose of approving, disapproving or adapting the requirements represented in the underlying implementation rather than eliciting additional requirements.

Cruzes and Jaatun (2015) elicit transparency requirements from stakeholder workshops. Their elicitation process was driven qualitatively by collecting and aggregating feedback via interviews with customers of cloud services and domain experts. Both groups reported about their preferences in terms of adequate information policies for cloud service providers. Cruzes et al. derive from this feedback a list of requirements of how cloud services ought to inform their users about various aspects related to the processing of personal data. Unlike the approach pursued by Cruzes et al., our approach is deductive in that we seek to approve, invalidate, or refine a list of requirements elicited from the literature.

Fischer-Hübner et al. (2015) present a list of principles and HCI requirements related to tools that facilitate transparency and accountability for cloud services against the backdrop of human-centered design. Many of the requirements proposed by these authors carry over to the specific context of mHealth environments. Some of these requirements are reflected in the collection presented in Section 5.

2.2. Contextualized privacy nudges

Designing UIs whose purpose is to facilitate privacy decisions on the part of the ones using it has been put on a level with nudging (Acquisti et al., 2017). By structuring, positioning, and framing information, design choices determine whether and how users are informed, and what experience they undergo while consuming the information conveyed. More importantly, the choice and manifestation of the information are likely to impact the decisions users make based on framing and presentation of the information displayed (Choe et al., 2013).

We consider the final set of design requirements for privacy notifications to be conceptually related to soft paternalistic privacy nudges in that their designated purpose is to guide users toward making choices that will lead to improving their privacy (Acquisti, 2009; Acquisti et al., 2017). The designs thus implemented are paternalistic in that they are based on the legal requirements stipulated by the regulatory framework of the GDPR. However, they acknowledge the freedom of the individual, leaving it up to the user whether, when, and how to leverage respective options.

The approach presented in this paper mirrors the dimensions of digital nudges discussed by Weinmann et al. (2016) and translates it to the context of privacy notifications. Throughout the phases of this process we aim to understand the goals and needs of users in a particular context, elicit the factors they depend on in terms of making decisions, implement respective nudges to address their needs, and evaluate the outcome.

Jackson and Wang (2018) propose personalized privacy notifications as a means to point out discrepancies between the predisposition of users of mobile devices and their actual behavior in terms of privacy. They conducted a user study in the context of mobile apps in which they provide test subjects with customized privacy nudges at the time of making decisions about installing an app. They report about the feedback they received in terms of designing the UI of their notifications. They report e.g. the ambiguity of iconography and the perceived effectiveness of communicating risks that will arise due to installing individual apps. We share the view presented by Jackson and Wang (2018) as to how notifications can be harnessed to facilitate informed decision-making by communicating the consequences of taking actions. However, whereas their work considers decision-making in terms of communicating risks that may arise in the future in response to an action taken in the present,
we go beyond this exclusively forward-looking approach. Our comprehension of privacy notifications contextualizes decisions made in response to past events, and hence primarily draws on ex post transparency.

Also in the context of ex ante transparency in the Android ecosystem, Chen et al. (2015) and Chong et al. (2018) investigate the effect of framing and priming on the decision-making of users who face the choice of installing a mobile app. Their work discusses how the installation process can be augmented by various cues pertaining to the privacy-friendliness of the app in question. The indicators can be provided via positive or negative framing that reflects the relative safety or risk associated with an app (Chen et al., 2015), respectively. Alternatively, such cues can take the form of neutral, factual or self-relevant priming provided in addition to customary information (Chong et al., 2018). We take from these findings that artifacts can support users in making informed decisions related to their privacy, which supports several of our design requirements related to the presentation of facts (Section 5.2).

2.3. Design recommendations to support intervenability

Various groups of authors investigated the conceptual and technical problems that users face when they attempt to intervene in the processing of their personal data. The findings of these user studies include design recommendations proposed to mitigate such issues. However, the context of the studies is related to data deletion (Habib et al., 2020; Ramokapane et al., 2017), opting out from unsolicited advertisements such as marketing e-mails (Habib et al., 2020), or to managing consent for cookies received in response to visiting websites (Utz et al., 2019). The recommendations provided comprise coarse-grained guidelines, such as to improve transparency by means of accessible and intelligible information to enable decision-making (Habib et al., 2020; Ramokapane et al., 2017). To facilitate informed decision-making, Cranor et al. (2020) suggest that the accessibility and usability of individual options to act ought to be complemented by clarifying expected outcomes and consequences. Hence, availability, intelligibility and the transparency of outcomes associated with individual actions are reflected in our design requirements.

Gabriele and Chiasson (2020) recommend not only to raise the awareness among users of how their personal data are processed, but also to encourage them to take control. In this regard, they recommend to convey information such that the actual processing satisfies the legal requirements of informed consent. They recommend occasional reminders as a means to nudge users into reviewing their settings, and, similar to Patrick and Kenny (2003) and the Article 29 Working Party (Data Protection Working Party, 2016), propose just-in-time notifications to contextualize consent. However, what reconciles their proposed means of facilitating transparency with what we consider to be the essence of privacy notifications is to rely on “customized notifications [...] based on the type of activities users engage in” (Gabriele & Chiasson, 2020). With this in mind, we employ privacy notifications specifically to accommodate the actual needs of users.

We build on these authors’ work by providing users of our prototype with options of how to exert influence, and by showing them the consequences of acting and not acting in one way or another.

3. Methodology

The approach described in this section is subdivided into the steps illustrated in Figure 1. The elicitation of requirements (Section 3.1) draws on guidelines from the literature. It serves the purpose of ascertaining a set of requirements that facilitate the design of a prototypical TET. The design of the prototype (Section 3.2) deals with the prototypical implementation of the requirements obtained from the elicitation. The design of the user study (Section 3.3) elaborates on how we designed a user study (Section 3.5) whose designated purpose was to evaluate the prototype and the design requirements on which it is built. Despite the iterative nature of individual phases, the overarching process is ultimately sequential in that it cumulates in a final set of refined design requirements.

3.1. Elicitation of requirements

The requirements engineering process underlying our research pursues the traditional phases of eliciting, analyzing, and validating the requirements for the design of a technological artifact (see e.g. Sommerville, 2005). The final set of the design requirements presented in Section 5 is based on the findings presented in previous work (Murmann, 2019), which proposes guidelines for the design of a TET that operates on the basis of privacy notifications. These guidelines reconcile the findings pertaining to two independent research fields. The first field covers research pertaining to the economics, ergonomics and framework conditions elicited against the backdrop of receiving notifications on mobile phones. The second branch of literature deals with notices presented to users of online data services in the context of improving their privacy and security. Jointly, both fields have led to the proposal of design guidelines that contextualize the notion of receiving privacy notifications on mobile phones. The guidelines thus proposed reflect principles encountered during the four interaction phases conceptualized for privacy.

Figure 1. Phases of eliciting, implementing, evaluating, and refining the design requirements.
notifications (Murmann, 2019): Configuration, Delivery, Presentation, and Intervention (Figure 2). As will be explained in Section 3.3, considering matters pertaining to the delivery of notifications was beyond the scope of this paper.

In this paper, we deduce from these guidelines a set of requirements that reflect the characteristics of a TET in the form of an application running on a mobile phone. The requirements cover functional, technical, and interaction requirements. They are framed such as to avoid ambiguity in terms of the scope and mutual demarcation of individual requirements. They are, however, specified to be open enough not to depend on any particular system architecture or operating system. Likewise, they are independent of any particular mhealth service provider.

The set of design requirements was elicited in multiple iterations. The original set consisted of a continuously numbered list of 65 requirements. The set lacked coherence in that the scope of some requirements was overlapping. We therefore merged multiple ambiguous requirements and removed the ones with negligible expressive power. The second generation consisted of 52 requirements and introduced codes with a theme-based numbering scheme. We thinned out the set by removing several thematic sections, merged the affected items under unified sections, and removed the ones that had become obsolete in the process. This yielded a set of 35 requirements, which served as the basis for the design of our prototype, and which was evaluated in the user study described in Section 3.3.

The first three iterations of requirements are the result of a deductive elicitation, which yielded the basis for the initial prototypical implementation. After conducting the study, we discussed the requirements once more, merging the ones we considered to be overlapping in terms of scope. We did, however, not remove requirements or include new ones due to the evaluation because the results did not sufficiently support respective changes. This resulted in the final set of design requirements presented in Section 5, all of which reflect the findings from the evaluation of the prototype. Transcripts of versions 1–3 and the revised version of the requirements including the ones not validated during the user study can be found on the companion website of this paper (Murmann & Karegar, 2020).

3.2. Designing the prototype

The TET was conceptualized as a mediator between an mhealth or fitness tracking application and the data subject, i.e. the user of the mhealth service. The designated target platform of the tool was the user’s smart phone (Murmann, 2019). As we were interested in rapid prototyping, we decided to rely on a combination of HTML/CSS/JavaScript, using the jQueryMobile framework to implement the prototype in the form of a rich mobile application (see e.g. Abolfazli et al., 2014). The goal was to emulate the behavior and look & feel of a native mobile app as accurately as possible.

The prototype ran in a standard Firefox web browser on a custom-made Android phone. It included a start screen, settings (Figure 4a), a mock-up of the notification center of the device (Figure 5a–c), and a navigable message display (Figure 5d–f). It implemented typical design concepts and interaction paradigms encountered in today’s apps, such as widget switches and swipeable contents. Each of the interaction phases depicted in Figure 2 was functional in terms of being responsive, allowed for navigating back and forth between multiple screens, and provided secondary information upon request. However, the transition between the main phases was not event-driven, which would have been the case for a real-world app operating on the basis of privacy notifications. Instead, each of the interaction phases served as a manual entry point to allow for exploring specific aspects related to our research questions.

As is mentioned by Murmann (2019), investigating privacy notifications through the lens of HCI takes a highly abstract perspective regarding the consistency and timely communication of information related to personal data processing. Given the inherently asynchronous nature of privacy notifications, TETs typically deliver notifications in response to events that were not entirely foreseeable (Murmann, 2019). Although the GDPR provides the legal ground for obtaining such information (Art. 12–14, 15), we presuppose that such data would include all the details and meta data necessary to draw meaningful inferences. Moreover, we do not take a stance as to whether it would be feasible to actually collect the information in question from a data controller, from a particular data processor, or from a trusted third party (Murmann, 2019).

When individual test subjects questioned the underlying technological infrastructure during the user study, we asked them to assume that respective information was available and authentic, and that the prototype issued its notifications based on these data.

3.3. Study design

Before empirically evaluating our design requirements we had to consider our limitations and adapt the study design accordingly. We were unable to conduct a longitudinal study, which could
have given us the opportunity to evaluate some of our design requirements related to the temporal and interruptive aspects of delivering notifications. In addition, it would have been difficult to simulate real-world environments to investigate the delivery of notifications (Figure 2). We therefore chose to focus on investigating how the Presentation of privacy notifications can facilitate Intervenability. To this end, we designed a qualitative lab study that provided us with a controlled environment and in-depth feedback from the test subjects.

Our user study consisted of three phases: (1) Prologue, (2) Notification, and (3) Epilogue, each of which will be addressed in the following subsections. Figure 3 provides an overview of the study design. During each phase the moderator asked the participants questions and encouraged them to think aloud and speak their mind about what they experienced and thought.

### 3.3.1. Prologue

At the beginning of the prologue, we welcomed our participants, gave them an overview of the study, and introduced the main goal of the study: To investigate their perception and opinion about the prototype of a new privacy-enhancing app. The mobile phone running the prototype was provided to the participants for the duration of the study.

The cover story set the scene for the actual study. It served as a means to provide common ground of the prototype they would experience in the study. We asked them to imagine the following fictitious scenario: They are monitoring their health using a fitness bracelet and its dedicated app available for their phone. However, they do not know how their health data are processed by their online mhealth service. Due to the lack of time to investigate the matter, they have decided to try out a new privacy-enhancing app, the prototype at hand, whose purpose is to help them keep track of how their data were processed by their mhealth service. The app does this by sending them privacy notifications and helps them take action to change how their data are processed and to improve their privacy. We informed the participants that the prototype they will be interacting with was in an early stage of development, which is why some of the functions were not fully implemented. However, we made it clear that the goal of the study was to gauge their general impression of its basic concept and functionality.

While narrating the cover story, the moderator asked the participants questions about their actual usage behavior of fitness tracking apps on their phone, and their general expectations of a TET the likes of which we had just described. The questions the moderator asked during the various parts of the study were scripted (transcript provided in Appendix A), but the order in which we asked them varied depending on the statements each participant made while going through and reflecting on the notifications.

The prologue was concluded by simulating the first-time use of the prototype. The participants were confronted with the start screen and asked to review the settings. The start screen featured a convenient button called “Settings” that opened the settings of the prototype. The settings consisted of three exemplary scenarios, each of which was accompanied by two switches (Figure 4a).

The first switch enabled or disabled receiving notifications about the scenario in question, whereas the second switch specified if the notification was supposed to be delivered immediately (“At once”) or delayed (“In the evening”). Per default, the notifications related to all three scenarios were enabled and delivered immediately to respect the principle of privacy by design and by default (GDPR Art. 25). These defaults also reflected recommendations proposed in previous work (Murmann et al., 2019), which suggests that the most privacy-preserving settings should be chosen if the user’s preference is unclear, effectively implementing a “default on/opt out” policy.

The purpose of asking the test subjects to review the settings in the prologue was two-fold. First, we wanted to give our participants insight about what types of notifications they would receive later on. The description participants received as part of the cover story was abstract and required tangible clarification. Second, suitable run-time behavior of a TET depends on appropriate settings, which is why we investigated our participants’ feedback regarding the configuration to evaluate respective design requirements (see Section 5.1 for requirements on configuration). While reading and reflecting on the settings, we asked our participants whether anything was unclear or unexpected. To gauge their interest in each of the scenarios, the test subjects were encouraged to change the settings as they saw fit. However, before leaving the settings, we asked them to undo their changes using a “Reset to defaults” button. We explained to them that this inconvenience was necessary to ensure that all participants experienced the same basic conditions while interacting with the notifications, since they all were expected to go through all three notifications regardless of the choices they made to the settings. To gauge their general habits in terms of changing settings, we also asked them to what extent they usually reviewed and changed the default settings once they installed a new app on their mobile phones.

---

**Figure 3.** Phases of the user study. Shaded boxes denote interaction with privacy notifications.
**Figure 4.** (a) Settings for the three exemplary scenarios (third iteration). (b) Expanded view of the instructions for taking an action (third iteration, Notification 2, option “Move to another service provider”). The highlighted border signifies that these expandable contents appeared upon touch.
3.3.2. Notification

The main part of the user study was designed to evaluate Intervention and Presentation requirements related to providing users with sufficient guidance to make informed follow-up decisions. To this end, we designed three different privacy notifications considering the design requirements of Intervention and Presentation, where applicable. As regards the content of privacy notifications received by users, we stick with the three categories of scenarios introduced and validated in previous work (Murmann, 2018; Murmann et al., 2019), namely (Personal data) Breaches, Consequences, and Tips:

The three categories served as a means of structuring the scenarios covered in the user study, and to enable us to map individual findings to that structure.

Breaches deal with incidences related to accidental mishaps and the unlawful processing of personal data. Their scope corresponds to what is specified in GDPR Art. 4 (12).

Consequences pertain to actual or hypothetical consequences that arise due to the lawful processing of personal data. They differ from Breaches in that respective scenarios are not the result of a misappropriation or inadvertent accident. Consequences are covered by the purposes and measures specified in the privacy policy of the data controller, which users consent to before they start using a service. This is not to say that users will anticipate respective outcomes, which motivates notifications that provide clarity about why their personal data are processed the way they are.

Tips cover any kind of customized advice to help users improve their privacy. Tips are customized in that they reflect previous choices and user preferences.

Our participants received three notifications in the prototypical notification center, one by one. Each notification consisted of two or more interaction phases. Each phase was implemented as dedicated screens that were accessible from their respective parent screen, facilitating access to secondary information via a nested informational structure. The first layer was a replica of the Android notification center (Figure 5a–c). We chose a prototypical notification center as the first line of contact because we aimed at simulating how users encounter notifications in the real world as far as possible. The “incoming” messages were brief summaries of the circumstances at hand, including a graphical and textual measure of the severity of the event. Notifications related to data Breaches had a warning symbol, a red triangle with an exclamation mark and an accompanying text conveying that taking action was advisable (Figure 5b,e). Tapping the items in the notification center opened the second layer, which consisted of a detailed view of the information pertaining to the event (Figure 5d–f). It contained links and expandable components that, when tapped, revealed additional information about the event. We asked all test subjects to open each notification to be able to reflect on the details. However, whether and which secondary information they explored while responding to the moderator’s questions was up to them.

The first notification (Figure 5a), which informed users about them being profiled, was from the Consequence category. The second one was a Breach notification about a potential disclosure of personal data due to an attack from the Internet (Figure 5b). The last one was a Tip and advised users about their right of data portability (Figure 5c), i.e. the possibility to have their data transferred to another service. The participants were supposed to open each of them, read them carefully, and reflect on the content. The order of receiving the three different notifications was assigned deliberately. The Breach notification did not come first because we did not want the test subjects to start with handling a severe case. We wanted to catch the test subjects’ attention by introducing the warning symbol as part of the second notification, and ask for their opinion afterward on how they perceived its absence in the third notification. Consequently, the Breach notification came second. The participants read each of the notifications, thought aloud, and then answered the moderator’s questions. For all three notifications, participants answered what action they would take and why, and what they felt was missing to reach a decision of whether and how to proceed. The moderator also asked specific questions related to each notification.

From top to bottom, the layout of the detailed view (Figure 5d–f) included a and a description of the scenario, a list of applicable actions in order of appropriateness, and additional links to the secondary information (Figure 5). The most appropriate action was presented first and was highlighted in blue color. Each applicable action had a title accompanied by an icon, both of which were followed by a description of the consequences of taking that action and the subsequent steps that were necessary when taken (expanded view shown in Figure 4b). Some of the actions presented to users included fictitious steps that had to be taken on the website of the original mHealth service. They were phrased such that the wording suggested that taking any one of the options required activity on the user’s part.

3.3.3. Epilogue

After interacting with the prototype, participants filled in a questionnaire to provide demographic information including their gender, age group, and professional background. The moderator asked them about their general impression of the prototype, how useful they considered receiving notifications compared to investigating matters on their own, and how the prototype could be improved to better reflect their needs.

At the end of the study, participants were compensated with a lunch coupon for the university canteen.

3.3.4. Scope

The notifications investigated during the study comprise a subset of the scenarios examined in our previous study (Murmann et al., 2019), which in turn covered but a fraction of the possibilities of how personal data can be processed in the context of personal health tracking. However, the goal of the current study was not to aim for exhaustive breadth or depth, but to enable us to relate the test subjects’ decisions and statements to the category the scenario was linked to (Breach, Consequence, Tip). Outwardly, the categorization of individual scenarios is apparent only in the form of a two-fold distinction of Breaches on the one hand, and Consequences and Tips on the other, depending on whether or not the accompanying warning symbol is present.
Conceptually speaking, our user study does not pursue the same goals as a usability test in that our test subjects were not tasked to accomplish predetermined goals, nor were their actions subject to measurement in terms of efficiency and effectiveness (International Organization for Standardization, 1998). The interaction with the privacy notifications was

![Figure 5. Notifications 1–3 (third iteration). (a–c) Notification center, (d–f) Detailed view.](image-url)
specifically designed to devise evaluative research and to facilitate participatory design. Methodologically speaking, our approach is therefore akin to desirability testing and artifact analysis, both of which are conducted on a qualitative level.

3.4. Ethical approval

Before planning and conducting the user study, we applied for ethical approval abiding by the local ordinance of Karlstad University. The evaluation of our application at the relevant Faculty of Health, Science and Technology yielded that seeking ethical approval at the next highest instance, i.e., on a national level, was not required.

Information letters were provided to the participants at the beginning of the study (transcript provided online Murmann & Karegar, 2020). The document contained details about the purpose of the study and the form it will take, the way the test subjects’ personal data will be processed, and contact details of how to reach the researchers in the event of any uncertainties. The information letter was available in both English and Swedish language. The document was available in duplicate, one serving as a legal consent form, and one handed out for the participants’ records.

3.5. Conducting the user study

We recruited the participants for the lab study via word of mouth and via posters pinned on the public bulletin boards of various faculties throughout the campus of Karlstad University. The advertisement stated that the purpose of the study was to investigate privacy in the context of fitness tracking, which is why we preferred test subjects who actually tracked their health. However, hands-on experience with fitness trackers were not a strict prerequisite, nor was previous knowledge in terms of mobile apps.

We conducted three pilot studies from 2019–09-25 to 2019–09-26, the results of which carried over to a refined version of the prototype and moderation script, respectively. The main study was conducted in English with 16 participants in total in the course of three iterations between 2019–10-01 and 2019–10-25. Each iteration produced a series of findings, which we discussed and translated into a list of design changes (Appendix A). This enabled us to confront test subjects of the second and third iteration with a rapidly evolving prototype, each iteration of which incorporated the changes conducted previously. We stopped testing after the third iteration when the list of what could be realistically addressed by further changes became sufficiently short.

3.6. Demographics

Eight of the 16 participants were female, and eight male. The age groups were distributed as follows: 18–25: 4, 26–33: 7, 34–41: 1, 42–49: 1, 50–57: 2, 58–65: 1.

All participants were connected to academia in the broadest sense, including undergraduate or doctoral students, lecturers and administrators. Six participants indicated to have backgrounds in computer science, information systems, or software engineering. Other disciplines included chemical engineering, mechanical engineering, and biology. All but one participant indicated to have at least average knowledge of the ecosystem of mobile apps.

4. Results

We start off Section 4.1 by reporting general findings pertaining to our user study, as well as insight we gathered during the prologue. We then report the findings that were specific to each of the three iterations in Sections 4.2–4.4. Each of these sections commences with a summary of how the iteration related to its predecessors. We then follow up with observations regarding more specific topics, such as the participants’ preferences for settings and their perception of transparency and actionability.

4.1. General findings

4.1.1. General usage behavior

Our participants reported that they rarely changed the defaults of the privacy settings of the apps they used, mostly because they did not know how to go about it or where to find the settings. We conclude that privacy settings that are hard to find will not give users the opportunity to scrutinize the behavior of an app, let alone to make changes.

As regards notification preferences, some of the test subjects showed a noticeable tendency to postpone individual notifications, especially those related to Tips. It shows that the default settings may not reflect all of the individuals’ preferences. The upshot of our findings regarding the test subjects’ general behavior toward privacy settings is discussed in Section 6.4.

4.1.2. Expectations

As regards our participants’ expectations in terms of the functionality and capabilities of a TET that operates on the basis of privacy notifications, we learned that they expected to be provided with insight of how their personal data were processed, and how they would be able to intervene in the processing. They suggested that the TET should support them in understanding various facets of data processing, such as how and by whom, and what consequences that would entail for them. Furthermore, they expected to be able to exercise their intervenability rights and manage their interaction with online service providers. They also expected to receive simplified notifications and information about noteworthy facts related to their privacy. These expectations are well covered by the principles underlying privacy notifications and are congruent with what we covered in our prototype.

4.1.3. General impression

The underlying concept of receiving privacy notifications as compared to proactively seeking information was well received. One test subject went so far as to say that the concept and functionality of the prototype introduced a new niche. Some participants believed that a tool like the prototype may compensate for a lack of time and knowledge. It was mentioned that after a while users might take fewer actions based on the notifications they receive. Nonetheless, the majority of test subjects stated that they would not engage in other proactive
activities to investigate the processing of their personal data, which underscores the efficacy of the concept.

One participant remarked that using such a TET might create dependence and fuel false expectations in terms of feeling secure. Others explained that they would prefer to receive system notifications, i.e. “notifications from the phone,” rather than notifications from a particular app. It was pointed out that the prototype would be more useful if it also worked with other types of data services. The level of commitment in terms of paying heed to the information provided by the prototype was questioned by individual participants.

The prototype was deliberately created as a simplified version of what one would expect in the real world. This is reflected in our design decisions, such as a very limited variety of scenarios and low-key settings. Depending on their inquisitiveness, individual participants preferred further details about particular aspects presented to them while interacting with the prototype. The test subjects preferred both simplicity and more granular control depending on their respective level of knowledge, which calls for individualization of the TET to accommodate the individual user’s proficiency and needs.

Irrespective of the iteration during which they interacted with the prototype, it was apparent that the test subjects had different preferences with respect to the colors and shapes they suggested as replacements of, or in addition to the ones we currently used. Furthermore, their tastes differed greatly in terms of what characteristics an app ought to provide to give it a more individual character or be considered professionally designed.

4.2. First iteration

4.2.1. Summary

Some of the terms used throughout the settings and the detailed view of the notifications were not self-explanatory. It was not always clear why one of the actions was designated as being particularly appropriate. Some participants questioned the efficacy and effectiveness of taking action, were unsure whether and how individual actions could actually be taken, and what subsequent steps that entailed. More details about the facts provided as part of the Tip and the Breach notifications were required by some participants to be able to make a decision. Many participants had negative feelings about receiving recommendations. The meaning behind the warning symbol was clear.

These issues could negatively impact the transparency of the information provided regarding users’ intervenability rights and their ability to make informed follow-up decisions. We therefore made some changes after the first and second iterations. These changes are outlined in detail wherever we report about the rationale behind them. Additionally, we present a compact list of changes in Appendix A.

4.2.2. Privacy settings

Some of the terms used to describe the incidents in the settings were not comprehensible by the participants, some being considered too complex. For example, the term “Mhealth” was not self-explanatory, and “cyber attack” was questioned in terms of the ambiguity of its meaning. Hence, we replaced “mhealth service provider” with “fitness tracking service” and “cyber attack” with “attack from the Internet”.

One participant wanted to know about the number of different types of notifications one would receive at what frequency before changing the default settings. However, the actual number of notifications users receive will depend on actual circumstances. Accordingly, for such a conceptual problem we could not take any counteractions.

4.2.3. Transparency and actionability

As regards their choice of how to act and why, the participants referred to different visual cues as indicators of whether they should take actions, including the most appropriate action in the blue box and the instructions of how to take individual actions. It was also mentioned that it was not clear enough whether actions should be taken and how (Figure 4b). To counteract this problem, we decided to visualize more prominently how to take action. Accordingly, we made the expandable area that served as the entry point for these instructions more prominent in all notifications. We also added a sentence above the action panel that read “To take this action, follow these steps.” (Figure 6b). Besides, some participants expected to take actions directly in the TET and were unsure as to whether they could actually do that. We did not explicitly convey the lack of actionability to our participants either as a part of the introduction to the user study or in the prototype itself because we wanted to gauge their actual expectations in terms of how they would like to handle individual actions. Nonetheless, based on the results from all three iterations, we recommend designers to point out the lack of direct actionability explicitly, preferably when using such the TET for the first time.

While dealing with Notification 3, one participant was unsure as to whether moving one’s personal data from one service provider to another entailed that the data would be erased from the old service once the transfer was completed. To address this ambiguity, we added more information in the form of additional optional steps whenever moving data was an option, which applied to Notifications 2 and 3. Figure 6 shows how the steps including the optional ones were presented to the participants. In addition to moving their data, users may e.g. decide to delete their data from the previous service or withdraw their consent.

Although our participants generally preferred concise information with more pictorial items, they asked for more details about each scenario to make a decision, particularly for scenarios related to Breaches and Tips. For the Breach notification, some wanted to know more about what exactly happened, how and why. The Tip that recommended a more privacy-friendly mhealth provider was perceived as advertisement and spam. The participants questioned the sincerity of this advice. To be able to act upon the Tip, the participants requested more information for comparing the current mhealth service and the recommended one. They suggested providing a side-by-side comparison that juxtaposed the two services in terms of the level of privacy-friendliness and the features they offered. Nonetheless, we deliberately decided not to make any immediate and possibly premature changes, right after the first iteration. We postponed making any changes in
this regard until we received additional feedback to justify changing the design. It was just after the second iteration when we had more participants who had suggested similar forms of visualization. However, as providing in-depth secondary information was beyond the scope of the study, we decided to present respective information as dummy texts rather than as fully functional mock-ups.

Some of the test subjects stated that the efficacy of choosing some of the actions was unclear in that they doubted that taking action would actually help them improve their privacy. For example, one test subject doubted that anything would happen by opting out from profiling although the participant knew that exercising one’s data subject right was legally binding. This raised the question of trust, which we discuss in more detail in Section 6.6. In the second notification, the effectiveness of changing one’s password as the most appropriate action was questioned, especially when personal data had already been leaked. Some of the participants also questioned the reason as to why an action was designated as the most appropriate one in the first and third notification. To counteract the dubiousness of the most appropriate action, we added a hyperlink that provided secondary information on why the action in question was considered to be appropriate (see Figure 6a,b). The information itself was a dummy text.

In Notification 1, the scope of profiling and the consequences that arose for users turned out to be ambiguous. The phrase “… no longer have the right to analyze your data for the purpose of sending you customized advertisements” lacked clarity as to whether the service provider would still have the right to collect and analyze the data, but not use them for sending advertisements (see Figure 6a,b). This led to different interpretations as to what would happen if a data subject chose to opt out. Hence, we changed the text to avoid ambiguity. Some of the participants preferred to have access to the profiles created about them. However, such profiles are the assets of the service providers, which explains why respective functionality could not be part of a TET that operates legally independently from such entities. We discuss the boundaries of legal entities in more detail in Section 6.5.

The meaning behind the warning symbol was clear. The participants stated that the lack of the warning symbol in Notification 3 gave them the impression that taking action was optional and not urgent. As requested by our participants and to better attract their attention, we increased the size of both the warning symbol and its associated text (Figure 7c). As regards alternative iconography, the participants suggested to change the color of the symbol from red to orange or yellow, and to use a light bulb as an alternative icon for notifications that were not meant to signal urgency. We postponed introducing an alternative icon for informative, non-critical notifications until we had received similar suggestions in the second iteration.

4.3. Second iteration
4.3.1. Summary
We obtained no additional findings related to privacy settings in this iteration. Despite the design changes that we had made

**Figure 6.** Changes made after iteration 1 and iteration 2, respectively. The highlighted border of the lowest bounding box signifies that the secondary information displayed in this box appeared upon touch in the form of drop-down contents.
after the first iteration it was not always clear why one of the actions was designated as being particularly appropriate. The role of actions as a part of the notifications was not clear for all participants. Despite the changes we had made after the first iteration, some participants were unsure whether and how individual actions could actually be taken, although we had tried to convey the instructions of how to take subsequent steps more clearly. More details about the Tip and the Breach notifications were required to be able to make informed decisions. Many participants had negative feelings about receiving recommendations. Similar to the first iteration, the participants suggested a light bulb as an alternative icon to refer to non-critical notifications.

4.3.2. Transparency and actionability
One participant showed interest in receiving more information about the privacy policy of an app similar to the prototype in the study. The participant believed that the prototype tracked other apps to produce notifications about the processing of personal data. We discuss the prerequisite of trust in TETs in more detail in Section 6.6.

For the majority of the test subjects, multilayered information was well understood. However, similar to the first iteration, some requested further details about some of the scenarios. In particular, it turned out that secondary information about the incident that triggered Breach notifications needs to be provided. It was suggested that if news or press releases by the data controller who was affected by the attack from the Internet were available, such information ought to be made accessible too. The Tip was still received poorly and misunderstood as advertisement. Many test subjects demanded further details about the alternative service. As before, some requested a comprehensive side-by-side comparison of the features of both services and of their privacy policies.

Based on repeated requests from our participants in the first and second iteration, we added additional secondary information to the notifications to provide more clarity. For the Breach notification, we added a link that provided further details about the incident. For the Tip, we added three links providing details about the recommendation, the recommended service provider, and its privacy policy (Figure 5e,f).

Similar to the first iteration, we provided all additional information in the form of dummy texts that said that providing exhaustive information was beyond the scope of the prototype, but that respective information could be expected to be shown in a full-fledged implementation.

Some participants stated that the presence of options indicated that they needed to make a decision and take action. However, the role of actions as a part of the notifications was not clear for all participants. As we had already observed a lack of clarity regarding the scope of actions during the first iteration, we introduced dedicated bounding boxes for each of the actions rather than aggregating them in a continuous list. We also changed the color and the size of the heading above all actions, which now read “Applicable actions” to introduce the subsequent boxes of actions (Figure 6c).

Similar to the first iteration, some participants expected to have immediately actionable options in the prototype, which is why the lack of actionability confused them. Despite the changes we had made after the first iteration, some participants did not know how to take action, and missed the instructions on what steps they should take. It was also stated that the meaning of the term “Further Steps” was not clear. We therefore removed the sentence above each expandable area and changed the label “Further Steps” to “See steps for taking this action” (Figure 6c). We changed the color of the title related to each action from blue to gray. The blue color was misleading in that it caused some participants to assume that the actions were clickable hyperlinks and thus could be taken from the prototype itself.

One participant pointed out that it was not clear in the first notification whether the data that had already been collected so far would be deleted once one stops using a service. We therefore added a sentence saying that withdrawing consent does not necessarily imply deleting or moving one’s data once the option ‘Stop using ‘ was chosen. We also provided
additional optional steps that could be taken if one was to delete or move one’s data while withdrawing consent.

Similar to the first iteration, the comments of some of our participants revealed that the effectiveness of taking actions was unclear. For example, in the second notification about the data Breach, the effectiveness of changing one’s password was questioned. We did not make any changes to resolve this issue because we assumed that the secondary information provided on the appropriateness of the action (Figure 6a,b) will have to provide sufficient justification as to why the action is considered appropriate and effective. In addition, the implications of opting out from profiling presented in Notification 1 was still not well understood by all participants even though we had tried to improve the readability of the statement after the first iteration. Hence, the reason of why some participants could not correctly explain what would happen if they opted out needs further investigation. The lack of comprehension could be due to the ambiguity of the text, or because the test subjects in question did not read the text carefully enough.

Similar to the first iteration, the meaning of the warning symbol was clear, and the lack of warning gave our participants the impression that taking action and opening the notification was optional. However, some participants suggested to display the warning symbol more prominently when details of the notification are displayed. Similar to the first iteration, changing the color of the symbol from red to green and using light bulbs were suggested by participants to complement the warning symbol in less severe cases. In addition, it was suggested that color coding could be used to differentiate different levels of urgency or severity. However, depending too much on color might run the risk of discriminating users with visual impairments, which is why such mappings would have to be optional. Heeding the suggestions we had received so far, we added a light bulb with and text saying “There’s an opportunity to improve your privacy” (Figure 7d) for non-critical notifications that informed users about Tips and Consequences. We also altered the text accompanying the warning symbol to emphasize the fact that privacy will be improved in both cases if action is taken (Figure 7a,c). The warning after the second iteration read: “Immediate action is advised to improve your privacy.” To better catch users’ attention, we moved the warning symbol to the very top of the detailed view.

4.3.3. Miscellaneous

Some test subjects preferred to use a TET with a more individual character, such as in the form of a dedicated font, color palette, or a unique logo. We took from these suggestions that a logo might help identify and brand the TET more distinctively. Moreover, we wanted to distinguish clearly between our prototypical TET and the fitness tracking app provided by, which collected the actual personal data. We found that for our discussions with the participants it would be less ambiguous if we could refer to our prototype using a name. As a result, we created a logo for the prototype and named it Privacy Pigeon. The name pays homage to the type of messenger bird known to bear good and bad tidings from afar.

4.4. Third iteration

4.4.1. Summary

Some participants were unsure whether and how individual actions could actually be taken, despite the changes we had made in the previous iterations. More details about the scenario in the Tip notification were required by the participants. Many participants had negative feelings about receiving recommendations. The meaning of the light bulb symbol introduced in the previous iterations to refer to non-critical notifications was clear.

4.4.2. Privacy settings

Regarding the timing of privacy notifications, one participant suggested that if a notification was deferred to be received at a later time, there should be an option to receive it also as an e-mail to avoid missing it later on. This may indicate that the participant considered e-mail as a tried and tested means to play things safe, whereas the volatile character of notifications did not seem to fulfill the notion of sustainable archiving. However, despite the fact that this view may reflect the concept of error recovery (Murmann & Karegar, 2020), we did not investigate this dimension of privacy notifications in our study.

4.4.3. Transparency and actionability

Some participants appreciated multilayering. However, one stated that the notifications had lots of information with a structure that was not entirely clear, which made it hard to make an informed decision.

Similar to the previous iterations, the recommendation of an alternative mhealth provider evoked negative feelings and was perceived as undue advertisement. One participant (P12) said “I do not like receiving ads. Maybe in the settings I can toggle it to not receive such things”. Likewise, despite the dummy text we had provided, the Tip was expected to be accompanied by further details, such as a comprehensive side-by-side comparison of the user’s current mhealth service and the recommended one. Our participants’ recurring comments on Tips suggest that special care must be taken to back up recommendations with sufficient evidence to justify the authenticity and benignity of the underlying intent. In particular, respective messages need to provide sufficient informational substance to be useful for the recipient.

Similar to the previous iterations, many test subjects expected and preferred immediate actionability from the prototype. Despite the changes we had made in the previous iterations, some participants still missed the expandable instructions of how they should take an action. Additionally, the implications of opting out from profiling was still not always well understood. Some participants correctly believed that there would be no ads anymore once they had opted out. Others either did not trust that their action would be effective, or did not understand the implication of taking it. We conclude that the consequence of taking individual actions still needs to be made clearer. If possible, designers should leverage visual cues to indicate consequences more prominently (see Section 5.3 for
Table 1. List of design requirements.

<table>
<thead>
<tr>
<th>Code</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.</td>
<td>Indicate cause</td>
</tr>
<tr>
<td>C2.</td>
<td>Indicate sources</td>
</tr>
<tr>
<td>C3.</td>
<td>Indicate reliability</td>
</tr>
<tr>
<td>C4.</td>
<td>Contextualize privacy policy</td>
</tr>
<tr>
<td>U1.</td>
<td>Target lay persons</td>
</tr>
<tr>
<td>U2.</td>
<td>Use intelligible language</td>
</tr>
<tr>
<td>U3.</td>
<td>Emphasize key factors</td>
</tr>
<tr>
<td>L1.</td>
<td>Provide secondary information</td>
</tr>
<tr>
<td>L2.</td>
<td>Emphasize secondary information</td>
</tr>
<tr>
<td>V1.</td>
<td>Use standardized icons</td>
</tr>
<tr>
<td>I1.</td>
<td>Indicate necessity to act</td>
</tr>
<tr>
<td>I2.</td>
<td>Order options appropriately</td>
</tr>
<tr>
<td>I3.</td>
<td>Provide visual cues</td>
</tr>
<tr>
<td>I4.</td>
<td>Indicate consequences of acting</td>
</tr>
<tr>
<td>I5.</td>
<td>Indicate subsequent steps</td>
</tr>
</tbody>
</table>

requirements I3 and I4). For example, consequences could be conveyed under a title called “Consequences”.

5. Requirements

This section elaborates on and motivates the classification system underlying the revised set of design requirements, which constitute the fourth generation of an iterative elicitation process (see Section 3.1). They present the requirements that are reflected in the prototypical design, and that have been evaluated during the user study. This is not to say that the requirements that have not been included compared to the previous generation of requirements have been invalidated, only that they were not supported by the evaluation. For this very reason, the entire Delivery phase (see Figure 2), is e.g. absent from the revised set. A comprehensive document that includes all requirements including the ones not validated in the user study is available online (Murmann & Karegar, 2020). A tabular list of the requirements covered therein is provided in Table A1 in Appendix A.

In addition to describing the requirements, this section discusses the necessity and scope of individual requirements and groups of high-level themes. The structural themes, Configuration, Presentation, and Intervention, mirror the interaction phases shown in Figure 2. Some of these themes overlap slightly in that parts of the concept reported therein are covered in multiple themes. For example, many concepts related to Presentation equally apply to Intervention. A compact list of all requirements is provided in Table 1. The codes represent unique identifiers that label each of the requirements. They consist of a letter that denotes its thematic group and a number that refers to its position within that group.

5.1. Configuration

The requirements of this section reflect the user’s ability to configure and exercise control over the behavior of a TET that operates on the basis of privacy notifications.

5.1.1. Default settings

Default settings represent the settings that apply at the time of first use. Such settings may be overridden by run-time settings (Section 5.1.2).

Provide reasonable default settings (D1). The TET shall have reasonable default settings that are available at the time the tool is put into operation. These presets should be based on heuristics that satisfy the needs of the designated target audience of the TET.

5.1.2. Run-time settings

Run-time settings represent the settings chosen by the user of the TET during run-time and override the default settings (Section 5.1.1).

Make settings accessible (R1). Once the TET has been put into operation, the settings shall be easily accessible at any time to adjust the run-time behavior.

Rationale. Gabriele and Chiasson (2020) report that one reason why the privacy settings chosen for mHealth services are often suboptimal stems from the fact that the settings are often not accessed via the fitness tracking app itself, but instead rely on means such as a website provided by the data controller. This inconvenience leads to the settings sometimes not being reviewed at all. Hence, the need for close proximity to the settings of an application at all times equally applies to TETs whose primary purpose is to facilitate transparency.

Against the backdrop of ergonomic heuristics for the design of UIs, Scapin and Bastien (1997) classify flexibility as a function of adaptability, which suggests that tools require the "capacity [of the interface] to adapt to the user’s particular needs" (Scapin & Bastien, 1997). Forsell and Johansson (2010) proposed "minimal actions" as a dedicated design heuristic that aims to let users accomplish their respective goals with a minimum amount of interaction. Among several heuristics evaluated by Forsell et al. said heuristic ranked noticeably high.

As regards privacy notifications, the requirements specified in this section complement the findings from the domain of InfoVis with the concept of “respect[ing] user needs” identified in our previous work (Murmann, 2019).

Evaluation. The evaluation of the prototype suggested that notifications related to Tips ought to be optional. Whereas notifications related to Breaches and Consequences should be delivered per default, Tips should be delivered on an opt-in basis. We follow up on the scope and limitation of Tips in Section 6. It was reported that settings are often not easily accessible. For a tool that so heavily depends on adequate customization this suggests that settings ought to be accessible at all times.

5.2. Presentation

Requirements pertaining to presentation specify how information is presented to users by means of privacy notifications.

5.2.1. Contextual cues

Privacy notifications are not received in response to an action being carried out as part of a primary task, but are the result of an asynchronous circumstance or event (Fischer et al., 2011; Miyata & Norman, 1986). Hence, the resulting messages will most likely be received unexpectedly. Contextual cues designate measures that help users better understand the interplay of cause and effect pertaining to notifications sent in response to an event.
Indicate cause (C1). It shall be motivated why the user has received a particular notification.

It shall, e. g., be explained what events took place regarding the processing of her personal data, and why, how and to what extent these circumstances affect her privacy.

Indicate source (C2). If notifications make references to entities, types of data, or concrete or presumed measures of data processing, it shall be clear to whom or what these references pertain.

Indicate reliability (C3). To help recipients of notifications tell proven facts from hypothetical or predicted outcomes, the TET shall provide them with a measure of how reliable the information is. The TET shall indicate the estimated level of confidence, certainty or probability pertaining to the facts conveyed as part of a notification.

Contextualize privacy policy (C4). To allow for an actual-target comparison of facts at any time, the original privacy policy based on which the user has given her consent shall be linked as a source of reference.

If users follow a link that takes them to the privacy policy, they should ideally be referred directly to the part of the document that is most relevant for clarifying the information the user is currently dealing with.

Rationale. As regards the informational character of contextual cues, Bertin (1981) specifies information related to the relationship between subsets of data as the "intermediate level" of information. Together with the "elementary level", which denotes the elementary statistics of concrete data, the two levels form the basis for "overall information" that comprises both the characteristics of its components and the inter-relationship thereof. Bertin maintains that it is the overall information level that is necessary to facilitate decision-making on the part of the user, which reflects the actual purpose of privacy notifications.

In their attempt to deconstruct what they call "black boxes" as part of visualizing information, Amar and Stasko (2004) describe the "rationale gap" as a user’s inability to rationalize and align individual elements represented in an artifact. To bridge this gap, they recommend to concretize such relationships, preferably including the outcomes that will arise from their interplay. Parallel to reconciling the factors related to causation, Amar et al. recommend to clarify to what extent data can or should be relied on to draw reliable conclusions.

Tarrell et al. (2014) recommend to “aid reasoning with mental models” as a facet of discussing cognitive heuristics related to information visualization. They maintain that a user’s mental model shall be aligned with the visualization by providing cues that enable users to recognize the semantics of underlying structures.

Zuk and Carpendale (2006) provide a summative analysis of methods provided in the literature as to how uncertainty of information can be expressed in InfoVis systems. They draw on the theories provided by Bertin, Tuft and Ware to derive heuristics for modeling uncertainty, and investigate the literature for cases in which these heuristics have been applied. The heuristics primarily cover principles related to visualization, some of which may be employed to model the level of (un-)certainty pertaining to the information displayed as part of a privacy notification.

In the context of discussing unsolved problems related to information visualization, Chen (2005) counts the paradigm shift from static structures to dynamics as one of the issues designers of InfoVis systems face today. More and more real-world problems deal with longitudinal processes rather than static snapshots of information, which necessitates capturing the temporal progression of the entities and informational facets involved. Chen points out the issue of illustrating the causality of, and interference between multiple facets represented in a visualization. The author explicitly covers security and privacy-related topics under this issue, maintaining that these fields pose particular constraints in terms of facilitating decision-making based on multivariate data.

In our previous work (Murmann, 2019), we have dealt with the issue of contextualizing informational contents specifically in the usage context of privacy notifications. The requirements specified here reflect the guidelines proposed previously as to how understanding of the causality of a longitudinal process may be established.

Evaluation. Most test subjects appreciated learning about various details pertaining to an event. Since it was not always evident how reliable individual pieces of information were, indicating a measure of reliability for individual facts seems crucial. Some participants explicitly asked for the privacy policy of a data service, which suggests that it ought to be readily available as a reference.

5.2.2. Intelligibility

The requirements in this section describe the quality of information presented to users in the course of receiving a privacy notification. They deal with content-related properties in terms of conveying information meaningfully and understandably.

Target lay persons (U1). TETs shall primarily target lay persons, not domain experts. Experts may find additional, more detailed information on lower layers (see Multi layering).

Use intelligible language (U2). Clear and plain language shall be used to explain the phenomena pertaining to a scenario. Technical and legal terms shall be avoided, if they cannot be expected to be self-explanatory for a lay person.

Emphasize key factors (U3). Important facts that are crucial for understanding a scenario shall be emphasized. The small screens of mobile devices may result in the contents of a message potentially spanning multiple paragraphs and even multiple screens worth of information. Hence, relevant information must be eye-catching in that attention is drawn toward aspects that are particularly relevant for the user.

Rationale. The literature is rich with work on visualizing information to accommodate the needs of readers in terms of form and scope. The requirements specified here are particularly motivated by the recommendations of the following authors:

Chen (2005) counts the consideration of prior knowledge among one of the unsolved problems of information visualization. A lack of common ground as regards knowledge may arise from two types of deficiencies: (1) a lack of technical knowledge, i. e. proficiency to interact with a system, and (2) a lack of domain knowledge, i. e. the ability to interpret
contents to which one is exposed. By targeting lay persons, we intend to set the entry barrier as low as possible.

Nielsen (1994) describes the prerequisite for a “match between system and the real world” as familiarity with the language and terms, but also with the concepts used by an information system. Similarly, ISO 9241–110 (International Organization for Standardization, 2006) specifies self-descriptiveness and the conformity with user expectations as design requirements that should to be followed to achieve congruence between the user’s mental model with the designer’s.

**Evaluation.** Despite the fact that we targeted an audience of lay persons and were dealing with well-educated participants, the first iteration of evaluating the prototype made it clear that some of the terms were not self-explanatory and needed refinement. Pointing out the key factors as part of the summary in the notification center and at the top of the detailed view lead to the core information being conveyed more effectively and efficiently.

### 5.2.3. Multilayering

The requirements in this group seek to minimize the cognitive effort that it takes a user to establish a relational connection between two sources of information. They substantiate the concept of multilayering in that they encourage the availability of secondary information on request. Unlike intelligibility (Section 5.2.2), multilayering requires users to act to have the TET present additional information.

Multilayering denotes a hierarchical, top-down oriented information structure. It implements multiple layers of information that users can navigate back and forth between. Moving fine-granular information to lower layers allows for brevity on higher layers. Making such information optional puts users in control about whether and how much further details they prefer to see.

Multilayering comprises, but is not limited to, two different types of secondary information: Explanations of terms in the form of glossaries, and clarifications about the circumstances pertaining to a particular scenario.

A **glossary** is typically facilitated in the form of a hyperlinked, context-related help text. Its purpose is to explain the meaning of a term or the role of an entity. Respective information tends to be static in that it equally applies to all instances of the same key term. For example, the definition of the term “data controller” (GDPR Art. 4 (7)) will always be the same, regardless of the scenario to which secondary information about this type of entity is linked.

Conversely, **clarification** refers to providing further details about circumstances outlined on an upper layer. Such information tends to be specific to the circumstances pertaining to the scenario at hand. For example, a text on an upper layer might say that organizations A and B were involved in a transaction that involved processing the data subject’s personal data. Further details about the identities of A and B, and details about the nature of the transaction might be provided as secondary information on a lower layer.

**Provide secondary information** (L1). All information that may not be clear to non-experts shall be accompanied by additional secondary information.

For example, if technical or legal terms are inevitable for conveying the details of a scenario, explanations of these terms shall be provided on request.

Where applicable, more details shall be provided about a scenario, as well as about particular aspects of it, such as on the nature and identity of particular entities who are involved in processing the data subject’s personal data.

**Emphasize secondary information** (L2). It shall be visible at any time whether secondary information is available. The hyperlink or button that functions as an entry point for further details shall be clearly marked as such by making clear (1) that it is _actionable_, and (2) what its _function_ is.

**Rationale.** Shneiderman’s (1996) visual information seeking mantra epitomizes the notion of stacking and navigating between multiple layers of information. The principle of spanning a varying level of detail applies equally to different types of data, such as spatial and temporal data, or tree-like structures. All these types of information lend themselves to the informational structure of privacy notifications.

Tarrell et al. (2014) call the process of grouping information for the purpose of facilitating cognition “chunking”. They maintain that grouping information with strong cohesive properties can help minimize the cognitive load on a user’s memory while processing information. Extending their train of thought to informational structures based on dedicated layers, this principle lends itself to motivate the notion of “divide and conquer” that underlies multilayering. Similarly, Dix (2012) discusses various methods of visualizing large data structures with hierarchical or multi-faceted topologies through the lens of perceptual and cognitive factors. He highlights the necessity for, and particularities of means of interaction that enable users to navigate through and between multiple views associated with such data.

As regards guidelines pertaining to implementing transparency of information related to privacy, the Article 29 Working Party (Data Protection Working Party, 2016) discusses what they call a layered approach toward conveying information. They maintain that segmenting lengthy legal information into smaller portions can mitigate the cognitive load required to process the information in question. Segmentation can also simplify attempts to make such information navigable, such as when users need to be referred to a specific part or section of a privacy policy (see requirement C4). However, the guidelines published by the Article 29 Working Party refer to the structure of privacy policies managed by data controllers, which is why our requirements primarily draw on the extended guidelines suggested in our previous work (Murmman, 2019).

**Evaluation.** Nesting secondary information in multilayered structures lead to individual facts being accessible at each user’s leisure. However, it also suggested that the entry points need to be clearly recognizable in terms of what function they constitute to avoid the underlying layers of information being overlooked.

### 5.2.4. Iconography

In the context of privacy notifications, icons represent graphical depictions that illustrate, visualize or underpin the circumstances related to a scenario.
Use standardized icons (V1). Where applicable, standardized icons shall be used to illustrate the circumstances pertaining to a scenario.

Rationale. Bertin (1981) calls the efficacy of the perceptual process underlying semiotics “sensory immediacy”. He describes pictorial semantics as a function of convention, which in turn is the result of cultural imprinting and personal experience. At an extreme level, the distinguishing features of an artifact that facilitates awareness, recognition or realization can border on stereotypes. Conversely, diverging too far from convention in terms of visual primitives or interaction paradigms, be it accidentally or deliberately, is likely to face resistance on the part of the one interacting with the UI (Norman, 2004).

Nielsen’s usability heuristics (Nielsen, 1994) and the dialogue principles specified in ISO 9241–110 (International Organization for Standardization, 2006) advise to aim for congruence between the user’s mental model and the design space implemented by a UI. Nielsen’s heuristic of “Recognition rather than recall” underpins the rationale of the efficacy of pictorial contents with regard to relying on well-established iconography. This applies as well for the principle called “conformity with user expectations”.

Scapin and Bastien (1997) highlight the significance of codes, both in terms of terminology (see Section 5.2.2) and signs. As regards semiotics, they maintain that codes become significant to users if the semantics between a sign and the associated meaning, function or action are strongly established.

Tarrell et al. (2014) recommend to aim for congruence with the user’s mental model to facilitate cognitive cues that build on experience and knowledge, and that therefore minimize the cognitive load required to make the connection between visual elements and their meaning.

To this day, the visualization of scenarios related to data protection in general, and to information privacy in particular, has not been standardized. Research on the use of iconography for the purpose of replacing textual information has produced sobering results (Holtz et al., 2010; Pettersson, 2014; Siljew, 2015). Whereas complementary icons manage to emphasize the meaning of simple operations related to data processing, complex scenarios have so far defied graphical depiction. The same goes for compounds of multiple icons, the combination of which still fail to satisfactorily illustrate real-world examples.

In their guidelines on transparency, the Article 29 Working Party (Data Protection Working Party, 2016) maintains that decisive information required to facilitate decision-making and to exercise data subjects rights should not be replaced entirely by icons. Despite the fact that these recommendations pertain to the liability of data controllers, an oversimplification of details might clash with the purpose of privacy notifications in that lacking respective insight might prevent data subjects from making informed decisions.

Evaluation. The iconography that we sparsely used to indicate the urgency of the notifications throughout the prototype was largely appreciated and well understood by the test subjects.

5.3. Intervention

The requirements listed in this section aim at supporting actions taken in response to receiving a privacy notification. Taking an action is an umbrella term for reacting to a privacy notification, such as to exercise a specific data subject right, or to query a data controller for further details.

It should be noted that TETs cannot take legal actions on behalf of a data subject as this would require that data subjects willfully exercise their legal rights. A TET can only guide a user toward such an action and inform her about the subsequent steps she will have to carry out in the course of it.

Indicate necessity to act (I1). It shall be indicated if the user is supposed to act, i. e. if it is necessary or advisable to act upon the notification at hand.

Order options appropriately (I2). If multiple actions to act apply, they shall be presented in descending order of appropriateness. Options suitable for responding to a scenario shall be presented more prominently than less appropriate ones. In other words, preferable actions that should be taken in response to receiving a privacy notification shall be presented prominently, whereas less suitable options should be prioritized lower.

Provide visual cues (I3). Where possible, the TET should provide visual cues to emphasize whether it is necessary or advisable to act upon a notification. Visual cues serve as a means to emphasize the prominence of an option and the recommendation to act (see Section 5.2.4 for requirements on iconography).

Indicate consequences of acting (I4). The consequences of acting and not acting upon a notification shall be pointed out to users.

Indicate subsequent steps (I5). It shall be indicated what subsequent steps (operational, legal or otherwise) users will have to take once they choose to act in a certain way.

Rationale. The literature mostly discusses the design of security and privacy warnings, the effect such indicators have on users (Bravo-Lillo et al., 2013), the communication of risks (Bravo-Lillo et al., 2011), and means of actionability that ought to be part of the information conveyed (Egelman et al., 2008; Schaub et al., 2017). Conceptually, most work on privacy indicators is tailored toward ex ante transparency, i. e. respective authors imply scenarios that facilitate awareness about what will happen if users take or do not take specific actions.

Privacy notifications comprise a superset of such instances in that they also deal with scenarios that present results based on actions taken in the past. In previous work (Murmann, 2019), we have discussed the need to communicate the risks and consequences pertaining to a scenario, and to provide actionable choices in addition to any information conveyed. These guidelines have now been refined and broken down into concrete design requirements for privacy notifications.

Evaluation. The placement and framing of our indicators in terms of severity, urgency, and advice whether to act were understood well by the test subjects, especially due to the visual cues used for this purpose. However, for a considerable number of test subjects the lack of immediate actionability posed a considerable obstacle. We suspect a misalignment of their mental model with the conceptual limitations of standalone TETs (see Section 6.5 for further discussion of this topic).
6. Discussion

6.1. Reflection

The purpose of conducting the study was to receive feedback from actual and potential users of mhealth devices to facilitate the rapid prototyping of a TET with designated properties. The quick succession of the changes performed in response to three iterations of evaluation has succeeded in achieving this goal. It enabled us to create and improve a prototype in the form of a proof of concept, during the implementation of which we were able to ascertain and refine the characteristics necessary to better meet the needs of our target audience.

6.2. Reception of privacy notifications

The majority of the study participants felt positive about the concept of privacy notification. Usefulness, convenience and the complementary character of notifications instead of, or in addition to proactive investigation were among the features they mentioned most frequently. Appreciating the advice and guidance the prototype provided them with, some test subjects pointed out that tools such as the prototype may help bridge knowledge gaps, and enable them to make decisions they might otherwise have refrained from. A few participants pointed out the novelty of the approach to receive privacy notifications based on one’s preferences. This, they said, may give rise to set new trends, but could also be indicative of the necessity for a transitional period to allow users of mobile phones to adapt their usage patterns.

These findings suggest that customized privacy notifications may constitute an adequate means to provide users of mhealth services with transparency about how their data have been processed, as well as to guide their decisions in terms of exercising their data subject rights. It also suggests that the prototype managed to capture the participants’ expectations in terms of how such information can be suitably conveyed on a mobile phone.

6.3. Ambiguity of recommendations

Despite the explanation we provided during the prologue in terms of the scope and limitations of the prototype, some of the concepts and purposes were not always perceived as intended. One of the more obvious uncertainties concerned a misconception regarding the purpose of Tips (Notification 3) to serve a means to improve the recipient’s privacy. Some participants found it useful to receive recommendations about alternative mhealth services, some said such messages made them curious, and some stated they may even heed respective suggestions, potentially after investigating the matter a little further.

Conversely, a considerable number of participants found recommendations disturbing in that recommending alternative services contradicted their conception of a tool that was supposed to help them improve their privacy. Many described the nature of such messages as ads and commercials, akin to unsolicited offers for products that they were, for the most part, not interested in. Some went so far as to say that such messages negatively impacted their trust in the tool itself, and that it diluted their positive impression of privacy notifications as such. Some stated that they were unsure about the relationship between the creators of the prototype and the fictitious company recommended as an alternative service, and speculated that the tool might serve as a promotional platform.

Although we introduced brief dummy texts as to why the recommendations were objectively justified in later iterations, not all test subjects read the explanations in question, let alone took them to heart. Hence, we were unable to refute the negative associations with recommendations.

6.4. Settings

The defaults of privacy settings may endanger users’ privacy if the principles of privacy by design and default (GDPR Art. 25) are not observed. In addition, the one-size-fits-all approach for default settings may not satisfy the individual user’s needs. Our participants stated that they rarely reviewed the default settings of their apps, in part because the settings were not always easy to locate. These issues justify the importance of providing support during the first-time use of a TET. Moreover, the fact that a considerable number of test subjects adapted the default settings to meet their individual needs suggests that settings ought to be easily accessible (requirement R1). Although evaluating the accessibility of the settings was beyond the scope of our study, our decision to nudge users to review the settings during the prologue might have informed and educated those test subjects who would never have investigated the privacy settings of their real-world apps.

6.4.1. Categorization

When the participants reviewed the default settings for the first time, only a few of them postponed the two notifications related to Breaches, and only two out of 16 disabled notifications related to Consequences outright. Given the lack of insight about the predisposition of the participants of the study, these observations lead us to believe that the defaults we had chosen for the notification settings adequately reflected the needs of the target audience (requirement D1). In particular, the noticeable preference to receive notifications about Breaches confirmed previous findings about the consistently high preference in all types of Breach notifications (Mummert et al., 2019).

When they reviewed the settings of the prototype, a considerable number of participants chose to disable receiving notifications of either one or both scenarios related to Tips or postponed the delivery to the evening. This observation is likewise in line with our previous work (Mummert et al., 2019) in that Tips were selected less frequently and more selectively. The negative impression provoked by receiving recommendations could have been the result of being exposed to a type of notification that some of the test subjects preferred to disable when they reviewed the settings, which may have caused frustration when they had to deal with respective notifications afterward. Regardless of potential reluctance, however, we sought to obtain feedback from all test subjects about all three types of notifications, including Tips.
6.4.2. Default settings
As far as default settings of TETs are concerned, our findings suggest that receiving Tips should occur on an opt-in basis, whereas the opt-out policy implemented for Breaches and Consequences adequately reflects the requirement of privacy by design and by default stipulated by GDPR, Art. 25. It also underscores the relevance of requirements D1 and R1 in that TETs need to reflect a user’s preferences to be considered intuitive and useful. The fact that the test subjects’ preferences mirrored the categories relatively well suggests that the tripartite partitioning might also serve as an adequate pre-selective top-level scheme. Optionally, each of the categories could allow for further customization on a scenario-based level.

6.5. Transparency and intervenability
The extent to which the prototype helped us address our research question to facilitate transparency and intervenability was mainly satisfactory.

6.5.1. Intelligibility
The feedback we received from the test subjects indicated two distinctive dimensions regarding the intelligibility of visualized information. First, they expressed their preference for pictorial elements, such as icons, to guide them when they scanned the information at their disposal. Their preferences regarding the shape and color of individual informational elements was, however, not consistent. This is reflected in our design requirements, which not only suggest the presence of visual cues as such requirement I3, but which also ask for standardized visualization aiming to avoid ambiguity (requirement V1).

Second, many test subjects asked for additional information to aid them in making decisions, especially in the case of Breaches and Tips. In this regard, the concept of multilayered contents was widely appreciated. However, the informational structure used in the prototype was not always self-explanatory. Optimizing respective cues to emphasize the navigational structure of secondary information, and investigating to what extent previous knowledge and habituation affect the recognizability of nested contents may constitute an interesting branch of future work.

Our study showed that the meaning of the warning symbol used to signify urgency was unambiguous, and that the lack thereof lead our participants to believe that opening respective notifications and taking actions was optional. This association worked well to differentiate between Breaches and Tips. However, additional research will be required to propose a reliable, more granular distinction between multiple non-urgent categories of messages, such as to reliably differentiate between Tips and Consequences. Decidability based on unambiguous indicators will be particularly important on the initial layer of a privacy notification, i.e. as part of the synopsis displayed in the notification center of a mobile device (Figure 5a–c). Until then, our design requirements reflect the notion of supporting decision-making in terms of whether recipients should act immediately, or whether they can feel at ease to defer respective decisions without jeopardizing their privacy. Moreover, the requirements suggest to provide users with insight into the consequences of acting and not acting in a particular way for each of the options presented to them.

6.5.2. Actionability
Many test subjects stated that they expected immediate actionability to carry out their choice, i.e. they expected to be able to initiate respective actions directly via the TET. This expectation conflicted with the options available in the prototype in that respective actions were merely pointed out and clarified rather than made available. The expectation of being able to rely on actionable means to carry out their choice, such as via buttons or hyperlinks, resulted in several participants overlooking the instructions provided as part of the options. This is in line with what Habib et al. (2019) recommend in terms of immediate accessibility of actions as compared to merely explaining respective functionality.

The remarks of multiple test subjects related to actionability suggest that the availability of options as such will not necessarily mean that they will actually take the action of their choice. The fact that most options will require users to sign in to their mhealth service and follow a series of instructions to actually take an action made many of the options less attractive than they seemed at first glance. Moreover, switching back and forth between the TET and a service portal would make it inconvenient to carry out the instructions provided by the TET. The reason for this disparity are the legal and technological constraints introduced by the interplay of two legal entities, the TET and the mhealth service.

6.5.3. Jurisdiction
Provided that actionability was available, several participants stated that they would have preferred assurances once they took a particular action, preferably in the form of a statement that said that by having performed the action in question their data would be secure. The difficulty of issuing respective warranties on the part of a TET is two-fold: First, the TET was conceptualized not to operate on behalf of a particular data controller, but merely draw on information provided by that entity. Any prediction as to how operational or organizational measures might affect the data subject would not only be purely speculative, but would also transcend the spheres of influence of multiple legal entities. These entities include, but are not limited to, the maintainer of the TET and the data controller responsible for the mhealth service. Second, even if the TET was entirely orchestrated by the data controller, conjectures of the efficacy of individual measures may still be inaccurate and far from deterministic. Assurances would be particularly problematic as soon as unknown third parties were involved, such as in the case of data Breaches. Respective assurances from either party regarding the efficacy of actions would, most likely, be premature.

Hence, any TET operating independently will have to rely on predictions and will not be able to make assurances. It will have to convey the uncertainty of respective statements and the actions taken in response regarding their causality, efficacy, and reliability (Amar & Stasko, 2004; Chen, 2005).
6.6. Trust

A recurring theme regarding TETs is the extent to which such tools can be or should be trusted in the first place (Janic et al., 2013; Murmann & Fischer-Hübner, 2017). While trust is often considered a prerequisite to overcome or mitigate concern related to information privacy (Janic et al., 2013), TETs take the notion of reliability to an even higher level in that they make judgmental statements about the appropriateness and trustworthiness of other data services (Murmann & Fischer-Hübner, 2017). We therefore argue that reliability is indispensable if TETs were to establish and maintain an adequate level of trust on the part of their users. We will not elaborate on possible means of establishing trust, such as via privacy seals or code reviews. We suggest instead that adequacy should be be achieved in the form of accordance between the functionality of a TET and the expectations of its users. If a TET does not satisfactorily cater to the needs and expectations of its users, such as by presenting unsolicited information or exhibiting unexpected behavior, users will question such behavior and potentially stop using the tool.

6.6.1. Efficacy of actions

Another dimension of trust concerns the issue of whether data services will actually pay heed to the choices made by data subjects. Several participants of our study questioned the efficacy of exercising their data subject rights because they suspected that their choices would not be honored. This lack of trust in the underlying data service is in line with what Habib et al. (2020) report about a user study, in which many participants doubted that their choice to have their data deleted and to opt-out from receiving marketing e-mails and targeted ads will be respected by the service in question. A study conducted by Herrmann and Lindemann (2016) reports that respective concerns may not be unjustified. It reveals that less than half of their data provision requests to exercise their right of access (GDPR Art. 15) were answered satisfactorily by the service providers involved. The analysis on the response rates of manufacturers of fitness trackers to data subject requests in Canada reported in an Open Effect Report (Hilts et al., 2016) provides results that are similarly disillusioning.

6.7. Holistic user experience

As far as client-sided TETs that operate locally under the user’s control are concerned, it has been pointed out in the literature (Angulo et al., 2015; Fischer-Hübner et al., 2016) that the effective sphere of influence governed by a technological artifact requires clarification. Users have difficulties to understand where exactly data reside at the time when they make decisions, and what potential influence they have to intervene in the processing. We therefore assume that the users of a TET will not always be able to differentiate between the TET itself and the data service for which it provides transparency. Hence, respective inadequacies on the part of a data service will most likely be perceived as a shortcoming of the TET. Only if data service and facilitator go smoothly hand in hand will users be able to experience usable transparency and intervenability. Our prototype exemplifies a TET that provides advice and guides decision-making. To actually take operational steps for users is beyond its scope. The first step toward a smoother integration of exercising a user’s data subject rights is to inform data controllers about the user’s choice. However, even if the technical and legal issues regarding the collaboration between TET and data service could be solved, heeding the user’s choice would ultimately be up to the data service.

At this point in time, the most promising solution might come as a TET provided by the data service itself. The TET could take the form of a dedicated app, as part of the original health tracking app, or as an extension of the dashboard provided on the service portal. For the foreseeable future, this approach will most likely be one of the few solutions that are technologically and legally feasible in terms of providing immediate actionability. Moreover, an integrated approach will most likely provide the smoothest user experience, and thus help create trust in the data service. It will, however, raise the question as to why data controllers should send notifications related to scenarios that go beyond what is necessary to satisfy legal compliance, e. g. in terms of data breach notifications (GDPR Art. 34). Receiving Consequences or even Tips may not only be similarly informative for certain users, but receiving such messages will also constitute a higher potential to exert palpable influence to improve the user’s privacy.

6.8. Limitations

With only three pilots and 16 actual test subjects, our user study is limited in terms of the generalizability of the results obtained. It is due to the small sample size that we have refrained from reporting any quantitative data, as individual outliers would have strongly affected the outcome. This goes especially for data collected during each iteration, which amounted to six, five, and five individuals for the first, second and third iteration, respectively.

Most test subjects were in their 20 seconds or early 30 seconds, were affiliated with academia, and had on average good knowledge of the mobile ecosystem. Some of the specifications made by individual participants reflected considerable expert knowledge and a high level of analytical ability. However, even though we received feedback regarding the need to increase, for example, the granularity of the settings, we also had opposing voices asking to simplify the UI even more. We surmise that a broader spectrum of users would have shifted the design requirements slightly toward simplicity. At the same time, the high diversity we observed even in a group as small as ours suggests that focusing exclusively on either end of the spectrum may exclude potential users residing on the other end. This implies that TETs will have to accommodate multiple levels of previous knowledge in more than one respect, such as during the configuration of the TET and its actual use. It also means that the population of our user study was not representative of the full spectrum of users envisioned for a TET employed in the usage context at hand.

To satisfy the contextual specificity required for evaluating the usability of an artifact (International Organization for Standardization, 2010) we chose personal health tracking as our context of use. Both the theme introduced during the prologue and
the exemplary scenarios presented during the notification phase primed our test subjects for this context. This raises the question as to whether our design requirements will be applicable to other application domains in the ecosystem of mobile phones. Hence, further research will be required to ascertain how well the requirements generalize in terms of using privacy notifications for other fields. Besides, our exemplary scenarios could have affected how our participants perceived the prototype as a whole, i.e. its usefulness and efficacy. For example, the scenario we had selected for the category of Tips (moving to an alternative service provider) could have influenced users’ preferences regarding the usefulness of receiving such notifications.

As is explained in Section 3.3, validating the design requirements related to the delivery phase of privacy notifications was beyond the scope of our user study. One possible way of how future work could complement our findings might be via a longitudinal field study. To gauge opportune moments for the delivery of various types of notifications, a test subject would receive privacy notifications at specific moments over a longer period of time. Harnessing participants’ mobile phones (BYOD) would ensure high availability and potentially more sustainable response rates than would additional supplementary devices. Ideally, the mobile agent issuing the notifications would not only collect feedback on the perceived usefulness of the messages, but also on why the message in question did or did not fulfill its designated purpose. The literature is rich in work on gauging notification preferences depending on the time and purpose of notifications (see e.g. Patil et al. 2015; Pielot et al. 2017). However, evidence about how well respective notification preferences apply in the context of helping users improve their online privacy is still lacking.

7. Conclusion

To this day, few usable tools exist to provide users of online data services with transparency of how their personal data have been processed, and advise them about making informed decisions of how to intervene in the process based on the information obtained. Privacy notifications can facilitate said functionality by accommodating user needs for the ecosystem of mobile phones. To address the lack of concrete design requirements for implementing usable artifacts, we elicited a preliminary set of design principles from the literature. We implemented a prototype for the usage context of personal health tracking and conducted a qualitative lab study to evaluate both the implementation and the requirements therein. Prototyping and evaluation were carried out in the course of three iterations. This iterative process yielded a proof of concept in the form of a prototypical implementation of a TET which demonstrates how privacy notifications can be suitably implemented. Moreover, it produced a set of revised design requirements that reflect the results of the evaluation.

The concept of privacy notifications and the overall functionality of the prototype were received positively. However, the test subjects preferred additional empowerment in terms of taking immediate actions instead of just being informed. The findings obtained during the evaluation of the prototype lead us to believe that privacy notifications have the potential to provide users of mobile devices with customized, situational awareness of matters pertaining to the processing of their personal data. This enables them to make informed follow-up decisions to improve their privacy. Moreover, the set of evaluated design requirements can provide designers with the principles necessary to harness privacy notifications to implement legal compliance in terms of transparency.

Notes

2. During the study, we used the name of a well-known manufacturer of fitness bracelets, which has been blinded using R as a placeholder.
3. The three categories Breaches, Consequences and Tips are capitalized to avoid ambiguity.

Acknowledgments

We kindly thank the participants of our user study for evaluating the prototype and for providing us with insightful comments. We thank Simone Fischer-Hübner for her extensive advice and her comments on our work. We thank the reviewers of this article for their detailed and insightful comments on our work.

Funding

The research that has lead to this publication has been supported by the EU’s Horizon 2020 Research and Innovation Programme under the Marie-Skłodowska Curie Grant [675730], and by the project PAPAYA (A Platform for Privacy Preserving Data Analytics), which is funded by the Horizon 2020 Framework of the European Commission under grant agreement No. [786767].

References


security-decision UIs to make genuine risks harder to ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS ’13 (pp. 6:1–6:12). ACM.


**About the Authors**

**Patrick Murmann** obtained his PhD from Karlstad University in Sweden. His research reconciles the legal requirements of information privacy and design principles related to HCI. His work focuses on creating transparency-enhancing tools that accommodate the needs of their users.

**Farzaneh Karegar** obtained her PhD degree in December 2020 from Karlstad University where she currently works as a postdoc researcher. Her research interests include, but are not limited to, legal and societal aspects of information privacy, usable privacy and consent, privacy-enhancing tools, and algorithmic transparency.

**A. Appendix**

**A1. Glossary.**

- Name of a well-known manufacturer of fitness bracelets used in the course of the user study.

**Breach.** Personal data breach. One of the three categories of scenarios.

**Category.** The category of a scenario. We consider three categories of scenarios: (personal data) Breaches, Consequences and Tips (introduced in Section 3.3).

**Consequence.** One of the three categories of scenarios.

**Data controller.** Entity that determines the purposes and means of how personal data are processed (GDPR Art. 4 (7)).

**Data processor.** Entity that processes personal data on behalf of a data controller (GDPR Art. 4 (8)).


**Intervenability.** The legal right to intervene in the processing of one’s personal data.

**mHealth.** Mobile health. We consider mhealth in the non-clinical context of fitness tracking, self-quantification, and personal informatics.

**Personal data.** “any information relating to an identified or identifiable natural person” (GDPR Art. 4 (1)).

**Privacy Pigeon.** Name of the prototypical TET used in the course of conducting the user study (Section 3.2).

**Scenario.** A particular course of events pertaining to the processing of personal data in the context of mhealth.

**TET.** Transparency-Enhancing Tool. A technological artifact facilitating transparency about how personal data have been or will be processed.

**Tip.** One of the three categories of scenarios.

**Transparency.** Clarity and intelligibility of information.

**A2. Questions.**
Questions asked during the prologue:
• Are you actually tracking your health by an app on your phone?
• If yes, with what kind of device, for what purpose, and for how long?
• What would be your expectation of such a privacy-enhancing app?
• In what way could such an app be useful for you?

Questions asked when the test subjects reviewed the default settings for the first time:
• Is there anything about the settings that you do not agree with?
• Is there anything unclear?
• Would you prefer to change the settings? – If so, what would you change?
• Do you usually change the default privacy settings for the apps on your phone?

Questions asked during Notification 1 (Consequence):
• How would you know whether you should take any actions based on this notification?
• What action would you take and why?
• What do you feel was missing for you to be appropriately guided in deciding what action to take?
• What would happen if you took the action you want to take?
• What should you do next if you chose to act in a certain way?

Questions asked during Notification 2 (Breach):
• Do you think that the red indicator at the top makes it clear enough for you to act upon this notification?
• What action would you take and why?
• What do you feel was missing for you to be appropriately guided in deciding what action to take?

Questions asked during Notification 3 (Tip):
• How do you feel about the fact that the red indicator, which we’ve discussed as part of the previous notification, is not there anymore?
• Could you think of an alternative indicator for the cases which do not need the red indicators?
• What action would you take and why?
• What do you feel was missing for you to be appropriately guided in deciding what action to take?

Questions asked during the epilogue:
• What is your general impression of the prototype?
• How useful do you consider receiving notifications compared to investigating the matters on your own?
• How can the prototype be improved to better reflect your needs?

A3. Changes.
Design changes made to the prototype after iteration 1:
• Settings: Change the term “Mhealth” to “fitness tracking service”.
• Settings: Change the term “cyber attack” to “attack from the Internet”.
• Notification center: Change size of the warning symbol and the accompanying text to 150% and 120%, respectively.
• Detailed view: Add “Why is this appropriate?” to justify the most appropriate action indicated for each notification.
• Detailed view: Change the link color of “Why is this appropriate?” from blue to dark blue to enhance its contrast.
• Detailed view: For the scenario related to profiling, change the text “from now on, will no longer have the right to analyze your data for the purpose of sending you customized advertisements” to “from now on, * will not profile you any longer and will not send you advertisement”.
• Detailed view: Move the label “to take this action,” from inside the expandable drop-down box above the box.
• Detailed view: For all scenarios related to moving to another service provider: Add optional further steps.

Changes made after iteration 2:
• Notification center: Introduce a light bulb as a graphical counterpart to the red warning symbol.
• Notification center: The text accompanying the bulb should read: “There’s an opportunity to improve your privacy.”
• Notification center: The text accompanying the warning symbol should read: “Immediate action is advised to improve your privacy.”
• Detailed view: Use dedicated bounding boxes for each of the actions.
• Detailed view: Above the boxes, add an additional heading saying “Applicable actions:”
• Detailed view: Move the warning symbol to the top of the detailed view.
• Detailed view: Change the heading of each action to “See the steps for taking this action”.
• Detailed view: Add secondary information using links in the notifications to improve transparency; further details about the Breach incident, and the recommended service provider and its privacy policy as part of the Tip.
• Detailed view: For the option called ‘Stop using ‘, add: “All your data will remain unchanged, unless you take additional steps to erase or move them.”
• Detailed view: For the same context, add optional steps to erase and move data, much like in the scenario related to data portability.
• General: Name the prototype “Privacy Pigeon.”
• General: Create and include a logo for Privacy Pigeon to be used on the start screen and in the notification center.

A4. Requirements.
Table A1 contains the full list of design requirements including the ones related to the actual delivery of notifications. Items marked with an asterisk (*) denote design requirements that have been validated, i.e., whose efficacy has been evaluated via the user study. The full document in available online Murmann and Karegar (2020).
Table A1. Full list of design requirements and superset of Table 1. ’ ’: requirement has been validated.

<table>
<thead>
<tr>
<th>Code</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td></td>
</tr>
<tr>
<td>D1.</td>
<td>Provide reasonable default settings *</td>
</tr>
<tr>
<td>D2.</td>
<td>Accommodate predisposition</td>
</tr>
<tr>
<td>R1.</td>
<td>Guide first time use</td>
</tr>
<tr>
<td>R2.</td>
<td>Make settings accessible *</td>
</tr>
<tr>
<td>Delivery</td>
<td></td>
</tr>
<tr>
<td>T1.</td>
<td>Provide scenario-wise timing</td>
</tr>
<tr>
<td>T2.</td>
<td>Implement privacy by default</td>
</tr>
<tr>
<td>M1.</td>
<td>Provide scenario-wise modality</td>
</tr>
<tr>
<td>M2.</td>
<td>Reflect situational circumstances</td>
</tr>
<tr>
<td>M3.</td>
<td>Provide multiple modalities</td>
</tr>
<tr>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>C1.</td>
<td>Indicate cause *</td>
</tr>
<tr>
<td>C2.</td>
<td>Indicate sources *</td>
</tr>
<tr>
<td>C3.</td>
<td>Indicate reliability *</td>
</tr>
<tr>
<td>C4.</td>
<td>Contextualize privacy policy *</td>
</tr>
<tr>
<td>U1.</td>
<td>Target lay persons *</td>
</tr>
<tr>
<td>U2.</td>
<td>Use intelligible language *</td>
</tr>
<tr>
<td>U3.</td>
<td>Emphasize key factors *</td>
</tr>
<tr>
<td>L1.</td>
<td>Provide secondary information *</td>
</tr>
<tr>
<td>L2.</td>
<td>Emphasize secondary information *</td>
</tr>
<tr>
<td>L3.</td>
<td>Contextualize secondary information</td>
</tr>
<tr>
<td>L4.</td>
<td>Aid navigation between layers</td>
</tr>
<tr>
<td>V1.</td>
<td>Use standardized icons *</td>
</tr>
<tr>
<td>V2.</td>
<td>Avoid non-standardized icons</td>
</tr>
<tr>
<td>V3.</td>
<td>Avoid compound iconography</td>
</tr>
<tr>
<td>Intervention</td>
<td></td>
</tr>
<tr>
<td>I1.</td>
<td>Indicate necessity to act *</td>
</tr>
<tr>
<td>I2.</td>
<td>Order options appropriately *</td>
</tr>
<tr>
<td>I3.</td>
<td>Provide visual cues *</td>
</tr>
<tr>
<td>I4.</td>
<td>Indicate consequences of acting *</td>
</tr>
<tr>
<td>I5.</td>
<td>Indicate subsequent steps *</td>
</tr>
<tr>
<td>X1.</td>
<td>Provide history</td>
</tr>
</tbody>
</table>