Pervasive and Mobile Computing 77 (2021) 101480

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Reconciling the what, when and how of privacy notifications in fitness tracking scenarios

Patrick Murmann [a], Matthias Beckerle [a], Simone Fischer-Hübner [a,*], Delphine Reinhardt [b]

[a] Karlstad University, Karlstad, Sweden
[b] University of Göttingen, Göttingen, Germany

ARTICLE INFO

Article history:
Received 15 December 2020
Received in revised form 1 September 2021
Accepted 8 October 2021
Available online 16 October 2021

Keywords:
Customisation
Fitness tracking
Privacy notifications
Transparency-enhancing tool (TET)

ABSTRACT

The increasing number of fitness tracking wearables deployed worldwide poses challenges to the privacy of their users, esp. in terms of transparency. Privacy notifications facilitate transparency by providing users with situational awareness about the processing of their personal data. We present the results of two online surveys including English-speaking ($n_{Eng} = 154$) and German-speaking ($n_{Ger} = 150$) users of fitness tracking devices from Europe, conducted to elicit determinants of notification settings. We found evidence for the perceived usefulness of privacy notifications, and for concordant predictors in terms of when and how users prefer to be notified about personal data processing in 12 scenarios related to fitness tracking.

1. Introduction

The worldwide number of shipped units of fitness tracking devices will grow from 77.85 m in 2019 to an estimated 105 m in 2023 [1]. As of 2022, this will account for projected penetration rates of 8%–10% in English- and German-speaking countries in Europe [2]. Personal health tracking constitutes a niche field of mobile health (mhealth), which is carried out by laypersons in non-clinical environments to improve their health [3]. Fitness trackers enable their users to track a large variety of physiological characteristics, their geographic location, and annotated sensitivities. Facilitating an advanced form of life-logging [4], this allows for far-reaching quantification of an individual's life [3,5].

At the same time, the EU General Data Protection Regulation (GDPR) [6] stipulates the principle of transparency for personal data processing (Art. 5, 12). Transparency can be provided *ex ante*, before personal data are disclosed, or *ex post* after data collection, to inform data subjects about the processing of their personal data [7]. The GDPR requires that individuals shall be able to exercise control about the processing of their personal data (recital 7). This constitutes the concept of *intervenability*, i. e. the right of data subjects to exert influence on the processing of their personal data [8]. However, these objectives have hardly been met as many data subjects do not seem to be aware of the consequences of personal data processing [9].

Notifications draw on a paradigm that is well established on mobile devices. Various authors investigated aspects related to optimising the delivery of push notifications (see e. g. [10,11]). In a different branch of research, researchers investigated privacy notifications as a means to facilitate transparency on mobile platforms (see e. g. [12,13]). We seek to contribute to this line of work by reconciling aspects related to usability with regard to facilitating ex post transparency.

* Corresponding author.
E-mail address: simone.fischer-huebner@kau.se (S. Fischer-Hübner).

https://doi.org/10.1016/j.pmcj.2021.101480

Drawing on the definition provided by Oxford[1] and Merriam Webster,[2] we comprehend the term *(privacy) notifications* as an abstract idiom indicating that someone or something (an app or service) notifies someone (the user/data subject) about something (the processing of their personal data). Various Transparency-Enhancing Tools (TETs) in the literature rely on customisation to help accommodate user needs, but only few authors systematically ascertain the needs of their target audience [14]. Since TETs are either not available or do not adequately cover mhealth services [14], our objective is to design a TET for the usage context of personal health tracking, and to rely on adaptability via customisation to satisfy user needs. By doing so, we aim at enhancing usable ex post transparency for users of fitness trackers by conveying insight about the processing of their personal data and provide personalised advice. This goal is aligned with the aspiration of most EU citizens to be informed about data breaches [15] and motivates our research questions:

RQ1. To what extent do users find different types of privacy notifications useful?

RQ2. To what extent do cultural context, demographics, usage characteristics, the option for intervenability, as well as the type, timing, and modality of privacy notifications serve as determinants that help predict suitable notification settings for users of mhealth services?

To address them, we conducted two online surveys, one for English-speaking users of fitness tracking devices from the UK ($\mathcal{C}_{\text{Eng}}$) and one for German-speaking users in Germany, Austria, and Switzerland ($\mathcal{C}_{\text{Ger}}$). Privacy is a cultural construct [16]. We chose to compare the UK vs. German-speaking European countries because of the large differences between these groups in terms of privacy perception and practices that may impact their notification preferences. Particularly, a recent Eurobarometer survey [17] showed that UK citizens feel to a large extent to be better informed about conditions of collection and further use of their data on the Internet. They feel to have more control over their data than German or Austrian citizens (where Germany is in fact the European country with the lowest level of perceived control with only 6% stating a perception of complete control). UK citizens reported that they had to a larger extent tried to change their social network privacy settings than German or Austrian users. Also, previous research showed a gravitation of German participants towards more advanced and active privacy methods, compared to US and UK participants [18], and that Germans found privacy controls more important than others [19]. According to [20], $\mathcal{C}_{\text{Ger}}$ represents uncertainty avoidance countries that try to avoid privacy risks, while in contrast $\mathcal{C}_{\text{Eng}}$ represents a country with a low uncertainty avoidance score. Moreover, our choice was motivated by the comparatively high penetration rates of wearables in these countries [2].

Our findings provide quantitative evidence of determinants for notifications settings and allow us to derive design guidelines for TETs.

The rest of this paper is structured as follows: Section 2 discusses related work. Section 3 reports the methodology, while Section 4 details the study design. Section 5 presents our results discussed in Section 6. Section 7 concludes the paper.

2. Related work

We discuss related work on privacy notifications (Section 2.1), on preference-based user segmentation (Section 2.2), and privacy personas (Section 2.3).

2.1. Privacy notifications

Usability aspects of TETs have mainly been studied for privacy notices that are presented to users *ex ante* [21]. Conversely, our work researches *ex post* privacy notifications, which users receive after having disclosed personal data. Other related work on ex post privacy notifications are e. g. provided by [13,22] targeting Android app permission settings, and the usability of a feedback mechanisms for contextual messaging [23]. However, they address other application areas and a smaller set of notifications than we do.

Wu et al. [24] researched the impact of the design of security notifications on users' perceived security and observed that "app users routinely ignore security notifications" and that "[d]isruptive mobile security notifications cause irritation". These findings motivate us to investigate user preferences for privacy notifications and signalling modalities such that they will be meaningful for the recipients, will not be ignored or be perceived as disruptive, and will thus facilitate usable transparency.

Our previous work [25] investigated the structural clustering of privacy notifications based on content. We confirmed a three-fold categorisation of scenarios related to personal data processing, which serves as the basis for grouping scenarios in this paper (Section 3.1). Whereas our previous results are based on dichotomous data, this paper relies on fine-granular valuations of how strongly respondents prefer to be notified about individual scenarios.

In addition to content, decisive factors of the efficacy of notifications are when they are received and how the delivery is signalled (see e. g. [10,11]). Micallef et al. [26] investigated multiple combinations of modalities in the context of 'privacy nudges' to induce behavioural change. Whereas multiple facets of notification preferences had been investigated in isolated contexts [25,27], we missed a holistic reconciliation of the determinants of privacy notifications, which we investigate in this paper.

[1] Oxford Dictionary, 2021: "The action of notifying someone or something".

[2] Merriam Webster Dictionary, 2021: 1: "the act or an instance of notifying", 2: "a written or printed matter that gives notice".

2.2. User segmentation

To assist users in customising their privacy settings, various authors have investigated the concept of user profiles in the context of the Android permission system. When apps request system permissions, they effectively request access to resources related to the user's personal data, such as the contact list, geographic location, or various sensor data.

Liu et al. [28] derived clusters of user profiles by considering users' preferences in terms of whether they preferred to allow or deny various kinds of permissions, or whether they preferred to be asked on a case-by-case basis when individual apps requested the permission in question. Lin et al. [29] derived the profiles from user ratings that indicate how comfortable users were with various combinations of permissions requested for specific purposes. Both groups of authors used the profiles to derive models that enable them to predict a user's future choices and support them with recommendations. Liu et al. [13] proposed a privacy assistant that provided users with personalised recommendations to improve their privacy with more restrictive settings. We draw on the notion of customisation to provide users with information they consider relevant and useful.

Jackson et al. [12] conceptualise their prototype as a tool that facilitates soft-paternalistic nudging at the moment when users make decisions that may affect their privacy in the future. They comprehend privacy notifications as an informational means to illustrate discrepancies between users' predisposition in terms of their privacy attitude and their imminent action of installing a particular app by informing them about the consequences that may arise from doing so. We acknowledge the necessity to reflect a user's predisposition to facilitate suitable privacy notifications. However, we do so mainly retrospectively, i. e. in response to events that have taken place in the past and that affect a user's privacy in the present or future.

Wijeskskera et al. [30] and Votipka et al. [31] discuss users' perception of permission requests issued in the background compared to requests issued at the time users actively use an app for a specific purpose. Votipka et al. [31] report that users are less comfortable with the fact that their personal data are shared with third parties by background processes than they are with data shared for a specific purpose and context. Wijeskskera et al. [30] report that an automated personalised permission manager can effectively adapt to a user's preferences, recommending customised settings based on the situational context of a permission request.

Since privacy notifications are inherently asynchronous in the sense that they provide their functionality independently from a user's foreground activity, we seek to elicit opportune moments to convey insight that enables a recipient to make informed decisions.

2.3. Privacy personas

Privacy personas segment users based on their privacy attitude or behaviour. Dupree et al. [32] clustered their users based on IT proficiency and the willingness to put such knowledge to good use. Morton et al. [33] based their analysis on statements related to constructs such as concern of and trust in online services. We use these constructs to model predisposition (Section 3.2) and leverage them as possible predictors of preferences.

2.4. Open questions

Obtaining knowledge about a user's predisposition and attitude towards privacy may help provide her with the appropriate type of privacy notifications. We therefore build on the work of these authors by leveraging the determinants of trust, concern, and technical proficiency (see Section 3.2). We harness user segmentation as a means to ascertain how individual determinants can be grouped into suitable clusters of notification settings in the context of mhealth.

In summary, this paper provides the first detailed study on users' privacy notification preferences in the context of mhealth services with regard to different categories of notifications, timing, and signalling modalities.

3. Methodology

We conducted two quantitative online surveys to investigate how users of mhealth services prefer to be notified about various scenarios related to personal data processing. We analysed how our participants' notification preferences related to their predisposition and usage characteristics. In doing so, we hoped to elicit relational patterns that would help us design TETs that effectively account for the needs of their users.

3.1. Modelling notification preferences

Depending on how personal data have actually been processed, the delivery of privacy notifications constitutes an asynchronous event whose frequency and actual time of arrival are non-deterministic quantities. We therefore investigate factors that may affect the efficacy and perceived utility of privacy notifications. We model notifications preferences by collecting quantitative measures related to incidences or facts that users prefer to be notified about. These measures take the form of three distinctive dimensions:

Table 1
The 12 scenarios: Breaches (B1–B4), Consequences (C1–C4) and Tips (T1–T4).

	Breaches
B1.	I want to be notified when my data have been stored for one month longer than what is specified in the privacy policy I have agreed to.
B2.	I want to be notified when my data have been processed for the purposes of assessing my creditworthiness or insurance risk even though these purposes were not specified in the privacy policy.
B3.	I want to be notified when my data have been shared with service companies not covered in the privacy policy I have agreed to.
B4.	I want to be notified when my mhealth service provider has been attacked by an unknown party on the Internet who might have got access to my data.
	Consequences
C1.	I want to be notified if someone with access to my data might possibly learn something about my lifestyle or about latent illnesses I might be suffering from.
C2.	I want to be notified when my mhealth service provider has profiled me for the purpose of sending me advertisements about healthy food, sport products and insurances based on the data I record.
C3.	I want to be notified if someone with access to my location data (GPS) and the location data of other people might possibly learn when we have spent time in the same place, and what type of activities we have been performing there.
C4.	I want to be notified when my data have been transferred across the borders of Europe.
	Tips
T1.	I want to be notified about alternative mhealth service providers that are more privacy friendly than my current one, while providing the same level of service quality and device compatibility.
T2.	I want to be notified about feasible options of what I can do once I stop tracking my health. I want, for example, to be notified about the option to download and/or erase my health data that are currently stored by my mhealth service provider.
T3.	I want to be notified about practical tips to improve my privacy, like to disable location tracking (GPS) to pinpoint my exact position in the building when I'm at home or at work.
T4.	I want to be notified about reading material, tweets and tutorials about how to improve my privacy while using mhealth services.

Request for notification. *Whether* the notification in question will be delivered. In our study, we investigated how strongly respondents preferred to be notified as compared to the dichotomous decisions measured in our previous study [25].
Timing. *When* the notification will be delivered.
Modality. *How* the delivery of the notification will be signalled.

Each dimension is orthogonal to one of 12 *scenarios* (Table 1), which describe fictitious circumstances related to personal data processing. We chose our scenarios such as to span a broad spectrum of comprehensible cases. Using the categorisation established in [25], we subdivide our scenarios into three thematic *categories* with four exemplary scenarios each:

Breaches mirror the specification of GDPR Art. 4 (12). They deal with incidences related to unlawful processing and accidental mishap.
Consequences relate to actual or hypothetical consequences as a result of lawful processing, which is how they differ from Breaches.
Tips are customised recommendations aimed at enabling users to improve their privacy.

3.2. Modelling predisposition

Collecting our participants' predisposition aimed at eliciting possible determinants of notification preferences. Based on the themes deduced in Section 2.3, we chose the following dimensions to model predisposition:

Concern. "I'm concerned that I might lose control of my health data".
Confidence. "I feel confident in using my mobile device for the Internet services I use".
Proficiency. "I'm knowledgeable about Internet technology".
Trust. "I trust my mhealth service provider to keep my health data safe".
Investigation. "I would spend some time per week on investigating how my mhealth provider processed by health data".
Usefulness. "I find it useful to receive notifications about how my mhealth data are processed by my mhealth provider".

The first five items were displayed in random order. For Concern, we did not rely on existing taxonomies, such as IUIPC [34] or MUIPC [35], as their large number of items would have significantly inflated the survey. For Investigation, we sought to elicit to what extent users of mhealth services would actively search for information related to their privacy. We collected Usefulness as the principal measure to address RQ1, and collected its valuation at the very end once the respondents had gone through the survey and could afford an opinion. Investigation differed from the other valuations in that its scale consisted of six discrete time periods that reflected how much time per week respondents would spend on investigating matters related to their privacy ({0, 5, 10, 15, 20, 25} min, 'Depends on the week').

3.3. Measurement

We measured valuations of statements using 6-point Likert-items (Not at all, No, Rather not, Rather yes, Yes, Very much so). We chose an even-numbered scale to avoid capturing indecisiveness [36]. All valuations included an option 'Prefer not to say' to capture abstention and ambiguity [37]. We use a normalised six-point scale (0.0, 0.2, 0.4, 0.6, 0.8, 1.0) to report valuations, which allows for quantitative collations of all three dimensions of notification preferences (Sections 5.3–5.5). Similar to the metric used by Gabriele et al. [38] to model privacy preferences, this quantification provides us with granular measures of individual determinants. Moreover, it allows for unequivocally mapping such determinants to binary settings, i. e. whether, when and how notifications will be sent.

To validate the linearity of our custom scale, we conducted a quantitative study ($n = 10$) that showed that all of our test subjects provided equivalent ratings for statements irrespective of whether they were confronted with a numerical scale or the six corresponding labels. The test subjects provided ratings for each of the scores at least once, and hailed from different age groups (18–72), cultural backgrounds, and levels of education.

Literature on ascertaining opportune moments for delivering notifications observed that messages received later in the evening are considered less disruptive than e. g. those received during office hours [11]. Building on the distinction between immediate, but potentially preoccupied, and postponed but more relaxed times of the day, we chose two timing options, 'At once' and 'Once per day at a specific time', which we coded as 1.0 and 0.0, respectively. We modelled modality as six multiple-choice options: System notification, Vibration, LED, Audio signalling, Pop-up message, and Email. The first four modalities constitute common signalling schemes employed on mobile devices. We added pop-ups and email as complementary means of notification used in interactive apps and as traditional means of messaging, respectively. Each modality was coded as 0.0 for 'no' and 1.0 for 'yes'.

3.4. Evaluation

We employed various statistical methods for analysing our quantitative results. The statistical analyses used to investigate relationships between various determinants reflected in RQ2 were chosen based on the types of data they consisted of. Assuming interval data for all valuations, we report averages as means (μ_{Eng}: English, μ_{Ger}: German, $\hat{\mu}$: overall) instead of medians to take advantage of the bounded range of values. We used Mann–Whitney U-tests to quantify the differences between the two cohorts, which constituted two independent sets of samples. To investigate pair-wise correlations between notification preferences and predisposition, we relied on Spearman rank coefficients. We conducted principal components analyses (PCA) across the 12 scenarios to extract coherent factors pertaining to various determinants (details provided on [39]). We used Cronbach's alpha to quantify the semantic cohesion of constructs based on groups of scenarios.

4. Study design and implementation

Our online survey (Appendix) was specifically designed for users of mobile phones. It collected data about the participants' demographics and usage characteristics, predisposition and notification preferences (Section 4.1).

4.1. Survey structure

We informed participants about the purpose of our study both when they signed up and at the beginning of the actual survey (Appendix A.1).

Demographics and usage characteristics. We collected our participants' gender, age group, and country of residence. We also collected the types of used devices, their usage purpose, the duration they had been using the devices, and with whom they were sharing the data they collected.

Predisposition. We collected our participants' predisposition, perceived usefulness of privacy notifications and their willingness to investigate the processing of their personal data as modelled in Section 3.2.

Notification preferences per scenario. The 12 scenarios (Table 1) were displayed in random order, each consisting of a textual description of how personal data had been or may be processed. For each scenario, we collected the *notification preferences* (see modelling in Section 3.1).

Impact of intervenability. For Breaches (B1–B4) and Consequences (C1–C4), we included an additional valuation of how much the respondents' intervenability affected their notification preferences. To familiarise them with this notion, we provided a succinct description (Appendix A.6).

Abstention. The valuation of the request for notification and the impact of intervenability on this choice (B1–B4, C1–C4), were each complemented by an option called 'I don't know'. For the request for notification, clicking this option opened a secondary panel that asked participants for the reason of their uncertainty (options: 'I don't understand the scenario', 'I can't relate to the scenario', 'I need further details to make a choice', and 'Other'). As regards the impact of intervenability, the secondary list of options read 'I don't understand the question', 'I don't know what it means to intervene in this context', 'I wouldn't know how to intervene', and 'Other'.

Table 2
Demographics, usage characteristics, and willingness to investigate (Investigation) overall ($\hat{n} = 304$) and per cohort ($n_{\text{Eng}} = 154$, $n_{\text{Ger}} = 150$). Figures in percent.

Facet	All	Eng	Ger	Facet	All	Eng	Ger
Age groups:				Sharing (multiple choice):			
18–25	15	18	11	Family*	41	49	34
26–33	24	34	14	Friends*	31	38	23
34–41	26	29	21	Online*	12	16	8
42–49	16	13	21	Coach	5	4	8
50–57	11	5	19	No one	43	38	53
58–65	5	1	7				
66+	3	1	7				
Devices used (mult. choice):				Period of use*:			
Bracelet*	51	61	49	None	12	1	22
Watch*	33	39	27	≤3 mon	10	5	14
Breast belt*	6	2	11	4–11 mon	21	20	21
Headband*	3	1	3	12+ mon	51	73	29
Other	7	5	12	Unspec.	7	0	14
Purpose of use (mult. choice):				Willingness to investigate*:			
Activity*	70	88	57	Not at all	41	47	33
Health	37	40	33	≤5 min	11	13	11
Sleep*	39	53	29	≤10 min	13	12	13
Location*	41	49	39	≤15 min	8	8	7
Motivate*	51	71	38	≤20 min	7	5	9
None*	17	2	33	≤ 25 min	9	5	12
				Depends	11	10	12
				Unspec.	2	0	4

*Significant differences based on Mann–Whitney U-tests ($p < 0.05$).

4.2. Preparation and implementation

Ethical approval and data protection. Ethical approval was obtained for our previous study [25]. As the current study was conducted under similar conditions, the approval applied equally for this study. Data were anonymously collected and processed in compliance with the GDPR. Participating was voluntary and required the participants' consent.

Recruitment. Our eligibility criteria were (1) legal age, (2) being an active or former user of a mhealth device, and (3) being a resident of the EU. We preferred European residents who could relate to their roles as data subjects against the backdrop of the European legislation. Our English-speaking participants ($\mathcal{C}_{\text{Eng}}$) were recruited via Prolific Academic Ltd. We were unable to recruit sufficient participants who fulfilled criterion 2, and hence recruited the German-speaking cohort ($\mathcal{C}_{\text{Ger}}$) via Splendid Research GmbH. As it proved difficult to recruit eligible German-speaking participants who were equally distributed across Austria, Germany and Switzerland in a timely manner, we had to make do with 154 and 150 participants for $\mathcal{C}_{\text{Eng}}$ and $\mathcal{C}_{\text{Ger}}$, respectively. The participants' remuneration complied with the European standard of minimum wages.

Implementation. The two surveys differed only in language. Texts were written in English and then translated independently to German by two of the authors. Differences were discussed until consensus was reached.

We ran three pilot tests that helped detect various inconsistencies. The survey for $\mathcal{C}_{\text{Eng}}$ was published on 2019-05-02. The equivalent for $\mathcal{C}_{\text{Ger}}$ was published between 2019-06-03 and 2019-06-18.

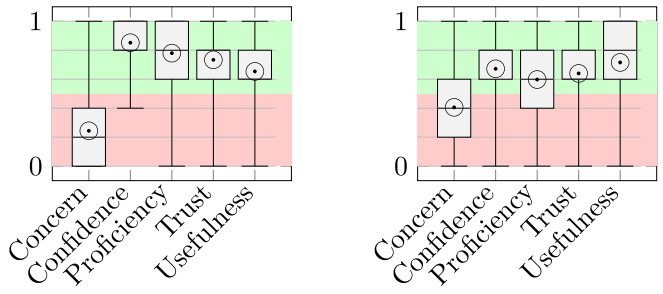
5. Results

Our results are subdivided into groups of possible determinants of notification settings: Section 5.1 reports demographics and usage characteristics. Section 5.2 reports predisposition. Sections 5.3–5.5 reports notification preferences. In Section 5.6, we investigate correlations between notification preferences and various determinants. Section 5.7 reports how intervenability affected the respondents' notification preferences. We finally provide a summary in Section 5.8. All raw data and additional results are available on [39].

We report the results of all valuations as means of the normalised range of the six Likert-items $(0.0, \ldots, 1.0)$ (Section 3.3). Since we aim to model binary notification settings (yes/no), we indicate percentages of the number of positive choices for valuations ('Rather yes', 'Yes', 'Very much so'). We also use percentages to report other dichotomous data, such as timing (now/later), modality (yes/no) and various usage characteristics.

5.1. Demographics and usage characteristics

$\mathcal{C}_{\text{Eng}}$ consisted of 152 participants from the UK and 2 unspecified. 77% were female and 23% male. $\mathcal{C}_{\text{Ger}}$ was almost equally distributed between Austria, Germany, and Switzerland. 51% were female, 47% male, and 2 unspecified. On average, it took both cohorts less than 15 min to complete the survey.



(a) English-speaking cohort (b) German-speaking cohort

Fig. 1. Valuations related to predisposition. '⊙' signifies arithmetic means. Valuation: 0.0: Not at all, 0.2: No, 0.4: Rather not, 0.6: Rather yes, 0.8: Yes, 1.0: Very much so. The colour coding signifies positively ( ) and negatively ( ) attributed choices.

Table 3
Predisposition: **Arithmetic** means (μ), percentages of positive valuations, and U-values (Eng./Ger. cohort).

Valuation	μ_{all}	μ_{Eng}	μ_{Ger}	$\%_{all}$	$\%_{Eng}$	$\%_{Ger}$	U
Concern	0.32	0.24	0.41	24	13	35	7537.50
Confidence	0.76	0.85	0.67	88	96	79	6659.00
Proficiency	0.69	0.78	0.60	81	92	68	6354.00
Trust	0.69	0.73	0.64	83	90	77	8448.00
Usefulness	0.68	0.65	0.72	83	81	86	9136.50

Our participants primarily used fitness bracelets and smart watches. Approximately one third shared their data with family or friends. $\mathcal{C}_{Eng}$ consisted mainly of long-term users (73%) who had been using their devices for at least one year (Table 2). Most were highly active in terms of tracking and used their devices to motivate themselves.

$\mathcal{C}_{Ger}$ was more balanced in terms of age distribution and usage characteristics. They were overall more reserved than $\mathcal{C}_{Eng}$ as regards sharing their data, but twice as many shared their data with medical professionals or coaches (Mann–Whitney test $U = 11230.00$, $p < 0.05$). A higher proportion consisted of users who had started tracking their health only recently. We were surprised to find a relatively large number of non-users in $\mathcal{C}_{Ger}$. Querying our crowd-sourcing provider about the high percentage, Splendid GmbH called this number realistic, as such users could be ex-users who might have lost interest in initially expected benefits, as is further discussed in Section 6.4.

5.2. Predisposition

Fig. 1 shows box plots reflecting the valuations. Table 3 lists the means and the U-values of the Mann–Whitney tests conducted to ascertain differences between the two cohorts. They differed significantly across all five valuations (all $p < 0.01$) in that $\mathcal{C}_{Eng}$ was less concerned and found privacy notifications slightly less useful than $\mathcal{C}_{Ger}$. They were also more confident, perceived themselves as more proficient with IT, and put more trust in the data services that processed their personal data.

Our participants did not want to spend much time on investigating matters related to the processing of their personal data. Almost one half of $\mathcal{C}_{Eng}$ and one third of $\mathcal{C}_{Ger}$ were not willing to spend time on it (Table 2). Another 10% ($\mathcal{C}_{Eng}$) and 16% ($\mathcal{C}_{Ger}$) were either undecided or said it depended on the day. About one third of both cohorts reported that they would spend up to 15 min per week on the matter, leaving roughly twice as many respondents of $\mathcal{C}_{Ger}$ to invest 16–25 min per week.

5.3. Notification request

Overall, our participants preferred notifications for all scenarios (arithmetic means for both cohorts $\hat{\mu}$: 0.51–0.86, 56%–92% positive). We observed differences between the two cohorts on a case-by-case basis, but found similar structural patterns across the scenarios (Fig. 2).

General findings. $\mathcal{C}_{Eng}$ was slightly less interested in receiving notifications about Consequences and Tips, especially about C2, a scenario about profiling for the purpose of receiving advertisements ($U = 10779.00$, $p = 0.47$).

These findings are in line with mhealth users' broad willingness to receive privacy notifications we reported in [25]. The valuation distribution is also similar in that Breaches were rated higher and more uniformly than Tips, whereas Consequences lay in between and showed higher variation.

Preferences per scenario. The distribution of the valuations deviated from the three-fold grouping we had assumed for the scenarios. E.g., C1, categorised as a Consequence related to health-based inferences drawn from a user's data,

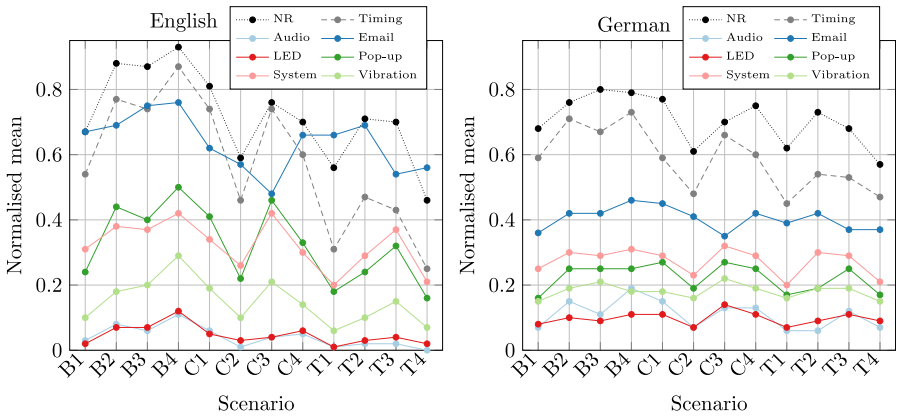


Fig. 2. Notification preferences: Normalised means of the notification request (NR), timing, and modality. The lines connecting the individual preferences per scenario *do not* indicate continuous data, but are drawn only for the purpose of readability.

Table 4
Cronbach's alpha for various clusters of scenarios.

(a) Reference (based on choice to be notified)

Cluster	Scenarios	Overall	English	German
Breaches	B1–B4	0.79	0.66	0.85
Consequences	C1–C4	0.67	0.53	0.77
Tips	T1–T4	0.81	0.75	0.87

(b) High-/low-priority (based on timing preferences)

Cluster	Scenarios	Overall	English	German
High-priority	B2–B4, C1, C3, C4	0.81	0.76	0.84
Low-priority	B1, C2, T1–T4	0.83	0.81	0.83

registered scores similar to those found for most Breaches (B2–B4). B1, actually a Breach notification about the retention period being exceeded, was rated similar to a Consequence or Tip.

To obtain a quantitative measure of the semantic cohesion of the Likert items, we calculated Cronbach's alpha (ρ_τ) for each of the three quadruples constituting the three categories (Table 4a). Whereas the values of $\mathcal{C}_{\text{Ger}}$ indicate satisfactory cohesion ($\rho_\tau \geq 0.77$) for all three categories, the values of $\mathcal{C}_{\text{Eng}}$ indicate weak cohesion. Across both populations, the values were barely acceptable, but the poor cohesion of Consequences was noticeable ($\hat{\rho}_\tau < 0.7$). Hence, the respondents' choices corresponded only partially to the original three-fold categorisation, which we also observed for preferences related to timing and modality (Sections 5.4 and 5.5). Given the current set of scenarios, modelling notification preferences required an adjusted segmentation of the valuations, which we accommodate via a new clustering based on high- or low-priority delivery scenarios (Sections 5.4 and 5.5).

Reasons for uncertainty. Only few ($\leq$3%) members of either cohort abstained from rating their notification request, which we consider non-significant in terms of drawing any conclusions.

5.4. Timing of notification

The *time of delivery* constituted the second determinant related to notification preferences. Timing preferences corresponded largely with the notification request: The more respondents preferred to be notified about individual scenarios the more immediate a delivery was chosen.

General findings. We reconciled the notification request, timing and modality using a normalised scale (Fig. 2). Similar to notification request, the timing preferences varied noticeably across the scenarios. The contextual variation was more pronounced in $\mathcal{C}_{\text{Eng}}$ (μ_{Eng}: 0.25–0.87) than in $\mathcal{C}_{\text{Ger}}$ (μ_{Ger}: 0.45–0.73). Note that the normalised means of notification preferences related to timing and modality include all participants, irrespective of how strongly they prefer to be notified (notification request).

Preferences per scenario. We observed two groups that seemed to reflect high-priority and low-priority scenarios in terms of the immediacy of the delivery. The timings related to three of the Breaches (B2–B4) and the Consequences related to lifestyle and health (C1), spending time in the same place with others who also track their location (C3), and cross-border transfers beyond the borders of Europe (C4) suggested immediate delivery for both cohorts ($\mu_{\text{Eng,Ger}} \geq 0.60$). This subgroup, which had also surfaced for the notification request, denoted scenarios for which immediate delivery was chosen more often than deferral. Except for C1, C3 and C4, $\mathcal{C}_{\text{Eng}}$ tended to postpone notifications about Consequences and

about Tips ($\mu_{\text{Eng}} \leq 0.47$). Conversely, $\mathcal{C}_{\text{Ger}}$'s timing preferences varied less. They chose more often not to respond. In both cohorts, notifications related to profiling for the purpose of receiving customised advertisements (C2) and Tips regarding alternative services (T1, T4) registered the lowest scores.

Certain topics seemed to warrant more consciousness than other scenarios of the same category. For example, notifications received in response to the processing of location data (C3, T2) called for more timely delivery ($\hat{\mu} \geq 0.50$). Conversely, Tips that required either strategical planning or further research on the part of a recipient were postponed more frequently. For example, moving to an alternative service provider (T1) or following up on secondary sources of information (T4) both registered comparatively high counts of postponed delivery ($\hat{\mu} \leq 0.37$). Weber et al. [11] reported similar findings about the choice of users of mobile devices who postponed receiving notifications considered as less urgent to the evening or night.

Due to the relatively weak cohesion of the original segmentation based on the three categories we investigated alternative high-level structures based on our respondents' timing preferences. A principal component analysis (details provided in [39]) of the normalised timing preferences yielded a two-fold clustering of the 12 scenarios. Table 4b shows Cronbach's alpha for the two factors that subdivide the scenarios into what we call high-priority (B2–B4, C1, C3–C4) and low-priority scenarios (B1, C2, T1–T4). The values ($\rho_\tau \geq 0.75$) indicate that the segmentation satisfactorily captures the preferences registered for both cohorts.

5.5. Modality of notification

Modality specified *how* respondents preferred to be notified. Despite differences across the 12 scenarios between the two cohorts for both timing and modality, we found similar structural patterns for these determinants, both of which mirrored the valuations of the notification request (Fig. 2).

General findings. Overall, we registered distinctively different preferences for the six modalities. $\mathcal{C}_{\text{Eng}}$ was selective both in terms of preferring certain modalities over others, and in distinguishing between multiple scenarios. Conversely, $\mathcal{C}_{\text{Ger}}$ selected modalities more uniformly and independently of the scenarios.

Email was selected most frequently (μ_{Eng}: 0.48–0.76, μ_{Ger}: 0.35–0.46), followed by system notifications (μ_{Eng}: 0.21–0.42, μ_{Ger}: 0.20–0.31) and pop-ups (μ_{Eng}: 0.16–0.50, μ_{Eng}: 0.16–0.27) in roughly equal proportions. $\mathcal{C}_{\text{Eng}}$ preferred LED (μ_{Eng}: 0.02–0.07) and audio signalling (μ_{Eng}: 0.00–0.08) except for notifications about attacks from the Internet (B4) ($\mu_{\text{Eng}} = 0.12$).

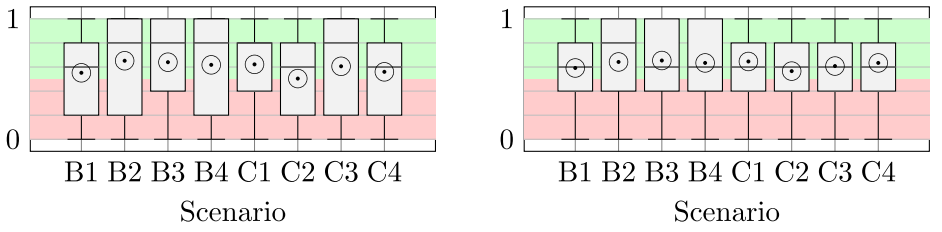
Preferences per scenario. We noticed similar patterns as for the notification request and for timing. B2–B4 and C1 were among the scenarios with the highest number of combined modalities. For both cohorts, scenarios related to spending time with others who track their location (C3) and cross-border transfers beyond Europe (C4) ranked second on the total number of combined modalities. Among them were the highest percentages of modalities that are commonly considered inopportune in daily life, such as audio signals. Conversely, C2, T1 and T4 collected the least total number of combined modalities, including the lowest counts of salient signalling.

This observation is in line with what Micallef et al. [26] reported in that salient privacy nudges were considered appropriate only if the corresponding alarm signalled a decisive event worthy of a recipient's attention. This rationale of severity and immediacy sheds some light on what types of scenarios our participants considered worth being notified about.

As for grouping modalities by scenarios, we confirmed the previous two-fold segmentation for notification request and timing by calculating Cronbach's alpha for high- and low-priority scenarios. We found satisfactory values ($\rho_\tau \geq 0.8$) for all modalities in both cohorts, except for audio signalling in $\mathcal{C}_{\text{Eng}}$ due to the small numbers registered for audio signalling.

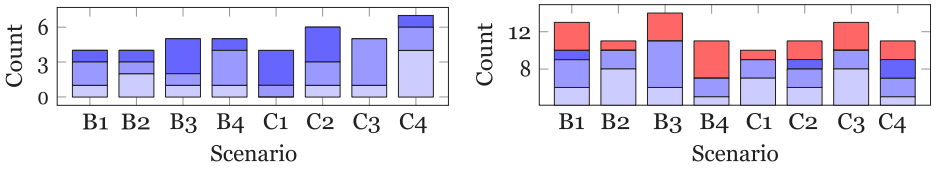
5.6. Correlations and dependencies

To ascertain whether predisposition served as a suitable predictor for their notification preferences, we calculated the Spearman rank correlation coefficients for pair-wise relationships between Concern, Confidence, Proficiency, Trust and Usefulness, and the notification request for each of the 12 scenarios. We found weak correlations (Spearman coefficient $\rho_S < 0.3$) between Concern and individual scenarios. We were able to ascertain that the notification preferences varied slightly depending on various factors related to the demographics and usage characteristics, such as gender and whether the respondents used specific types of devices. However, these effects applied to individual scenarios only, and could not be reproduced across both cohorts. Perceived Usefulness proved to be the only dimension that consistently correlated with all 12 scenarios for $\mathcal{C}_{\text{Ger}}$ and for all but one scenario (C2) for $\mathcal{C}_{\text{Eng}}$ (Bonferroni-corrected $p < 0.01$). The correlations were noticeably stronger for $\mathcal{C}_{\text{Ger}}$ (ρ_S: 0.51–0.73) than they were for $\mathcal{C}_{\text{Eng}}$ (ρ_S: 0.24–0.49). Overall, they indicated mediocre correlation ($\hat{\rho}_S$: 0.32–0.56). In the absence of any other viable determinants, the perceived Usefulness of privacy notifications can thus serve as a weak, if blanket, predictor of how strongly users prefer to be notified.



(a) English-speaking cohort (b) German-speaking cohort

Fig. 3. Impact of intervenability on the notification request. The colour coding signifies positively ( ) and negatively ( ) attributed valuations.



(a) English-speaking cohort (b) German-speaking cohort

Fig. 4. Reasons why respondents abstained from specifying how intervenability affected their notification preferences: Lack of comprehension, Intervenability unclear, Inability to intervene, and other reasons.

5.7. Intervenability

Intervenability was the last studied determinant of notification settings. The valuations of how strongly intervenability affected the notification preferences indicated that this was actually the case (Fig. 3). All Breaches (B1–B4) and Consequences (C1–C4) were rated positively (69% positive), which shows that on average our participants felt that intervenability affected their choice to be notified. This is in line with our previous findings [25].

Reasons for uncertainty. We registered more abstentions regarding the impact of intervenability than for the notification request (Section 5.3). $\mathcal{C}_{\text{Eng}}$ abstained in 2%–5% of the cases, while $\mathcal{C}_{\text{Ger}}$ chose not to answer in 6%–9% of the cases. The two cohorts reported slightly different reasons for their abstentions (Fig. 4). $\mathcal{C}_{\text{Eng}}$ reported their inability to understand the question, the lack of contextual clarity of the term intervenability, and a lack of knowledge of how to intervene in approximately equal amounts. Conversely, $\mathcal{C}_{\text{Ger}}$ hardly reported that they did not know how to intervene. For them, the incomprehensibility of individual scenarios and the concept of intervenability posed greater an issue.

Given the weak, yet noticeable impact of intervenability on the respondents' notification preferences for all Breaches and Consequences, we conclude that intervenability is an important factor for implementing privacy notifications. However, the amount of abstentions suggests that the concept of intervenability should be clarified, and guidance on how users can exercise their legal rights should be provided. We discuss this further in Section 6.2.

5.8. Summary of key results

A majority of participants found notifications useful and the perceived Usefulness correlated with the request for notification. Most preferred immediate delivery. Notification based on email was chosen most frequently followed by system notification and pop-up. In general, participants who preferred to be notified were also more likely to choose immediate delivery, a wide variety of notifications, as well as more salient signalling. Scenarios had a noticeable impact on the decisions of $\mathcal{C}_{\text{Eng}}$. For $\mathcal{C}_{\text{Ger}}$ it was still noticeable for notification request and timing, but not so much for modalities. We found a two-fold segmentation that clusters scenarios into whether respective notifications warrant high- or low-priority delivery. Finally, intervenability had a weak impact on scenarios related to Breaches (B1–B4) and Consequences (C1–C4).

6. Discussion

To address RQ1 and RQ2, we discuss the quantitative evidence of the efficacy of privacy notifications (Section 6.1) and the interplay of the determinants pertaining to notifications preferences (Section 6.2). Further, we discuss the implications our findings have on the design of usable TETs (Section 6.3).

6.1. Efficacy of privacy notifications

The results of how much time our participants were willing to spend on investigating how their personal data have been processed (Investigation) indicate that few members of either cohort were willing to do so. Conversely, the perceived Usefulness of privacy notifications indicated that overall our participants considered it useful to be notified about the 12 scenarios ($\hat{\mu} = 0.68$, 83% positive). Moreover, both cohorts were largely positive about receiving notifications across the full spectrum of all 12 scenarios. As regards the respondents' request for notification, 56%–92% chose positively in terms of whether they preferred to be notified ($\hat{\mu}$: 0.51–0.86).

We thus conclude that for users who try to understand how their personal data have been or might be processed, or who want to learn more about how to improve their privacy, such notifications could serve as a viable means of complementing their effort to investigate matters on their own.

6.2. Determinants of notification settings

Addressing RQ2, the findings (Section 5.8) indicate the following facts:

Inter-cultural commonalities and differences. Our findings on predisposition and usage characteristics are in line with inter-cultural differences of Internet users as highlighted in [17], in which UK citizens feel more in control of the processing of their personal data than citizens from Austria or Germany (p. 35) and more frequently share personal data online (p. 36). Moreover, our finding that $\mathcal{C}_{\text{Eng}}$ was less concerned and found privacy notifications less useful than $\mathcal{C}_{\text{Ger}}$ can be explained by Hofstede's cultural comparison findings [40,41] showing that the UK has a low score on uncertainty avoidance, while the German-speaking countries Germany, Austria and Switzerland are among the countries that avoided uncertainty. Hence, UK citizens are higher risk takers who feel more confident with ambiguity. Conversely, German-speaking countries are cultures that feel more uncomfortable due to ambiguous or unknown situations, and may thus perceive privacy notifications providing awareness and guidance as more useful. This is also in line with the findings by Trepte et al. [20], which show that people from countries ranking high in uncertainty avoidance specifically emphasise the need to avoid privacy risks.

$\mathcal{C}_{\text{Eng}}$ preferred more diverse signalling modality than $\mathcal{C}_{\text{Ger}}$. This suggests that cultural context might serve as a determinant of notification settings. In particular, $\mathcal{C}_{\text{Eng}}$'s higher diversity in terms of preferences in combination with their higher perceived Confidence and Proficiency with IT may indicate a higher interest of that group for changing preference setting. This is in line with [17], in which UK users have to a larger extent tried to change their social network privacy settings than German or Austrian users. However, further research will be required to ascertain whether distinguishing users based on their cultural background persists for different samples.

High- and low-priority delivery. The two-fold segmentation of clustering scenarios based on timing equally reflected our participants' notification preferences in terms of their request for notification and the corresponding modality of signalling. This suggests that in general notification preferences can be captured by two profiles that bundle respective settings. The fact that all scenarios related to Tips belonged to the low-priority segment makes non-committal recommendation the principal candidate for low-priority delivery. The same goes for scenarios that do not require immediate attention, which suggests deferred signalling using non-salient modalities. Conversely, the high-priority profile would capture scenarios that require immediate response, such as most Breaches and profiling based on mhealth data, using salient signalling to raise immediate awareness.

Timing. Due to the general preference for immediate delivery of privacy notifications, messages should only be deferred in cases when prompt decision-making is not of the essence, such as for scenarios that can unequivocally be classified as low-priority.

Modality. The high demand for email notification is particularly noticeable because our participants were mainly tech-savvy young adults who were confident in using their mobile phones. The reason why email was frequently selected individually as well as in addition to other modalities could have been that email clients constituted a convenient means of archiving incoming messages compared to the more volatile nature of other types of notifications. System notifications and email could have been special in that, depending on the configuration of a device, forwarding such messages to the notification centre or email client may trigger secondary signalling. This may have been the reason why whenever either of these two modalities was selected, audio, LED and vibration were rarely selected too. Pop-up messages, which are usually not employed as part of signalling mechanisms, were more often selected complementarily.

Intervenability. The fact that intervenability affected our participants' request for notification suggests that they realised a connection between obtaining awareness about personal data processing and making follow-up decisions or taking action in response. This means that designers of TETs may want to cater to this expectation by featuring respective options in the course of facilitating transparency.

6.3. Implications for the design of TETs

Drawing on our findings, on legal requirements and on findings from the literature, we infer the following qualitative guidelines regarding the design of usable ex post TETs employed in fitness tracking scenarios:

Default settings. The positively attributed valuations of our participants' request for notification across all 12 scenarios indicate that the default practice of a TET should be to send the privacy notification in question. To avoid spamming users with notifications they may not be interested in, receiving Tips would be optional. This would implement default-on/opt-out, which is in line with the Data Protection by Default principle stipulated in GDPR Art. 25. All notifications should be delivered immediately via email.

Selectable profiles. Selectable bundles of settings could consist of profiles that represent either high- or low-priority scenarios. Notifications classified as high-priority might, for example, be delivered immediately, whereas the delivery of low-priority scenarios, e. g. Tips, could be postponed until the evening. As our results show that scenario-specific differences existed for modalities (emails, pop-ups, and system notifications) among $\mathcal{C}_{\text{Eng}}$ but hardly for $\mathcal{C}_{\text{Ger}}$, culture-specific profiles should further be considered. As vibration, audio and LED were hardly chosen as signalling modalities, they should per default not be included in profiles.

Fine-grained customisation. The diversity of the responses of $\mathcal{C}_{\text{Eng}}$ in contrast to $\mathcal{C}_{\text{Ger}}$ suggests that there are cultural differences in regard to how far users benefit from fine-grained customisation. TETs might therefore enquire users about their future plans when the TET is first put into operation, and suggest further customisations 'on the fly' once a change of the user's usage pattern is detected [27,42]. Approaches based on machine learning, such as suggested by Liu et al. [13], might accommodate initial preferences and culture-specific profiles, recommending adaptive changes towards different profiles depending on a user's behavioural pattern. With a machine-learning-based customisation based on culture-specific profiles, users with different cultural backgrounds may be guided differently to change to suitable culture-based profiles while using the system.

Archiving. Since email was the predominant modality across all scenarios, we hypothesise that our participants considered privacy notifications important enough to warrant post processing and archiving. The notion of storing messages is congruent with what Murmann designates a means of 'preventing user errors' [27], such as when a notification is accidentally dismissed, or when users want to refer back to messages at a later time.

Guidance. Intelligible facts will be required to facilitate transparency and to enable data subjects to make informed decisions [43]. A considerable proportion of the respondents did not specify how intervenability affected their request for notification. Hence, brief descriptions may not suffice to clarify the potential consequences of taking action in response to receiving notifications. TETs should therefore not only point out facts but also provide suitable secondary clarification on request. Customised guidance will help accommodate the needs of users with different backgrounds and levels of knowledge. To avoid imposing unnecessary cognitive load on users, secondary information could be implemented as multilayered information [44].

Intervenability. TETs have the potential to guide users in exercising their right of intervenability. However, our findings indicate that the concept of intervenability and the options it entails are not common knowledge. Moreover, a recent Eurobarometer survey [17] showed that about one third of EU citizens are not familiar with their legal rights stipulated by the GDPR. In addition to providing clarity about the facts of how personal data have been or will be processed, TETs may therefore provide users with actionable choices that enable them to make follow-up decisions based on the information at their disposal [45,46]. Receiving customised advice about suitable options, the follow-up steps required, and the consequences that will arise when taken, may enable users to weigh up individual options against each other [47]. Respective advice may also provide the insight necessary to weigh up these options against not to act at all.

Data protection by design and default. It is worth mentioning that personal information conveyed by privacy notifications needs to be protected in compliance with Art. 25 GDPR. This means that personalised privacy notifications related to sensitive medical data (such as "XYZ could learn that you have a high risk of diabetes…") should, at least per default, not be conveyed via pop-ups or audio messages. Users may not have full control over who else in their proximity might learn about such facts. Such messages should instead be framed in general terms (such as "XYZ could profile your health status. More details can be retrieved here…") and provide a link or button to secondary information. This motivates a multilayered design that facilitates transparency by revealing details on request [44].

6.4. Limitations

Demographics. $\mathcal{C}_{\text{Eng}}$ was largely comprised of middle-aged females from the UK (Table 2) because Prolific [48] supplied participants independently of gender or age on a first-come, first-served basis.

Impact of German-speaking non-users. The considerable amount of non-users of $\mathcal{C}_{\text{Ger}}$ (Section 5.1) raised the question as to what impact this group had on the conclusions we draw. Removing this group from the data set changed individual valuations related to predisposition and intervenability. After removing this group, the percentage of positive answers increased for Confidence (80% to 92%), Proficiency (69% to 78%), Trust (77% to 85%), Usefulness (86% to 91%), and for intervenability (69%–75%). However, we found no significant difference regarding Concern (34% vs 36% positive), the request for notification (83% vs 79%), and Timing (58% vs 59%). For modality, the average absolute difference was just 2%, and would not change the general results or our interpretations.

It is an open question as to whether non-users are part of the cultural difference or a selection bias on the part of Splendid Research GmbH. However in summary, while some of the results change depending on the underlying data set, the conclusions of our discussion stay valid in both cases.

Request for notification. Our two surveys outlined theoretical events that did not reflect actual choices that users made and adapted over time. This means that our participants' request for notification may have been slightly higher than

in real-world scenarios, especially for notifications such as Tips. Future field studies might capture longitudinal aspects of decision-making by analysing the actual choices users make in response to receiving privacy notifications. This may yield insights of whether and how users' notification preferences change over time.

Normalisation. Reconciling the request for notification, timing and modality by normalising their range of values may seem arbitrary. The same could be said about our choice to assign discrete values to the two timing states, i. e. treating deferred delivery as 0 and immediate delivery as 1, respectively. However, alternative forms of discretisation might also be questioned. The purpose of normalising the measurements is not to compare the absolute values of the three types of determinants between each other, as each is based on a different type of measurement. The normalisation enables us to investigate the three different kinds of measurements/determinants across multiple scenarios. Our discussion of the difference of individual values across scenarios would also apply for other scales as long as such scales reflect interval data.

7. Conclusion

The results of our study provide quantitative evidence that determinants exist for customising privacy notifications. The determinants surface in the form of cultural context, demographics and predisposition, and in that the participants' right to intervene in the processing of their personal data affect their choice to be notified. Moreover, the results indicate that the participants of two online surveys appreciated receiving privacy notifications to help them improve their privacy. Analysing when, how, and what scenarios they preferred to be notified about provides us not only with insight about their notification preferences, but also yields a two-fold segmentation that subdivides scenarios into high- and low-priority notifications.

Based on the elicitation of the respondents' notification preferences, we are able to infer a series of design guidelines for usable TETs that facilitate transparency by harnessing privacy notifications. Our research was conducted in the usage context of fitness tracking. As people perceive health data as more sensitive than other types of data [49], our results on notification preferences may differ from other application areas. Nonetheless, we found that determinants for privacy notification settings exist for a specific context, which leads us to believe that such determinants can also be found for different contexts. Further research will be required to verify to what extent preferences for privacy notifications apply in general, or how they differ from application contexts other than fitness tracking.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was funded by EU H2020 under the Marie Skłodowska-Curie grant No 67573, and CyberSec4Europe grant No 830929.

Appendix. Transcript of the online survey

This appendix contains a transcript of the English version of the online survey. Notice that Appendix A.7 shows only one out of 12 exemplary scenarios. The other 11 scenarios were displayed identically and were based on the statements shown in Table 1. Only scenarios B1–B4 and C1–C4 contained the part related to intervenability. The 13th scenario mentioned in the introductory part of Appendix A.6 was an attention test, which we used to screen our participants.

A.1. Survey on fitness tracking & mobile health

Thank you for participating in our survey on fitness tracking, mobile health (mhealth), and the processing of mhealth data. The survey is conducted by Karlstad University, Sweden, in cooperation with Georg-August University Göttingen, Germany. Taking the survey will take approximately 12 min of your time.

Participating in this study is voluntary. You can drop out of this survey at any time, in which case all data you have entered will be deleted. You must be at least 18 years old to participate.

The following types of data will be processed for the purpose of scientific research:

- Your demographics
- Your usage of mhealth devices
- Your preference regarding notifications of how your mhealth data are processed
- The date and time of your participation

□ I accept the privacy policy of this study and I want to participate

A.2. Background of this survey

You have been invited to this survey because you either

- Own a fitness tracker/mhealth device, like a smart watch or fitness bracelet,
- Have hands-on experience with such devices, or
- Are generally interested in such devices.

We will not test your knowledge on mhealth. Instead, we will ask you to reflect on how your mhealth data are processed by your mhealth service provider.

The study consists of four parts:

- We will ask you about your demographics.
- We will ask you about how you use your mhealth device.
- We will ask you about your opinion on IT and Internet services.
- We will ask you to read through 13 hypothetical scenarios related to mhealth and tell us whether and how you would like to be notified about them, if you were to find yourself in the circumstances described in the text.

A.3. Demographics

Where do you live? [options: Prefer not to say, List of countries]
Gender [options: Prefer not to say, Female, Male, Other]
Age group [options: Prefer not to say, 18–25, 26–33, 34–41, 42–49, 50–57, 58–65, 66+]

A.4. Why and how do you use your mhealth device?

What kind of device do you use? (multiple choice possible)
[options: □ Fitness bracelet, □ Smart watch, □ Breast belt, □ Headband, □ Other, □ None, I don't use a mhealth device]
What do you use your device for? (multiple choice possible)
[options: □ Keep track of my activities, □ Keep track of my health, □ Keep track of my sleeping behaviour, □ Keep track of the routes and distances I cover, □ Motivate me to exercise and move, □ I don't use any devices right now/yet/anymore]
For how long have you been using your device? [Prefer not to say, Up to 3 months, 4–11 months, 12+ months, Not used (yet/anymore)]
With whom do you share your data? (multiple choice possible)
[options: □ Family or relatives, □ Friends or acquaintances, □ Online social networks or open data platforms, □ Medical professionals or coaches, □ No one]

A.5. Your opinion on IT and internet services

I'm concerned that I might lose control of my health data.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ Prefer not to say]
I feel confident in using my mobile device for the Internet services I use.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ Prefer not to say]
I'm knowledgable about Internet technology.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ Prefer not to say]
I trust my mhealth service provider to keep my health data safe.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ Prefer not to say]
I would spend some time per week on investigating how my mhealth provider processed by health data.
[options: ◯ I wouldn't spend any time on that, ◯ Up to 5 min, ◯ Up to 10 min, ◯ Up to 15 min, ◯ Up to 20 min, ◯ Up to 25 min, ◯ Depends on the week, ◯ Prefer not to say]

A.6. Scenarios

On the next 13 screens, we will show you hypothetical scenarios related to how the mhealth data you record are processed by your online mhealth service provider, such as Apple, FitBit or Google Fit. Imagine you could receive notifications on your smartphone if the events described in the scenarios actually took place. Please indicate how likely it is that you would want to receive such notifications under the respective circumstances. If you cannot decide, you can choose the option "I don't know". In this case, please indicate the reason why you hesitate.

Note that in Europe you have the legal right to *intervene* against how your personal data are processed. We would like you to indicate to what extent having this right makes any difference for you as far as your choice about receiving notifications is concerned.

For your reference:

- A *privacy policy* is the document that lays down the terms and conditions about how your personal data are processed.
- Your right to *intervene* against the processing of your personal data means that you can challenge how your mhealth service processes your data.

A.7. Scenario x/13

I want to be notified when my data have been stored for one month longer than what is specified in the privacy policy I have agreed to.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ I don't know]
My ability to intervene against the processing of my data affects my choice to be notified.
[options: ◯ Not at all, ◯ No, ◯ Rather not, ◯ Rather yes, ◯ Yes, ◯ Very much so, ◯ I don't know]
When would you like to receive the above notification?
[options: ◯ At once, ◯ Once per day at a specific time, ◯ Prefer not to say]
I want to be notified about the above circumstances via… (multiple choice possible)
[options: □ Standard system notification, □ Vibration, □ LED, □ Audio signal, □ Pop-up message, □ Email, □ Prefer not to say]

References

[1] Tractica, Fitness tracker device unit shipments worldwide from 2016 to 2022 (in millions), 2019, https://www.statista.com/statistics/610390/ (accessed 11/2020).
[2] Tractica, Wearables (penetration, users by age, users by gender, users by income), 2019, https://www.statista.com/outlook/319/137/wearables/germany (accessed 11/2020).
[3] D. Lupton, Quantifying the body: Monitoring and measuring health in the age of mhealth technologies, Crit. Public Health 23 (4) (2013).
[4] ENISA, Risks and benefits of emerging life-logging applications, 2011, https://www.enisa.europa.eu/publications/to-log-or-not-to-log-risks-and-benefits-of-emerging-life-logging-applications (accessed 06/2021).
[5] G. Wolf, Know thyself: Tracking every facet of life, from sleep to mood to pain, Wired Mag. 365 (2009).
[6] The European Parliament and the Council of the EU, Regulation (EU) 2016/679 of the European parliament and of the council, 2016.
[7] M. Hildebrandt, Behavioural Biometric Profiling and Transparency Enhancing Tools, D7.12, FIDIS, 2009.
[8] M. Hansen, Top 10 mistakes in system design from a privacy perspective and privacy protection goals, in: IFIP PrimeLife Int. Summer School on Privacy & Identity Management for Life, Springer, 2012.
[9] B. Lowens, et al., Wearable privacy: Skeletons in the data closet, in: Proc. of the IEEE Int. Conf. on Healthcare Informatics, 2017.
[10] M. Pielot, B. Cardoso, K. Katevas, J. Serrà, A. Matic, N. Oliver, Beyond interruptibility: Predicting opportune moments to engage mobile phone users, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1 (3) (2017).
[11] D. Weber, A. Voit, J. Auda, S. Schneegass, N. Henze, Snooze! investigating the user-defined deferral of mobile notifications, in: Proc. of the ACM Int. Conf. on HCI with Mobile Devices and Services, 2018.
[12] C.B. Jackson, Y. Wang, Addressing the privacy paradox through personalized privacy notifications, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2 (2) (2018).
[13] B. Liu, M.S. Andersen, F. Schaub, H. Almuhimedi, S.A. Zhang, N. Sadeh, Y. Agarwal, A. Acquisti, Follow my recommendations: A personalized privacy assistant for mobile app permissions, in: Proc. of the Symposium on Usable Privacy and Security, 2016.
[14] P. Murmann, S. Fischer-Hübner, Tools for achieving usable ex post transparency: A survey, IEEE Access 5 (2017).
[15] EU Commission, Special Eurobarometer 431 – Data Protection, Technical Report, 2015.
[16] R. Lunheim, G. Sindre, Privacy and computing: a cultural perspective, in: Proceedings of the IFIP TC9/WG9. 6 Working Conf. on Security and Control of Information Technology in Society, 1993.
[17] E. Commission, Special Eurobarometer 487a – The General Data Protection Regulation, Technical Report, 2019.
[18] K.P. Coopamootoo, Usage patterns of privacy-enhancing technologies, in: Proceedings of the 2020 ACM SIGSAC Conf. on Computer and Communications Security, 2020.
[19] T. Soffer, A. Cohen, Privacy perception of adolescents in a digital world, Bull. Sci. Technol. Soc. 34 (5–6) (2014).
[20] S. Trepte, L. Reinecke, N.B.e.a. Ellison, A Cross-Cultural Perspective on the Privacy Calculus, Vol. 3, Social Media+ Society, 2017.
[21] F. Schaub, R. Balebako, A.L. Durity, L.F. Cranor, A design space for effective privacy notices, in: Proc. of the Symposium on Usable Privacy and Security, 2015.
[22] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L.F. Cranor, Y. Agarwal, Your location has been shared 5, 398 times! a field study on mobile app privacy nudging, in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2015.
[23] G. Hsieh, K. Tang, W. Low, J. Hong, Field deployment of IMBuddy: A study of privacy control and feedback mechanisms for contextual im, in: Proc. of the Int. Conf. on UbiComp, 2007.
[24] D. Wu, G. Moody, J. Zhang, P. Lowry, Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention, Inf. Manag. 57 (5) (2020).
[25] P. Murmann, D. Reinhardt, S. Fischer-Hübner, To be, or not to be notified – eliciting privacy notification preferences for online mhealth services, in: Proc. of the Int. Conf. on Information Security and Privacy Protection, 2019.
[26] N. Micallef, M. Just, et al., Stop annoying me!: an empirical investigation of the usability of app privacy notifications, in: Proc. of the ACM Australian Conf. on Computer-Human Interaction, 2017.
[27] P. Murmann, Eliciting design guidelines for privacy notifications in mhealth environments, Int. J. Mob. Hum. Comput. Interact. 11 (4) (2019).
[28] B. Liu, J. Lin, N. Sadeh, Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?, in: Proc. of the Int. Conf. on World Wide Web, 2014.
[29] J. Lin, B. Liu, N. Sadeh, J.I. Hong, Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings, in: Proc. of the Symposium on Usable Privacy and Security, 2014.
[30] P. Wijesekera, J. Reardon, I. Reyes, et al., Contextualizing privacy decisions for better prediction (and protection), in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2018.

[31] D. Votipka, S. Rabin, K. Micinski, et al., User comfort with android background resource accesses in different contexts, in: Proc. of the Symposium on Usable Privacy and Security, 2018.
[32] J. Dupree, R. Devries, et al., Privacy personas: Clustering users via attitudes and behaviors toward security practices, in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2016.
[33] A. Morton, M. Sasse, Desperately seeking assurances: Segmenting users by their information-seeking preferences, in: Proc. of the IEEE Annual Int. Conf. on Privacy, Security and Trust, 2014.
[34] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, Inf. Syst. Res. 15 (4) (2004).
[35] H. Xu, S. Gupta, M.B. Rosson, J. Carroll, Measuring mobile users' concerns for information privacy, in: Proc. of the int. conf. on information systems, 2012.
[36] R. Armstrong, The midpoint on a five-point likert-type scale, Percept. Motor Skills 64 (2) (1987).
[37] J. Brown, What issues affect likert-scale questionnaire formats, Shiken: JALT Test. Eval. SIG Newsl. 4 (1) (2000).
[38] S. Gabriele, S. Chiasson, Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours, in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2020.
[39] Supplementary material, 2020, https://ekkaia.org/kau/np19.
[40] G. Hofstede, G.-J. Hofstede, Lokales Denken, Globales Handeln: Interkulturelle Zusammenarbeit Und Globales Management, Deutscher Taschenbuch Verlag, 2006.
[41] Hofstede insights, 2021, https://www.hofstede-insights.com/country-comparison/austria,germany,switzerland,the-uk/, (accessed 06/2021).
[42] J. Angulo, S. Fischer-Hübner, E. Wästlund, T. Pulls, Towards usable privacy policy display and management, Inf. Manag. Comput. Secur. 20 (1) (2012).
[43] F. Schaub, R. Balebako, L.F. Cranor, Designing effective privacy notices and controls, IEEE Internet Comput. 21 (3) (2017).
[44] Art. 29 Data Protection Working Party, Guidelines on transparency under regulation 2016/679, WP260 rev.01, 2018.
[45] S. Egelman, L.F. Cranor, J. Hong, You've been warned: An empirical study of the effectiveness of web browser phishing warnings, in: Proc. of the ACM Conf. on Human Factors in Computing Systems, 2008.
[46] S. Patil, R. Hoyle, R. Schlegel, et al., Interrupt now or inform later? Comparing immediate and delayed privacy feedback, in: Proc. of the acm conf. on human factors in computing systems, 2015.
[47] C. Bravo-Lillo, L.F. Cranor, J. Downs, S. Komanduri, Bridging the gap in computer security warnings: A mental model approach, IEEE Secur. Priv. 9 (2) (2011).
[48] Prolific Academic Ltd., Participant pool demographics, 2019, https://www.prolific.co/demographics (accessed 11/2019).
[49] E.-M. Schomakers, C. Lidynia, D. Müllmann, M. Ziefle, Internet users' perceptions of information sensitivity – insights from Germany, Int. J. Inf. Manag. 46 (2019).