# Understanding Fitness Tracker Users' and Non-Users' Requirements for Interactive and Transparent Privacy Information

Sabine Theis
German Aerospace Center (DLR),
Institute for Software Technology
51147 Cologne, Germany
sabine.theis@dlr.de

Carolin Stellmacher
University of Bremen,
Human-Computer Interaction
28359 Bremen, Germany
cstellma@uni-bremen.de

Sebastian Pütz
RWTH Aachen University,
Institute of Industrial Engineering
and Ergonomics
52062 Aachen, Germany
s.puetz@iaw.rwth-aachen.de

Matthias Georg Arend
RWTH Aachen University,
Institute of Industrial Engineering
and Ergonomics
52062 Aachen, Germany
m.arend@iaw.rwth-aachen.de

Verena Nitsch
RWTH Aachen University,
Institute of Industrial Engineering
and Ergonomics
52062 Aachen, Germany
v.nitsch@iaw.rwth-aachen.de

## ABSTRACT

While fitness tracker users consent to the processing of their sensitive data based on privacy policies, previous research has demonstrated that legal texts often remain unread or incomprehensible. This questions whether the given consent is indeed informed. While past research concentrated on improving privacy comprehension, our research aims to better understand user requirements for interactive and transparent privacy information and control systems. We mainly focus on users' assessment of contextual and functional aspects. Findings from an online survey with fitness tracker users and non-users ($N = 204$) reveal that such systems need to support users and potential users throughout the usage life cycle, illustrating a dynamic change in requirements and their prioritization of information transparency and privacy control. Design recommendations derived from our results support the development of interactive and comprehensible privacy systems that enable more knowledgeable decisions on sharing and processing fitness tracker data.

## CCS CONCEPTS

• **Human-centered computing** → *Visualization application domains*; • **Security and privacy** → **Human and societal aspects of security and privacy**.

## KEYWORDS

Privacy information, privacy choice, interactive visualization, user requirements, fitness tracker

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
*CHI EA '23, April 23–28, 2023, Hamburg, Germany*
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3585698

**ACM Reference Format:**
Sabine Theis, Carolin Stellmacher, Sebastian Pütz, Matthias Georg Arend, and Verena Nitsch. 2023. Understanding Fitness Tracker Users' and Non-Users' Requirements for Interactive and Transparent Privacy Information. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3544549.3585698

## 1 INTRODUCTION

During the past decade, wearable technologies have become an integral part of people's everyday lives. For many, daily health activity tracking using fitness trackers is standard practice and is even gaining traction in professional health contexts. Large amounts of sensitive data are collected while the user's main attention is on an activity detached from the active operation of a computer, making data collection less salient to the user and, hence, less of a user focus [8]. However, like many data-collection technologies, fitness trackers – considered wrist-worn wearable devices collecting fitness data accessible via original vendor apps (e.g., Garmin, Apple, or Fitbit) – require users' consent for acquiring, storing, converting, or sharing data. To this end, technology providers strive to comply with legal frameworks such as the General Data Protection Regulation (GDPR) by obtaining user consent to corresponding textual privacy policies. That said, it remains questionable to which extent frequent consent requests and the comprehensibility of such textual privacy statements lead to an informed decision, with research highlighting that users are often unaware of the data practices [13]. Previous research has demonstrated extensively that these legal texts often remain unread due to their length, complexity, and readability, while users still provide the requested consent [20, 26, 37, 40, 44]. In addition, these textual statements rarely provide individual privacy choices [2]. In practice, decoupled from the initial privacy notice, few privacy controls are available inside the account settings. However, dark patterns [16] and common usability errors such as non-privacy-related labels often make privacy settings even more difficult to find, and understand [18], or users are unaware of the related security risks [24], underlying today's user challenges

to control their data [4]. This issue is further exacerbated by fitness tracker users forgetting their privacy settings or having inaccurate mental models of corresponding processes [48] and how fitness tracker ecosystems work [43]. A large body of research has been dedicated to addressing these limitations and increasing the digital sovereignty and self-determination of the individual. A substantial portion focused on designing better comprehensible privacy statements, showing that higher visibility of privacy information alone could improve decision-making [42]. Various strategies that differed in interactivity, application of textual format, and visualizations were explored. A common approach is shortening or breaking textual privacy information into smaller chunks to enhance transparency, such as multi-level policies with short, condensed, or complete textual representations [31]. Short text snippets were also utilized as contextual privacy notices embedded with the affiliated software feature [10, 30, 46]. However, work performed in the context of fitness trackers also showed that removing familiar privacy practices from statements to reduce the amount of information and to sharpen the focus does not always lead to higher awareness for the remaining privacy information [14]. Instead, icons as visual aid were able to better highlight the presence of privacy choices [19], or by helping users to compare their preferences with vendors' policies [5], even in combination with textual elements [9]. Moving away from the textual format, other authors explored a standardized table layout, similar to nutrition labels, allowing users to find relevant information faster and more accurate [22, 23]. More playful strategies encompass a mobile escape room game to improve understanding [38] or a comic-based policy to increase user attention [41]. However, designing privacy systems that allow users to adapt privacy choices to their individual needs has received less attention, despite the meaningful effect on users' privacy awareness, leading to less information disclosure [25]. To facilitate higher control over user data, a few studies investigated interactive systems and user requirements for managing privacy choices. Past work identified design recommendations to increase awareness, control, and deployment of contextual privacy choices [13]. Other previously derived guidelines show that privacy systems should prevent information overload, allow direct control, use accessible language, and allow comparisons between privacy policies [34]. Based on their results, the authors designed a standardized table layout integrating privacy information with embedded additional user interface (UI) elements such as help icons and toggle buttons, significantly reducing the time spent by users compared to the textual privacy policy. Regarding the design specifics for providing privacy choices, type, functionality, timing, channel, or modality should be considered during the design process [11]. Although some approaches were explored, the established user requirements often remain limited to general concepts, isolate privacy choices from the related privacy information, or do not consider potential new users. Thus, a deeper understanding of the usage context of this novel interactive and transparent technology is required. Using the potential of interactive visualizations to facilitate privacy control and enable users to make an informed decision about their fitness tracker data requires the initial understanding of user needs [28] and characteristics.

In the following, we aim to understand the usage context for privacy decisions embedded into privacy systems and relevant software functionalities. With this work, we contribute a first outline of user requirements for researchers and practitioners to develop interactive and transparent privacy systems. The present survey represents the first of a series of user research activities from which we aim to derive requirements.

## 2 METHODS

To better understand users' requirements for interactive and transparent privacy systems, we conducted an online survey. The following reports on our sample and the design of the questionnaire.

### 2.1 Sample

Participants were recruited from September 30th to November 9th, 2020, in Germany via online channels of the project partners (Chair of Software Engineering, Institute of Industrial Engineering and Ergonomics, and Institute of Applied Ethics at RWTH Aachen University; the research group Human-Computer Interaction at the University of Bremen; the Privacy and Security in Information Systems group at the University of Bamberg; the Digital Opportunities Foundation; the German Informatics Society), including website announcements, newsletters, and Twitter. This resulted in $N = 204$ responses, including 149 complete and 55 partial responses. Partial response means that the analyses for individual user requirements are based on all responses received for the respective questionnaire item, including responses from participants who did not provide an answer to other items. We consider this reasonable since the requirement items are – other than the ones from standardized questionnaires – conceptually distinct. The age of the participants ranged from 18 to 82 years, with a mean ($M$) of 39.47 years and a standard deviation ($SD$) of 16.65 years ($n = 149$). Of the 145 participants that disclosed their gender, 44% identified as female, 56% as male, and none as non-binary. 29% ($n = 59$) of the sample were users of fitness trackers at the time of the survey.

### 2.2 Questionnaire

The questionnaire was implemented in the online survey tool Unipark and consisted of two parts. The first part included questions focusing on participants' current behavior concerning privacy policies, the disclosure of their personal data, and their information needs for making decisions on fitness tracker usage. The second part included psychometric scales to assess relevant characteristics of the participants that are expected to affect their attitudes and actions in this context. This article focuses on questions addressing user needs and requirements for the central areas of user interaction with privacy information. Items that question these topics are included in the first part of the questionnaire. These include (a) the *use cases* in which users would like to receive privacy information, (b) the accepted *time* users are willing to spend on controlling their privacy settings, (c) which *devices* they want to use for receiving privacy information and controlling privacy settings, (d) which *representations* they prefer for receiving privacy information, and (e) the *functions* users require for improving the understanding and control of their data (items are provided in the supplemental materials). The second part of the questionnaire contained items

assessing the affinity for technology interaction (ATI) [12] and the mobile users' information privacy concerns (MUIPC) [47] scales. The ATI theory is based on the *need for cognition* construct [6] and models a human's tendency to actively engage in technology interactions as a critical personal resource. Therefore, individuals with higher ATI are expected to cope more easily with difficulties in interacting with technical systems, facilitating the adaptation of new technologies. The MUIPC construct builds on central theoretical work in the domain of privacy attitudes, including the *Concern for Information Privacy Model* [36] and the *Internet Users' Information Privacy Concerns Model* [27], and transfers them to the application domain of mobile devices. To our knowledge, there was no validated German version of the nine-level MUIPC scale developed by Xu and colleagues [47], so we created a translated version of the English original (see supplementary materials). To ensure translation quality, three independent translators produced parallel translations, see [17], which were then compared and merged by a team of two subject matter experts with German and English as their native languages, respectively.

## 3 RESULTS

Our work aimed to identify users' needs and requirements for tools that seek to provide comprehensible privacy information, as well as support users in efficiently controlling their data by adapting privacy settings. Since the scope of the presented analyses was descriptive and not confirmatory, mostly confidence intervals (CIs) are reported.

### 3.1 User Group

To identify the needs and requirements of specific user groups, the user characteristics were analyzed concerning fitness tracker usage, ATI, and MUIPC. As outlined in the Method section, the user group consisted of $n = 55$ participants who have used a fitness tracker at the time of data collection, and $n = 134$ participants who have not ($n = 15$ participants did not make an indication). To account for differences in behavioral variables between the two major groups, non-parametric permutation tests (accounting for the vastly different group sizes) were performed. Participants' values on the MUIPC scale were, on average higher than the mid-point of the 7-point-Likert scale ($M = 5.50$), with small and non-significant mean/median differences in the fitness tracker user ($M = 5.26$) and non-user group ($M = 5.59$; $Z = 1.38$; $p = .167$). Similarly, the ATI-scale values were slightly higher than the scale mid-point in the complete sample ($M = 3.98$). Again, there were no considerable differences between the fitness tracker user group ($M = 3.91$) and the non-user group ($M = 4.12$; $Z = -1.00$; $p = .324$). Hence, the sample was reasonably representative (e.g., in terms of the means of ATI) [12].

### 3.2 Use Cases

The first question was during which *usage phases* enhanced data privacy information would be required (see Fig. 1 for the selection of usage phases). In the fitness tracker non-user group ($n = 114$), all phases were approximately rated as equally important (see Figure 1), including phases before device ownership (e.g., during purchase decisions). In contrast, fitness tracker users ($n = 44$) had a preference for usage situations in which they already owned the device (i.e., for device setup, during usage, and for updates).

### 3.3 Time for Privacy Settings

We wanted to assess how much *time* users perceived as acceptable for adapting their privacy settings to their individual and specific needs. The participants willing to spend more than 60 minutes adjusting their privacy settings were only non-users (see Figure 1). This user group, on average, also indicated being willing to spend more time ($M = 27.99min$) than users ($M = 20.82min$). Yet, this mean difference was not significant ($Z = 0.90$; $p = .370$; as indicated by a permutation test), which is why further interpretation is based on the complete sample. As depicted in Figure 1, the majority of the $N = 204$ participants who responded to the question would accept spending approximately 10 minutes adapting their privacy settings (46.20%). Yet, a substantial share of participants was willing to spend 15 to 30 minutes (36.71%) and even 35 to 60 minutes (13.92%). Furthermore, this variable correlated positively with an affinity for technology interaction (Spearman rho correlation coefficient; $\rho = .19$; $p = .019$) and users' privacy concerns ($\rho = .18$; $p = .026$), although both correlations had small effect sizes.

### 3.4 Devices for Information and Control

Users were asked which *devices* they would like to use to receive information and exert control over their data. For fitness tracker users, the order of most frequently indicated devices was smartphone (86.36%; 95%$CI$ = 72.65% − 94.82%), notebook (65.91%; 95%$CI$ = 50.08% − 79.51%), tablet (40.91%; 95%$CI$ = 26.34% − 56.75%), and smartwatch (29.54%; 95%$CI$ = 16.76% − 45.20%) or desktop computer (29.54%; 95%$CI$ = 16.76% − 45.20%) with the same percentage. For non-users of fitness trackers, the order of preferred options was notebook (73.68%; 95%$CI$ = 64.61% − 81.49%), smartphone (69.30%; 95%$CI$ = 59.97% − 77.60%), desktop computer (54.39%; 95%$CI$ = 44.79% − 63.74%), tablet (35.97%; 95%$CI$ = 27.19% − 45.49%), and smartwatch (10.53%; 95%$CI$ = 5.56% − 17.67%).

### 3.5 Representations of Privacy Information

To identify requirements for *representations* of privacy information, users were asked how privacy-related information should be presented to them by a visual transparency-enhancing tool. As can be seen, when considering the confidence intervals (CIs) in Figure 1, there were no substantial differences between fitness tracker users and non-users. Participants preferred the presentation of privacy-related information through static visualizations, keywords, interactive visualizations, text, animations or videos, and interactive games. In summary, there was a tendency for participants to vote for a simple presentation of information, mainly through visualization techniques.

### 3.6 System Functions

To identify the *system functions* users require to improve understanding and control of their data, they were asked about their preferred features. Again, considering the confidence intervals (CIs) in Figure 1, observing no substantial differences in responses between

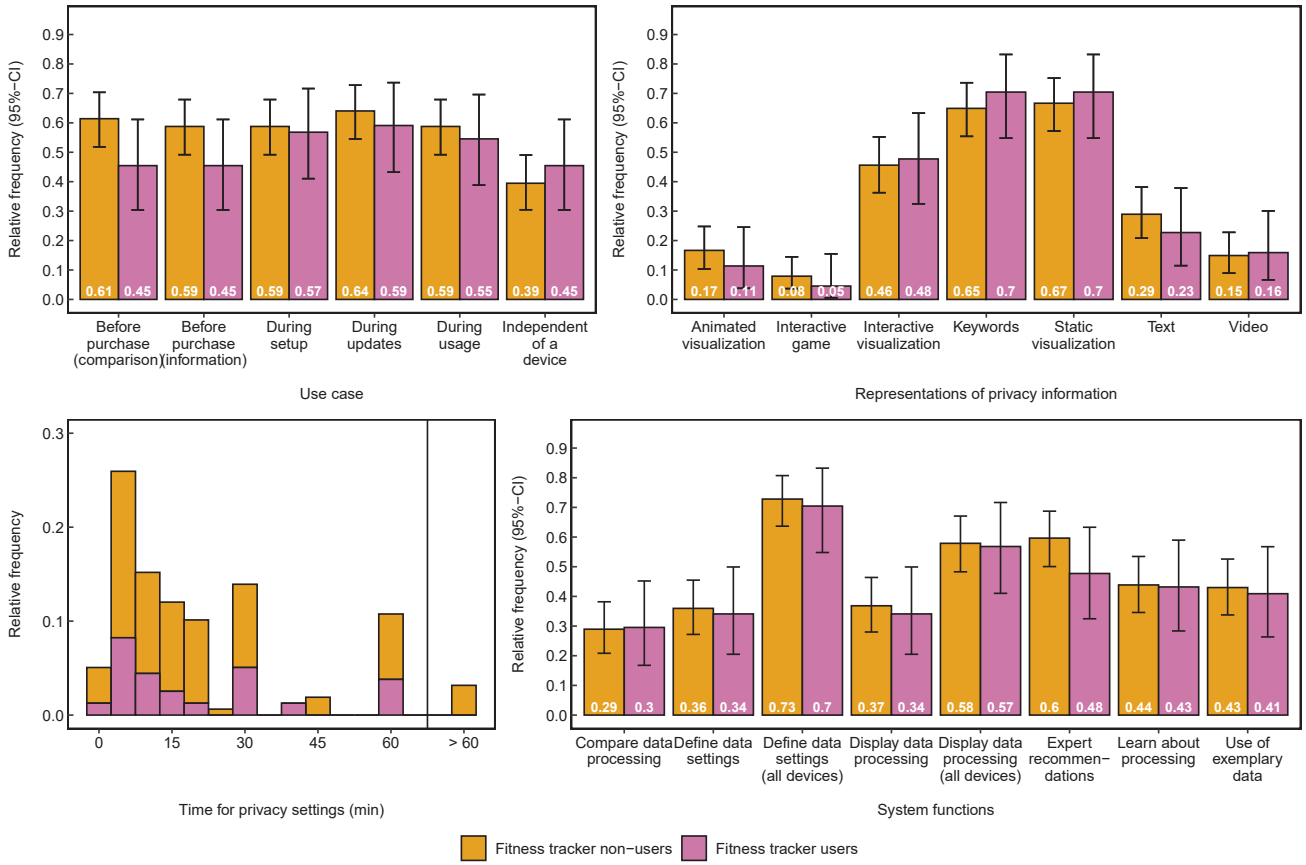


**Figure 1: Relative Frequency and 95%-Confidence Intervals of the closed questions for *use cases, time for privacy settings, privacy information representations* and *functionalities,* for the fitness tracker non-user and user group**

fitness tracker users and non-users led us to report aggregated results. Notably, for most users (72.15%), defining general data settings that would be applied to all their devices was an important aspect, followed by being able to display the data processing for all their devices (57.60%). In contrast, defining which data may be processed for single devices was reported to be prospectively being used less often (35.44% for defining data settings and 36.08% for displaying data processing). Only comparing how different devices process one's data received a lower share of positive ratings (29.11%). Other categories were expert recommendations (56.33%), learning about data processing (43.67%), and the usage of exemplary data (42.41%).

## 4 DISCUSSION

In the present study, we explored user needs and requirements as a basis for designing comprehensible visual representations of privacy policies and controls. We expect them to promote the development of information systems that support digital self-determination when using fitness trackers. The rationale for considering non-fitness tracker users was that the system to be developed based on user requirements should promote acceptance or use. Additionally, the vendors' perspective was incorporated by considering the optimal time within the usage cycle to access privacy information or functional requirements derived from the overall project objective.

### 4.1 Facilitating Privacy Control Exceeds Transparent Privacy Information

It was found that participants considered their control over the data collection and processing to be far more critical than receiving detailed information about these data practices (see section 3.6). Future privacy-preserving systems should, therefore, emphasize easy-to-use functionalities that allow users to exercise control over their data as pursued e.g., in recent work [34], while previous research often focused on enhancing privacy comprehension [14, 46]. At the same time, limits need to be investigated regarding how much control is appropriate or overwhelming for users. Together with [33, 35], current work confirms the importance of these requirements for users. However, this need cannot be addressed solely by developing a technical system. It would involve unified, multi-vendor labeling of technical or legal actors, activities, and processes to accommodate changes to the external framework conditions. Defining concrete data models might also be challenging due to

imprecise legal formulations (e.g. *legitimate interest*). Moreover, centralized control over data collection and processing requires systems to control concurrent ones. However, this contradicts economic interests or would increase implementation efforts.

## 4.2 Central Privacy Control and Access to Multiple Fitness Tracker and Applications

Defining privacy settings that apply to all devices received a considerably large agreement of over 70% percent among participants (see section 3.6). In addition, the fact that participants preferred a one-time privacy setting for all devices and applications reflects the need for a user interface that facilitates central access to various digital services and their privacy settings and is, therefore, open to all vendors and manufacturers. This means moving away from the current status quo in which users manage multiple user accounts from different vendors towards an inter-device control and inter-device presentation of information. Beyond the context of fitness trackers, other data-collecting devices could also be integrated. However, moving to centrally controlling privacy across data-collecting devices would require increased device integration [1], which in turn poses even more security and privacy risks [7, 15] through more comprehensive user data, vulnerable to misuse [29]. On the other hand, connected devices [39] share less data [32] and would only bear privacy risks through insecure connections. However, considering data security throughout development while applying encryption technologies may overcome this contradiction [3].

Finally, a diversity of technologies was also reflected in the question of which devices should be offered for accessing transparent and interactive privacy systems, highlighting smartphones and notebooks as the most commonly preferred with an agreement of at least 65% from both user and non-user groups (see section 3.4). As desktop computers achieved still over 50% with non-users, devices with screen sizes of smartwatches or larger should be included, especially for tasks that require more time or for which more visual information needs to be conveyed. For example, tasks that mainly concern fitness tracker non-users or new users, such as comparisons between vendors or initial setup (see section 3.2). One-third of fitness tracker users also selected the smartwatch, which, however, only received 10% voting of the non-user group. Based on these results and considering the limited screen size, we see the smartwatch as most valuable for fitness tracker users during usage for short privacy-related tasks, such as deciding on contextual privacy choices or receiving notifications about concise privacy updates.

## 4.3 Different Users Want to Spend Different Amount of Time on Privacy Settings

Almost half of the participants are willing to spend up to 10 minutes adapting privacy settings to their needs (see section 3.3). To be accessible for broader user groups, interactive privacy information should support participants in controlling and adjusting their privacy settings efficiently, with a time scope of max. 10 minutes. This is an important finding, as current textual privacy policies disclose extensive information about data handling by complying with the GDPR, which leads to considerably higher reading time. For example, privacy policies from popular vendors such as Fitbit or Xiaomi require 29 mins and 33 mins, respectively[1], which can even go up to, e.g., 63 mins for Facebook's app privacy statement. However, only one out of six available legal bases for data practices requires the user's consent. Isolating or highlighting, e.g., these privacy decisions, can reduce users' time on mandatory privacy consent. At the same time, to support users with a higher interest or concerns who want to invest more time and resources (almost 40%), privacy systems should provide enough optional depth to manipulate the settings more fine-grained.

## 4.4 Diverse User Requirements at Different Stages of the Usage Cycle

As our results show a consistent demand for all considered use cases, requirements are not only user-specific but also concern individual steps within the usage cycle, from purchase decision support to setup, usage, and update support (see section 3.2). Since each stage serves a specific purpose and comes with its own user requirements and primary user group, privacy-enhancing tools should adapt to these diverse conditions. For example, fitness tracker non-users might be mainly interested in comparing data practices of different vendors *before a potential purchase* and, therefore, rely on high-level and comparable privacy information. However, during *the initial setup* of a device, in-depth privacy controls would become more relevant for fitness tracker users. During *long-term use*, only minor adaptations of the settings in response to data privacy updates might be required. The different timing options of privacy choices identified by previous work, such as at setup, context-aware or periodic, could be applied here throughout the usage cycle [11]. To accommodate the dynamic change of requirements, we also recommend adapting the choice of information representation to the individual use case's primary purpose. Comparing different vendors' data practices relies on an efficient comparable, transparent display of data, making keywords or static visualization more valuable. Interactive visualizations should be provided during initial setup and long-term use to support individual privacy controls.

## 4.5 Supporting Decision-Making for Privacy Choices

Our results for system functions showed a considerable need for learning about data practices and expert recommendations, suggesting an essential requirement to provide not only transparent privacy information and controls but also guidance to support users in their privacy-related decision-making (see section 3.6). Such need for knowledge resources has also been identified in previous findings [13] and should support users with a better understanding of the consequences of privacy practices and their own privacy decisions. The underlying decision-making process of weighing benefits against potential privacy-related risks is known as the privacy calculus [21]. For example, the purchase decision of a fitness tracker from a specific vendor, the disclosure or non-disclosure of certain data types, or the sharing of activity data among friends or social media platforms can considerably impact users' data privacy and the scope of the tracker's functionality. Hence, the value users get out of their devices. Privacy decisions can be, therefore, often a

[1]Calculated with the tool Ratte from the University of Regensburg [45].

subjective trade-off between gained functionality and impacted data privacy security. Our recommendation is to support the substantial amount of users (>40%) seeking to gain data literacy by facilitating the acquisition of competency with privacy information.

### 4.6 Limitations and Future Work

While present work provides valuable insights into fitness tracker users' and non-users' needs, study limitations and future opportunities should be acknowledged. As with many online surveys, their subjective character might be subject to social desirability. Future studies on users' needs for interactive and transparent privacy information would profit from controlling this variable. In addition, confounding variables could include different background knowledge and the fact that respondents had to imagine the functional and non-functional properties to evaluate them. Additionally, surveyed participants may have a different understanding of terms about the queried criteria than initially assumed. Furthermore, acquiring participants through universities and social media may have led to an over-representation of individuals from Germany with higher education and technical affinity.

## 5 CONCLUSION

The present work investigated user needs as a basis for the development of comprehensible visual representations of privacy policies and privacy controls. We found that an efficient and personalized one-time setting to control data collection and processing across different devices and platforms is far more critical for people than being informed about these processes. This has implications for technology development and the governance of legal and economic frameworks. One question to be answered in this regard is how we want to resolve or mitigate the conflict between individual and economic interests. After the legal and economic groundwork has been done to prioritize individual needs, systems that enable digital self-determination can be developed. We further found that information about and the control of privacy must be provided at different levels of detail at various stages of the usage cycle. This finding is essential for developing adaptive systems, assistance systems, and dynamic user models. These would allow for dynamic adjustment of the degree to which background and expert knowledge must be included. Future work can build on these results, investigate more detailed requirements, and validate them for various application scenarios. Furthermore, quantifying the impact of particular user requirements on digital self-determination would prioritize them.

## ACKNOWLEDGMENTS

This publication is part of the research project "InviDas" financed by the Federal Ministry of Education and Research (BMBF, under Grant No.: 16SV8536) and promoted by VDI/VDE Innovation + Technik GmbH.

## REFERENCES

[1] Abdulmalik Alwarafy, Khaled A Al-Thelaya, Mohamed Abdallah, Jens Schneider, and Mounir Hamdi. 2020. A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet of Things Journal* 8, 6 (2020), 4004–4022. https://doi.org/10.1109/JIOT.2020.3015432

[2] Vinayshekhar Bannihatti Kumar, Roger Iyengar, Namita Nisal, Yuanyuan Feng, Hana Habib, Peter Story, Sushain Cherivirala, Margaret Hagan, Lorrie Cranor, Shomir Wilson, Florian Schaub, and Norman Sadeh. 2020. Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text. In *Proceedings of The Web Conference 2020 (WWW '20)*. Association for Computing Machinery, New York, NY, USA, 1943–1954. https://doi.org/10.1145/3366423.3380262

[3] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. 2019. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* 7 (2019), 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872

[4] Alex Bowyer, Jack Holt, Josephine Go Jefferies, Rob Wilson, David Kirk, and Jan David Smeddinck. 2022. Human-GDPR Interaction: Practical Experiences of Accessing Personal Data. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 106, 19 pages. https://doi.org/10.1145/3491102.3501947

[5] Simon Byers, Lorrie Faith Cranor, Dave Kormann, and Patrick McDaniel. 2004. Searching for privacy: Design and implementation of a P3P-enabled search engine. In *International Workshop on Privacy Enhancing Technologies*. Springer, Berlin, Heidelberg, 314–328. https://doi.org/10.1007/11423409_20

[6] John T. Cacioppo and Richard E. Petty. 1982. The need for cognition. *Journal of Personality and Social Psychology* 42, 1 (1982), 116–131. https://doi.org/10.1037/0022-3514.42.1.116

[7] Jiska Classen, Daniel Wegemer, Paul Patras, Tom Spink, and Matthias Hollick. 2018. Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1, Article 5 (mar 2018), 24 pages. https://doi.org/10.1145/3191737

[8] Niël H Conradie, Sabine Theis, Jutta Croll, Clemens Gruber, and Saskia K Nagel. 2022. The impact of smart wearables on the decisional autonomy of vulnerable persons. In *Künstliche Intelligenz, Demokratie und Privatheit*. Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, 377–402. https://www.nomos-elibrary.de/10.5771/9783748913344-377.pdf

[9] Lorrie Faith Cranor, Manjula Arjula, and Praveen Guduru. 2002. Use of a P3P user agent by early adopters. In *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*. Association for Computing Machinery, Washington, DC, USA, 1–10. https://doi.org/10.1145/644527.644528

[10] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 67, 12 pages. https://doi.org/10.1145/3411764.3445516

[11] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[12] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. https://doi.org/10.1080/10447318.2018.1456150

[13] Sandra Gabriele and Sonia Chiasson. 2020. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376651

[14] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, Yuvraj Agarwal, Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 2016. How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In *Symposium On Usable Privacy and Security (SOUPS) (SOUPS '16, Soups)*. USENIX Association, Denver, Colorado, 321–340. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf

[15] Rohit Goyal, Nicola Dragoni, and Angelo Spognardi. 2016. Mind the Tracker You Wear: A Security Analysis of Wearable Health Trackers. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing* (Pisa, Italy) *(SAC '16)*. Association for Computing Machinery, New York, NY, USA, 131–136. https://doi.org/10.1145/2851613.2851685

[16] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108

[17] Einar Gudmundsson. 2009. Guidelines for translating and adapting psychological instruments. *Nordic Psychology* 61, 2 (2009), 29–45. https://doi.org/10.1027/1901-2276.61.2.29

[18] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu,

HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376511

[19] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 63, 25 pages. https://doi.org/10.1145/3411764.3445387

[20] Carlos Jensen and Colin Potts. 2004. Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vienna, Austria) *(CHI '04)*. Association for Computing Machinery, New York, NY, USA, 471–478. https://doi.org/10.1145/985692.985752

[21] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* 25, 6 (2015), 607–635. https://doi.org/10.1111/isj.12062

[22] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security (SOUPS '09)*. Association for Computing Machinery, New York, New York, USA, 1. https://doi.org/10.1145/1572532.1572538

[23] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'10)*. Association for Computing Machinery, New York, NY, USA, 1573. https://doi.org/10.1145/1753326.1753561

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

[25] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security (SOUPS'20)*. USENIX Association, USA, Article 23, 20 pages. https://www.usenix.org/system/files/soups2020-kitkowska.pdf

[26] Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for All: Revealing the Hidden Complexity of Terms and Conditions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 2687–2696. https://doi.org/10.1145/2470654.2481371

[27] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[28] Tamara Munzner. 2009. A nested model for visualization design and validation. *IEEE transactions on visualization and computer graphics* 15, 6 (2009), 921–928. https://doi.org/10.1109/TVCG.2009.111

[29] Boubakr Nour, Kashif Sharif, Fan Li, and Yu Wang. 2019. Security and privacy challenges in information-centric wireless internet of things networks. *IEEE Security & Privacy* 18, 2 (2019), 35–45. https://doi.org/10.1109/MSEC.2019.2925337

[30] Anna-Marie Ortloff, Maximiliane Windl, Valentin Schwind, and Niels Henze. 2020. Implementation and In Situ Assessment of Contextual Privacy Policies. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference (DIS '20)*. Association for Computing Machinery, New York, NY, USA, 1765–1778. https://doi.org/10.1145/3357236.3395549

[31] Data Protection Working Party. 2004. *Opinion 10/2004 on More Harmonised Information Provisions.* Technical Report. EU Commission.

[32] Paola Pierleoni, Roberto Concetti, Alberto Belli, and Lorenzo Palma. 2019. Amazon, Google and Microsoft solutions for IoT: Architectures and a performance comparison. *IEEE access* 8 (2019), 5455–5470.

[33] Robert W Reeder, Clare-Marie Karat, John Karat, and Carolyn Brodie. 2007. Usability challenges in security and privacy policy-authoring interfaces. In *IFIP Conference on Human-Computer Interaction*. Springer, Berlin, Heidelberg, 141–155.

[34] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual Interactive Privacy Policy: The Better Choice?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 66, 12 pages. https://doi.org/10.1145/3411764.3445465

[35] Manuel Rudolph, Denis Feth, and Svenja Polst. 2018. Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction*. Springer, Berlin, Heidelberg, 587–598.

[36] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly* 20, 2 (1996), 167–196. http://www.jstor.org/stable/249477

[37] Nili Steinfeld. 2016. "I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior* 55 (2016), 992–1000. https://doi.org/10.1016/j.chb.2015.09.038

[38] Carolin Stellmacher, Jette Ternieten, Daria Soroko, and Johannes Schöning. 2022. Escaping the Privacy Paradox: Evaluating the Learning Effects of Privacy Policies With Serious Games. *Proc. ACM Hum.-Comput. Interact.* 6, CHI PLAY, Article 232 (oct 2022), 20 pages. https://doi.org/10.1145/3549495

[39] Shengjing Sun, Xiaochen Zheng, Javier Villalba-Díez, and Joaquín Ordieres-Meré. 2020. Data handling in industry 4.0: Interoperability based on distributed ledger technology. *Sensors* 20, 11 (2020), 3046.

[40] Ali Sunyaev, Tobias Dehling, Patrick L Taylor, and Kenneth D Mandl. 2015. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* 22, e1 (2015), e28–e33. https://doi.org/10.1136/amiajnl-2013-002605

[41] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing User Attention With a Comic-based Policy. In *Conference on Human Factors in Computing Systems - Proceedings (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3173574.3173774

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

[43] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2022. Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 181 (dec 2022), 41 pages. https://doi.org/10.1145/3494960

[44] Kim-Phuong L Vu, Vanessa Chambers, Fredrick P Garcia, Beth Creekmur, John Sulaitis, Deborah Nelson, Russell Pierce, and Robert W Proctor. 2007. How users read and comprehend privacy policies. In *Symposium on Human Interface and the Management of Information*. Springer, Berlin, Heidelberg, 802–811. https://doi.org/10.1007/978-3-540-73354-6_88

[45] Johannes Wild. 2019. Das Regensburger Analysetool für Texte: RATTE. In *Sprachschätze. Materialsammlung*. o.V. (LISA, Bildungsserver Sachsen-Anhalt), Halle (Saale), 1–8. https://epub.uni-regensburg.de/45121/

[46] Maximiliane Windl, Niels Henze, Albrecht Schmidt, and Sebastian S. Feger. 2022. Automating Contextual Privacy Policies: Design and Evaluation of a Production Tool for Digital Consumer Privacy Awareness. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 34, 18 pages. https://doi.org/10.1145/3491102.3517688

[47] Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John Millar Carroll. 2012. Measuring Mobile Users' Concerns for Information Privacy. In *ICIS 2012 Proceedings*. Association for Information Systems (AIS), Atlanta, Georgia, USA, 2278–2293. https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10

[48] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2023. "Revoked just now!" Users' Behaviors toward Fitness-Data Sharing with Third-Party Applications. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 1–21.