Our Data, Our Solutions: A Participatory Approach for Enhancing Privacy in Wearable Activity Tracker Third-Party Apps

Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, Kévin Huguenin

Our Data, Our Solutions: A Participatory Approach for Enhancing Privacy in Wearable Activity Tracker Third-Party Apps

Noé Zufferey
ETH Zurich
Switzerland
noe.zufferey@gess.ethz.ch

Kavous Salehzadeh Niksirat
University of Lausanne & EPFL
Switzerland
kavous.salehzadehniksirat@unil.ch

Mathias Humbert
University of Lausanne
Switzerland
mathias.humbert@unil.ch

Kévin Huguenin
University of Lausanne
Switzerland
kevin.huguenin@unil.ch

ABSTRACT

Wearable activity trackers (WATs) have recently gained worldwide popularity, with over a billion devices collecting a range of personal data. To receive additional services, users commonly share this data with third-party applications (TPAs). However, this practice poses potential privacy risks. Privacy-enhancing technologies have been developed to address these concerns, but they often lack user-centered design, and therefore, are less likely to be directly related to users' concerns and to be widely adopted. This study takes a participatory design approach involving $N = 26$ experienced WAT users who share data with TPAs. Through a series of design sessions, participants conceptualized 19 solutions, from which we identified seven different design features. We further analyze and discuss how these features can be combined to assist users in managing their data sharing with TPAs and, therefore, enhancing their privacy. Finally, we selected the three most promising features, namely PARTIAL SHARING, REMINDER, and REVOCATION ASSISTANCE, and conducted an online survey with $N = 201$ WAT users to better understand the potential effectiveness and usability of these features. This work makes an important contribution by offering user-centered solutions and valuable insights for integrating privacy-enhancing technologies into the WAT ecosystem.

KEYWORDS

privacy, fitness trackers, wearables, fitness data, third-party applications, participatory design, user survey

1 INTRODUCTION

Wearable activity trackers (WATs), such as wrist-worn fitness trackers and smartwatches, have become increasingly prevalent [58], as there are more than one billion wearable devices worldwide [67]. In addition to their WAT service provider, users can also choose to share their data voluntarily with other individuals, such as family, friends, co-workers, and healthcare professionals, or entities, such as employers, insurance companies, and third-party service providers. This is typically done through online social networks or third-party applications (TPAs). A TPA is an app or service that is not provided by the company that manufactured the device (e.g., Apple, Fitbit). For example, the Strava app[1] qualifies as a TPA: (1) users can grant reading access to the data collected by the WAT, (2) the app is owned and managed by a company other than the manufacturer; user data is therefore shared with a *third-party* entity. A TPA does not necessarily correspond to a mobile app installed on the user's smartphone. Indeed, it is, first and foremost, a simple service using a service provider API in order to access user data, with a dedicated authorization key. In multiple cases, this access is granted by the users in exchange for some given service, which may or may not involve installing a mobile app.[2]

Users share WAT data to gain social [48, 89] or financial [37, 110] benefits or receive additional features not offered by the original services or app. WAT data sharing with TPAs is widespread, but only a limited number of studies have been devoted to it [6, 115]. Despite the numerous advantages offered by TPAs, there are potential risks associated with their usage. TPAs could collect more data than they actually need to provide their services [80], which might lead to sharing data with other parties or using it without the users' consent/awareness. Due to their physiological (e.g., heart rate) and contextual (e.g., activities) nature, WAT data are highly sensitive and might raise various privacy issues. For instance, WAT data can be used to infer daily activities and habits (e.g., eating) [1, 32, 66, 76], drug usage (e.g., cocaine) [78], SARS-CoV-2 infections [54], mental health [2], and even personality traits [114]. Aggregated location data have even been used to locate military bases and to infer their internal structures [53], specifically in remote areas where unusual activity patterns were observed. More on the users' side, users unwittingly could lose track of their TPAs [99], forgetting which apps and what data they have already granted access to. Previous investigations on users' awareness, understanding, attitudes, and behaviors [41, 102, 115] revealed that about half of WAT users underestimate the number of TPAs to which they have granted access to their data, and almost two-thirds share data with at least one TPA that they do not actively use (anymore).

Proceedings on Privacy Enhancing Technologies 2024(4), 734–754

https://doi.org/10.56553/popets-2024-0139

[1] See https://www.strava.com/features, Last accessed May 2024.
[2] For example, anyone with a Fitbit development account can register an app on the dedicated platform (see Figure 4 in Appendix A) and ask users to grant them data access using a specific link. Note that this is not the case for Apple Health, as it does not provide a web API, but only a local (i.e., mobile) one, and so data are transmitted directly from one to another mobile app, on the phone.

Furthermore, a large number of users do not revoke TPA access to their data because they had forgotten that they gave access to it in the first place or were not even aware they could revoke access to their data [115]. In the meantime, the companies that provide the users with TPAs are still able to request their data (e.g., through a dedicated API) [56]. In fact, the main difference between WAT data-sharing and smartphone permissions is that the former is based on Web API permissions that can persist after the dedicated smartphone app is uninstalled. This is because requests are often not made to the mobile OS but are directly sent to the API provider's servers (e.g., Fitbit). To request data using, for example, a REST API permission, an entity would only need to get an access token. In this way, the requests and responses can be transmitted from their server to the WAT company's server without any communication with the user's WAT or smartphone. Thus, it does not matter if any app is installed or not. Furthermore, whereas online social network (OSN) TPAs work similarly to WAT TPAs, the process differs in the nature and context of WAT data. First, physiological data are (almost) continuously collected (e.g., step count for each minute). Second, most of the time, the user adopts a passive attitude to data collection (the data is collected whatever they do), which is not the case when they post on OSNs, for example.

Whereas smartphone permissions and OSN TPAs have been widely studied [8, 13, 59, 105], there has been very little similar work on WATs to date. Despite similarities between WATs and OSN TPAs or smartphone permissions, the particular structure of WAT data such as time series, particularly sensitive physiological data, and continuous tracking requires the development of solutions specifically tailored to this context. Therefore, it is crucial to design privacy-enhancing technologies (PETs) to help TPA users better manage their multiple applications and better understand how the WAT-data sharing ecosystem works. Such PETs could help them avoid risky behaviors for privacy, such as sharing more data than is actually required or not regularly checking the previously granted permissions to revoke them if necessary.

Several studies on PETs in the context of WAT have been published. These studies provided different types of solutions to preserve WAT users' privacy, e.g., data minimization [30, 60, 104], pedagogical solutions [4, 90, 91, 99], and AI assistance [70]. However, there is still a significant research gap that needs to be addressed—**a gap that concerns the focus on *users* in the development of these solutions.** Although some of the previously designed solutions have been evaluated by users afterward, the studies mentioned earlier did not involve the end-user in the design process and do not particularly focus on WAT-data sharing with TPAs. Moreover, participants of these studies are not necessarily WAT users with actual experience in data sharing with TPAs. Yet, involving users upstream in the design process would often highlight problems and solutions that developers and researchers would not have thought of. Furthermore, a recent literature survey work about the utility, privacy and security of WATs suggests that user-centered methods, such as participatory design, would bring relevant insight for developing PETs [79].

To enhance the privacy of WAT users during the data-sharing process with TPAs and to adopt a user-centered approach, we propose utilizing participatory design [109]; a cooperative method involving users in the design process. In this study, we ask: *What solutions will be suggested by WAT TPA users to help them better manage data sharing to eventually avoid risky behaviors for privacy?*

To address this question, we recruited participants who were *actual TPA users*: WAT users who had used their WATs for at least six months and shared their data with at least one TPA. Our report presents designs suggested by $N = 26$ participants in three participatory design sessions (8–9 participants for each session). We conducted informational sessions for participants, focusing on increasing their understanding of the WAT data-sharing ecosystem and raising awareness of the potential related privacy threats. Participants engaged by reflecting on their personal experiences and conceptualizing 19 different solutions through low-fidelity paper prototypes. We then categorized these solutions based on their characteristics, resulting in seven distinct features. We also collectively (i.e., all co-authors in plenary meetings) analyzed and evaluated the participants' design solutions to further assess the feasibility, effectiveness, adoption, and usability of the features they proposed as PETs. Lastly, we selected the three most promising features (according to the evaluations) and conducted an online user survey with $N = 201$ respondents to evaluate the potential for adoption (effectiveness and usability) on a larger scale.

Our efforts led to a possible comprehensive solution to provide privacy protection and support for WAT users throughout their interaction with TPAs.This solution leverages multiple design features, including PARTIAL SHARING, which would allow the users to selectively share only part of their data; REMINDER, which would periodically remind the users they share their data with TPAs; and REVOCATION ASSISTANCE, which would facilitate the revocation of data access authorization and data removal. Our work makes several key contributions: (1) We present seven distinctive features, created by actual WAT and TPA users to assist them in managing their data-sharing with TPAs. (2) We discuss and evaluate these features by providing qualitative and quantitative analysis. (3) We propose a solution composed of the most well-evaluated previously discussed features. (4) We provide insights on implementing the solution within already established WAT ecosystems.

2 RELATED WORK

Prior research has three main streams. The first stream explores the (self-reported) behaviors, habits, concerns, and attitudes of WAT users regarding privacy and WAT-data sharing. The second stream has developed new PETs for WATs. Additionally, a third stream has investigated third-party app permission in different contexts, mainly smartphones and online social networks (OSNs).

2.1 WAT users privacy concerns, awareness, behavior, and attitude

Many studies focused on understanding WAT users' privacy concerns, awareness, behaviors, and attitudes. Lidynia et al. [68] examined WAT users' privacy concerns and the perceived sensitivity of their data and found that users perceive some data as more sensitive than others (e.g., sleep data).

Vitak et al. [103] asked users to read the relevant part of the terms of service and showed that most users were unaware of what they had agreed to (gave consent) and were surprised by the extent of access they had given to WAT service providers. Schneegass

et al. [92] analyzed how WAT users' willingness to share WAT data changes depending on the type of data (including the sensors used to collect it), the derived data, and the data recipients. They found a negative correlation between the willingness to share and the size of the audience. They also found that users prefer to share specific derived data rather than raw sensor data. Furini et al. [40] analyzed the willingness of WAT users to share WAT data *for altruistic reasons*, specifically, to help fight the COVID-19 pandemic, and found that individuals are more likely to share data when they have a strong altruistic motivation.

Gabriele and Chiasson [41] studied WAT users' general attitudes, knowledge, and behaviors toward their devices. They focus on the user's awareness regarding the effect of WAT data collection on their privacy, their sharing intentions and behaviors, and their general feelings toward data sharing. They showed that users' concerns and behaviors depend primarily on the data type and recipients. Velykoivanenko et al. [102] studied WAT users' perceptions of the associated privacy risks and found that their respondents were generally aware of the possibility of inferring sensitive information from WAT data. However, they could not think about inferring information unrelated to physiological data, which could be inferred to some extent using WAT data (see for example [114] for inferring users personality based on WAT data). Lupton [71] studied how users share WAT data with other individuals, where most of their respondents reported considering only privacy from a "social privacy" point of view and do not view how their data can be used by third parties (e.g., advertisers and health insurers). Pinchot and Cellante [83] measured the relationship between WAT users' data-sharing habits and their understanding of privacy settings. They found that self-reported data-sharing behavior is negatively correlated with the understanding of privacy settings and privacy policies.

While the aforementioned literature has studied WATs in general, there is only a limited number of studies with a specific focus on WAT TPAs. Alqhatani and Lipford [6] studied WAT-data-sharing behavior and the concerns of WAT users. They reported that five of their participants reported sharing fitness data with TPAs such as health insurance companies (to reduce their premiums). More relevant to TPAs, Zufferey et al. [115] recently conducted a user survey on WAT user behavior and understanding of data sharing with TPAs. They found that half of their respondents underestimated the number of TPAs they shared their data with. Surprisingly, almost two-thirds of the respondents reported that they did not use all of the TPA's mobile apps installed on their phones.

2.2 Privacy Enhancing Technologies

Many studies on PETs for WATs have been published in recent years. In this section, we review them. Multiple studies focus on methods for effectively anonymizing WAT data. Given that WAT data have a high dimensionality and a sequential time-series nature, anonymizing such datasets presents a challenge. Parameshwarappa et al. [82] use a multi-level clustering anonymization technique to prevent the re-identification of WAT users. Gong et al. [44] propose a theoretical framework for federated learning that preserves individuals' privacy while training a machine learning (ML) model by using data from multiple WATs. Garbett et al. [42] designed an activity-sharing platform for classrooms, enabling students to use pseudonymized avatars to share WAT data without exposing their identity.

Some studies focus on limited sharing and data minimization. Wang et al. [104] investigate user preferences and sharing behavior related to partial-data release. Epstein et al. [30] explore how fine-grained step-count sharing can help WAT users in maintaining user privacy while sharing activities. Velykoivanenko et al. [102] assess users' utility perceptions to inform future PET design related to fine-grained data sharing. Kalupahana et al. [60] propose a framework that employs random noise from WAT sensors to generate noise for differential privacy protection. Zufferey et al. [115] evaluated the likelihood of WAT users adopting different PETs in the context of data-sharing with TPAs, which represents, to the best of our knowledge, the only published study directly related to WATs and TPAs. They also show that there is a high potential for implementing *data minimization* to mitigate certain privacy risks. Other studies focus on pedagogical solutions. Torre et al. [99] model the complexity of WATs and TPAs to compute the probabilities of inferring different information from WAT data. Their model is designed to demonstrate to WAT users that they can protect their privacy by refraining from sharing certain data. Aktypi et al. [4] design a pedagogical tool that informs WAT users of the risks they face when sharing specific WAT data (e.g., running routes), along with other information (e.g., information available on their social media). Alvarez et al. [9] show that watching a video about the privacy and security risks of collecting and sharing WAT data can significantly improve attitudes toward cybersecurity, whereas a text version of the information has no significant effect. Sanchez et al. [90] model the privacy preferences of WAT users and developed a system for recommending personalized privacy settings for users in different scenarios. Other studies are more centered on designing new functionalities to help WAT users in data-sharing. Data integrity is critical for healthcare providers and insurance companies that are interested in users' WAT data. du Toit [25] designed PAUDIT, a decentralized data architecture that enables users to store their WAT data in a personal online data store and permits healthcare providers to read data and audit the logs (i.e., changes made to the access control list). Ghazinour et al. [43] propose an access-management tool that enhances users' decision-making by enabling them to share their WAT data after considering four aspects: purpose (why), visibility (who), granularity (how), and retention (when). Murmann et al. [77] studied the possible adoption of privacy notifications for WAT usage (survey with $N = 304$), where most of their respondents found privacy notifications useful for monitoring their data-sharing and for increasing their privacy. Liu et al. [70] propose an ML framework to provide WAT users with personalized fitness recommendations without collecting personal information. Kazlouski et al. [61] analyzed unnecessary communication from the Fitbit companion app (as well as six of the most used TPAs) to their business partners and proposed an easy-to-use methodology to block them. In their work, Alqhatani and Lipford [7] review already existing PETs provided by well-known WAT brands. Contrary to previous work, we conducted a participatory design study to involve users early in the PETs design process. By doing so, we aim to bring to light issues and solutions that might not have been considered by developers and researchers, as they may not align with the primary target audience.

2.3 Smartphone and OSN Permissions

In addition to the studies focusing on WATs, it is important to recognize research that examined smartphone permissions and proposed related privacy-enhancing technologies. Researchers analyzed mobile apps and spotted the overprivileged ones [24, 35, 55, 80]. Such apps often ask for more permissions than are required, as engineers may misunderstand some permission data scope [96]. Users also do not fully understand smartphone permissions, and they are usually overloaded due to the high number of different permissions to be settled [5], thus, they often overlook permissions [29, 39]. Alsoubai et al. [8] observed users and identified different categories of users' behavior toward permissions. Wottrich et al. [113] analyzed how smartphone users perceive the privacy trade-off. Ismail et al. [59] used a crowd-sourced approach to study the impact of removing some previously enabled smartphone app permissions on users' privacy and utility. Also, some studies investigated how users make permissions decisions [17], including one in the context of permission run-time dialogue [16]. Finally, several studies [20, 52, 95] explored the potential of using a personal privacy assistant to manage data-sharing and permissions. Elahi and Wang [28] propose a framework to distribute the responsibility of choosing the privacy settings to reduce the amount of effort required of the users. Smullen et al. [94] used machine learning to assist users in adjusting their permissions.

As for permissions and TPAs related to OSNs, King et al. [63] explored what Facebook users understand about their data-sharing with TPAs and how they interact with them. Wang et al. [106] analyzed a large number of Facebook TPAs on how the permission box dialog reflects the true app behavior. Krasnova et al. [65] studied the users' privacy concerns and attitudes toward data-sharing with TPAs on Facebook, whereas Wisniewski et al. [111] focus on how their concerns and attitudes are related to Facebook users' engagement with their "Facebook friends". Recently, Arias-Cabarcos et al. [13] studied the effect of transparency on users' attitudes toward data sharing by confronting them about Facebook TPAs' behavior toward data sharing. Multiple studies have proposed protection mechanisms to improve the OSN data-sharing ecosystem, such as a policy file-oriented solution [23], an alternative design for data-sharing panel [106], solutions for flexible and minimal data-sharing (e.g., fine-grained sharing) [12, 18, 64, 93], and a framework enabling OSN users to quantify the privacy and utility implications of data-sharing with TPAs [3].

To sum up, while multiple studies have been conducted on users' behavior and understanding of smartphone and OSN permissions, and other studies have explored the potential of using and adopting mechanisms to improve app permissions, to the best of our knowledge, there is no study—particularly, in the context of WAT TPAs—that involves users in designing solutions to help them manage their privacy better.

3 PARTICIPATORY DESIGN METHODOLOGY

In this study, we focus on the solutions proposed by WAT users to enhance their privacy when sharing their data. As the problem we aim to address is related to the end-users behaviors and understanding, it is crucial to develop solutions tailored to their specific needs. To achieve this, we conduct participatory design sessions [109] with WAT users who actively share data with TPAs. Whereas there are few studies discussing PETs in the context of new functionalities for data sharing [7, 102, 115] or as tools to improve comprehension of privacy policies [50], to the best of our knowledge, all published works related to PETs for WAT-data sharing have been about solutions designed by developers or researchers. We believe that developers and researchers may carry biases related to their roles, potentially overlooking usability issues with their solutions. Consequently, involving users directly could provide us with relevant perspectives and insights, as they are the primary stakeholders in the use of WATs and data sharing. Participatory design is a user-centered approach designers use to incorporate end users into the design process [62]. This approach has been used in multiple studies related to utility, including WAT utility [22, 69, 72], and privacy [57, 88]. It proves especially valuable in developing solutions related to usable security and privacy [116]. We scheduled three participatory design sessions. By soliciting direct input from users for proposed solutions, we gather insights from the individuals who are the most affected by privacy issues and the usage of the related technology (i.e., WATs). We designed our study according to the participatory design approach employed in prior studies [45, 88, 109]. Most of the content presented to the participants during the design sessions was adapted from earlier research findings (e.g., [115]). We performed different participatory design activities to raise participants' awareness about the risks associated with data sharing, stimulate their creativity, and elicit effective solutions.

Ethical Considerations. Before each design session, participants were required to sign a consent form outlining the conditions of participation, details regarding the data being collected (and the associated data-management plan), the procedure for withdrawing from the study, and information about the financial incentive. The institutional review board (IRB) at our university reviewed and approved the consent form and the study itself. Participants received compensation in 70 CHF (∼ 75 USD) at the conclusion of each session.

3.1 Recruitment

LABEX, a dedicated structure of the University of Lausanne (UNIL), helped us in the recruitment process by managing a pool of approximately 8000 students from two universities (a technical one, i.e., EPFL, and a general one, i.e., UNIL itself, covering a broad range of disciplines). Interested students participated in our experiment by completing a brief screener survey, which we utilized to assess their eligibility for participation. The online screener survey was designed to be as concise as possible (taking approximately 5 minutes to complete). It consisted solely of questions necessary to filter participants based on our criteria (see below), collecting basic demographic information to ensure a balanced sample (e.g., concerning gender), WAT usage, and gathering insights into WAT usage and data-sharing behavior. The recruitment criteria were as follows: (1) regular use of a WAT device (a minimum of three days a week) for more than six hours per day, (2) a minimum of six months experience using their WAT (to ensure we had "experienced" users [19, 75]), (3) active data-sharing with at least one third-party application, and (4) proficiency in French (i.e., the local

language at the universities). By applying these criteria, we aimed to engage individuals who already had a substantial connection with their devices and possessed prior experience and familiarity with the ecosystem. A total of 831 individuals responded to the screener questionnaire, and 54 met the experiment's criteria. To ensure high-quality discussions and to facilitate interaction between the participants, we strategically conducted the sessions *in person* with a limited number of attendees.

For each session, 11 individuals were invited to finally obtain nine participants, anticipating a few potential "no-shows." In cases where more than nine individuals attended a given session, the last arrivals were provided with 10 CHF (~ 10 USD) as compensation. However, the latecomers did not receive compensation. Should an invited individual withdraw before the session commencement, we extended an invitation to someone else. Overall, we invited 40 individuals (selected to achieve a balanced gender representation), nine of whom withdrew before their session, two did not attend, and three additional participants were sent back (including one who was not compensated due to lateness). Ultimately, a total of $N = 26$ individuals participated in the sessions. This sample size aligns with the range observed in related work, with studies reporting sample size of $n = 9$ [46], $n = 15$ [109], $n = 25$ [45], and $n = 26$ [88], among others.

3.2 Participants & Groups Composition

Table 1 in Appendix D provides an overview of the sessions and the composition of each group. The groups were carefully arranged to ensure gender balance. Each group consisted of three participants, except for Group 2 in Session 1, which had only two participants. Out of all the participants, 42% were women (11 participants), whereas 58% were men (15 participants). Their average age was 21.1 years, with a standard deviation of 2.5 years. On average, they reported wearing their WAT for 5.9 days a week, with a standard deviation of 1.4 days. Approximately 35% wore their WAT for around seven to 12 hours a day, 27% for 13 to 18 hours, and 38% for 19 to 24 hours. Our sample was composed of 65% of Apple users, 12% of Fitbit users, 19% of Garmin users, and only one of them (4%) had another type of device. Half of the participants (50%) shared their data with only one TPA and 42% with two to five TPAs. Only two participants shared their data with six to nine TPAs (4%), or with 10 or more TPAs (4%).

3.3 Session Procedure

To facilitate focused design sessions, we assigned participants to different sessions, ensuring that each participant attended only one session. Figure 6 in Appendix C describes the room and furniture that we used during the session. We conducted all three sessions on two consecutive days without overlap (one on the first day in the afternoon and the other two on the second day, respectively, in the morning and the afternoon). Each session lasted approximately two and a half hours. Three researchers conducted the sessions: the first author of this article, who served as the main facilitator, and two assistants (including the second author of this article). We recorded audio from all sessions and obtained consent from participants to take photos of the artifacts. Before the study commenced, we conducted a trial session with two external researchers (non-co-authors) from our university who had expertise in distributed systems and security & privacy, respectively. This aided us in refining the protocol, making minor adjustments to the presentations and slides, and slightly shortening the session by removing a global discussion activity about personal experience sharing, instead encouraging participants to share their experiences during the sketching part.

For an overview of the session procedure, refer to Figure 5 in Appendix B. Each session comprised five main segments: (1) Introduction, (2) Setting up the situation, (3) Upgrading knowledge, (4) Sketching, and (5) Value ranking. These activities encompassed three types: (a) Presentations, aimed at providing participants with insights into the problems, state-of-the-art information, and general ground truth about the WAT data-sharing ecosystem; (b) global activities, where all nine participants collectively shared their knowledge, experiments, and thoughts about WAT data-sharing; and (c) group activities, involving three participants each, to help them focus on specific problems and propose relevant solutions. Below, we provide a detailed description of these activities.

3.3.1 Part I. Introduction (20 min.) Participants were invited to attend participatory design sessions and were asked to wear their WATs and bring their phones. Two researchers welcomed them, ushered them into the room, and guided them through the process of filling out and signing the consent form. Afterward, they were seated around a table, free to choose their seats. Once everyone was seated, a few participants were asked to switch places to form gender-balanced groups. Following verbal confirmation of participants' consent, the session commenced with audio and video recording. The study's main goals were outlined after a brief description of the schedule. The main facilitator emphasized the purpose: Designing tools to enhance users' data-sharing management and/or improve their understanding of the data-sharing process.

3.3.2 Part II. Setting Up the Stage (20 min.) Each session began with a brief presentation highlighting how WAT-data sharing could impact users' privacy. This activity aimed to ensure participants were aware of the issue and encouraged to share their concerns and experiences regarding data sharing. The facilitator demonstrated various ways WAT users share their data and presented a short video illustrating the process of granting and revoking access to data for a specific TPA. Strava was used as an example due to its widespread use as a fitness app. Participants were then prompted with thought-provoking questions about data privacy: "Who do you think might be interested in accessing your fitness data, and why?", and "What do you think it is possible to do with or learn from your fitness data?"

Participants discussed these questions with their group mates for five minutes. By instructing them to engage in small-group discussions, we encouraged everyone to participate and think deeply about it. This provided opportunities for participants to express their opinions and thoughts. Indeed, pedagogical research has shown that, compared to simple lectures, asking people to discuss specific questions in small groups increases their engagement and retention of knowledge [38, 101]. Participants shared and debated their answers; they raised additional related questions and answers. The facilitator supervised this discussion. Subsequently,

the facilitator briefly presented the potential privacy threats caused by WAT-data sharing. The facilitator presented a summary of previous research, indicating that WAT data can be used to infer multiple sensitive information, such as activities [76], food, alcohol and drug consumption [15, 51, 78], health and mental health condition [26, 54, 66, 107], and personality traits [114]. Additionally, the facilitator presented media sources demonstrating the intention of certain organizations (e.g., government, business) to use this data to monitor the behavior of specific individuals [27, 86, 98].

3.3.3 Part III. Upgrading Knowledge (20 min). Participants need to have an accurate mental model of the WAT ecosystem before designing solutions for it. Therefore, we discussed the process of WAT-data sharing with TPAs and how the data-sharing environment works [80, 115]. Together with the participants, we reconstructed the data flow by asking them what the different entities are, what their relations are, and how the data is shared between them. We rectified any misconceptions among the participants At this juncture, we aimed to construct an accurate visual representation of the process on a flip chart. As active learning increases knowledge acquisition and performance [38], by involving everyone in this process, we increased their engagement to ensure they acquire a correct mental model of the ecosystem. However, as we wanted to provide them with only the correct model and needed the activity to be reasonably brief, we conducted it together. Also, to help the participants be at the same knowledge level and aware of the research problem, we briefly presented the current literature knowledge about users' behavior and their understanding of data sharing with third parties and the related threats [41, 102, 115].

3.3.4 Part IV. Sketching (70 min). We tasked each group with conceiving and proposing at least two solutions to enhance users' privacy concerning data sharing. Participants were instructed to: (1) Determine one or two specific problems (challenges) that they want to solve, (2) Imagine at least two new functionalities/solutions to fix the problems (i.e., either two solutions for one problem or two solutions for two problems), and (3) Draw sketches to visualize their solutions. Before sketching, we conducted a short presentation sharing tips and instructions about designs and how to sketch [46, 47] to ensure participants have basic information to sketch. Time permitting, we welcomed more solutions from each group. We provided the participants with large paper sheets (A3), sticky notes, colored pens, and markers. Each group worked separately, and there were no interactions between groups at this stage. The participants were encouraged to share their own experience with WAT data-sharing with others to raise the positive and negative points of their own experience with data sharing. From time to time, we visited the different tables to observe the progress of the activity, where facilitators asked a few questions, without too much interrupting or priming the participants. This enabled us to understand where participants were in defining their problem and/or the design of their solution. It also helped to check that participants understood the process and had no questions about what they were doing. Figures 8 and 7 in Appendix E demonstrate the sketching stage and the drawings produced by the corresponding groups.

3.3.5 Part V. Value Ranking (30 min). This activity aims to make the participants evaluate and provide feedback for each other's solutions. We asked the participants to present their sketches (i.e., individually or together) and discuss them with the other participants from different groups—in the same session. Each presentation (5 min) was in three phases: presentation, Q&A, and evaluation. Figure 9 in Appendix E shows participants during the presentation of one of their designs. After each presentation, participants were asked to evaluate the proposed solution regarding usability [14] (i.e., if such technology would be easy to use) and potential adoption [85] (i.e., if they would use such technology in everyday life if it exists). Adoption mostly refers to the likelihood of users indeed using the solution. They assigned grades on a five-point Likert Scale for each of these points. The grades were collected using an online form that the participants could access with their phones (i.e., with a URL address or by scanning a QR code). The evaluation was anonymous, and we just asked the participants to indicate if they were one of the designers of the same solution or not. The evaluation by the participants is directly related to the proposed solutions and not to the design features we later identified from the solutions. This evaluation provides us with insightful information about how the participants perceived the different proposed functionalities. After grading, one of the facilitators collected all the material (text and drawing) related to the presented design. The anonymity of the evaluation served to mitigate potential social biases that could influence the evaluation. Subsequently, we asked the participants if there were any comments or questions about the session, or information security & privacy in general, and we discussed them if necessary. Finally, each participant was paid in cash and signed a payment form upon leaving.

3.4 Data Analysis

We coded the sketches to identify design features from the various proposed solutions. Subsequently, we assessed these identified design features.

3.4.1 Coding. In total, we collected 19 solutions from three sessions, with each group proposing two designs, except for one group that proposed three. We used open coding [87] to categorize the multiple functionalities (i.e., design features) included in the different designs. Two researchers, who were the facilitators of the participatory design sessions, independently developed a codebook before exchanging their codes (henceforth Coder 1 and Coder 2). We noted a high overlap rate between the codes and design feature categories defined in the two codebooks. After comparing both codebooks, Coder 1 built a new final codebook by merging overlapping codes and designing feature categories, which was subsequently reviewed and refined by Coder 2. Finally, both coders reached an agreement on the coding. Table 2 in Appendix G summarizes the results of the coding with all the categories. In total, the final coding identified 16 distinct codes classified into seven themes. As they describe design features, and one specific design could implement multiple features, these codes and categories are non-exclusive. As a result, regarding their functionalities, each design could correspond to multiple design-feature categories.

3.4.2 Feature Evaluation. In addition to the evaluation of the design provided by the participants themselves (see Section 3.3.5) to provide a more in-depth perspective on how these solutions could

be implemented and used, we evaluated these different types of technologies (i.e., the pre-defined categories). We gathered around a table, and Coder 1 presented the features to the other researchers, including two researchers who did not take part in the coding. Coder 1 showcased a slide with the feature's name, a brief description, and representative examples from the drawings. We discussed the feature (5 minutes), with the opportunity for all of them to pose questions to the presenter. Finally, we (i.e., all researchers) provided comments (3 minutes), offering graded evaluations on a scale ranging from 1 to 5 points for feasibility (i.e., if it is feasible to develop the solution) and effectiveness (i.e., if it would be effective in protecting the users' privacy). The feasibility criteria refers to technical feasibility (i.e., is it easy to implement for the developers) but also more generally to the amount of effort for companies to implement a solution regarding other criteria (e.g., legal, financial). Following the grading, a free discussion ensued, encompassing comments on their evaluations, suggestions for improvement, and examples of similar designs implemented in different contexts. The meeting was recorded, and lasted approximately 90 minutes.

3.4.3 Score Analysis. For each design feature, we computed the mean and standard deviation of the scores for usability and adoption of all designs (rated by the participants). The rating given by the designers themselves were excluded from consideration, as their perspectives may be biased due to their vested interest in their designs performing well. Also, we computed the mean and standard deviation of the scores for feasibility and effectiveness (rated by the researchers).

4 PARTICIPATORY DESIGN OUTCOMES

Figure 1 shows seven features extracted after coding the 19 designs presented in the participatory design sessions. For each feature, we begin with a complete description of its functionalities. Then, if applicable, we provide examples of similar features that already exist in another context (e.g., mobile phone permissions, social networks), that usually help users to easily monitor what type of data is shared with which application. Next, we first present our own qualitative evaluation and then the quantitative evaluation rated by the participants and ourselves.

4.1 Feature 1 - Partial Sharing

Partial sharing enables WAT users to share only part of their data according to a specific time frame or a given context. Granting access to WAT data permits the TPAs to access every data of a specified type regardless of when the data has been collected by the device. In other words, a TPA can access WAT data that was collected before a user granted access. Using this feature, the user would be able to choose a specific data-collection time frame that they want to share (excluding the others). PARTIAL SHARING was present in three different designs proposed by the participants. Whereas one of the designs allows users to select a time frame by indicating dates, another one simply enables the user to choose between sharing all the data or only the data that has been collected since the access was granted. In a different approach, the third design (see Figure 11 in Appendix F) is context-aware, allowing users to indicate the data type and the activity type they would want to share (e.g., sharing only the heart rate data that were collected while running). This last design also proposes a "start sharing" feature that the user could enable and disable to select the time frame during which the data is shared (and only the data collected during this specific time frame). This feature shares some similarities with the so-called run-time permission of Android [11]. However, whereas in this case, Android may only allow an app to access a given data source (e.g., GPS, camera) while this app is running, in the case of WATs, this will not prevent the TPA from accessing all the collected data for a given type (e.g., all the step count) as the API key does not currently allow access to be limited to a certain timeframe (as proposed by PARTIAL SHARING). This feature should be implemented by the service providers (e.g., Apple or Fitbit).

This feature is promising to address one of the issues detected in previous work, that is users' misunderstanding that when they grant access to their data, they also grant access to data that was collected in the past [115]. However, we think that this feature may be a bit restrictive, and we can propose more functionalities than only basing the access control on time, like the possibility for the users to choose with which granularity they want to share the data (e.g., the step counts for each minute, hour, or day).
Regarding the scores, this feature received the second-highest score for feasibility (4.75) and effectiveness (4.00). As for the evaluations by the participants, this feature received the second-highest score for adoption (4.12) and usability (4.41). Therefore, we can affirm that, with all scores above 4, this feature is particularly appreciated.

4.2 Feature 2 - Visualization

Such solutions aim to enhance users' understanding of their sharing behavior by designing new visualization tools. These tools can help the users explore the shared data and the different related TPAs by classifying them either by data type or by TPAs. Some proposed visualization features also allow users to keep track of all shared data through a logging system and by displaying an accurate data-sharing history. Additionally, this feature aids users in tracking their behavior toward sharing by presenting specific statistics about their usage of the different TPA services that are installed on their phones. VISUALIZATION was present in five different designs. Currently, most platforms allow users to check a list of connected TPAs (see Figure 14a in Appendix F). However, no companion app provides a list of TPAs classified based on the type of shared data. This feature should be implemented by service providers. An example of VISUALIZATION, in a different context, is available on iOS and Android for access management of mobile applications (see Figure 14b in Appendix F). The behavioral and log statistics feature is also similar to the macOS screen time.[3]

The weakest aspect of VISUALIZATION is effectiveness. Indeed, one of the main drawbacks of this approach is that it may not be highly effective. Whereas it may lead to a change or increase awareness of the users, the mechanism itself is not directly protecting privacy. Therefore, we gave this feature a low score for effectiveness (3.00). However, feasibility received the second-highest score (4.75, tied with three other features). In terms of evaluation by the participants, this feature did not receive a high score for adoption (3.82); however, it received a decent score for usability (4.21). We

[3] https://support.apple.com/en-us/HT210387, Last accessed May 2024.

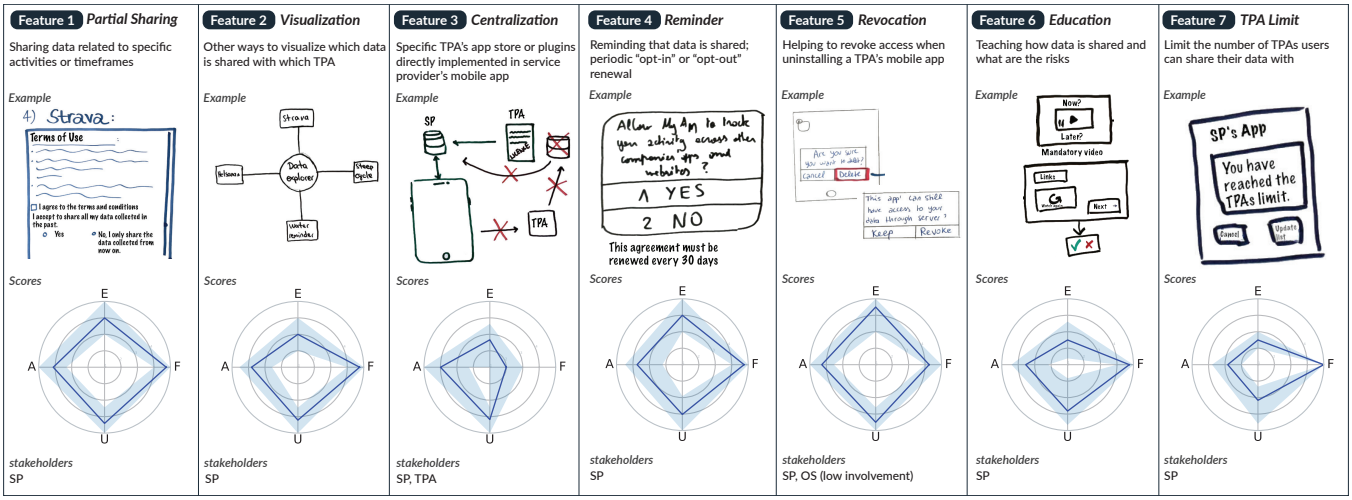


Figure 1: Presentation of the seven identified design features. For each, we provide a title, a short definition, a translated example sketch, examples from different contexts, the result of our evaluation and that by the participants (means and standard deviation on a five-point Likert Scale), and the stakeholders who should take action to implement the design. E, F, U, and A stands for *effectiveness*, *feasibility*, *usability*, and *adoption*, respectively. Note that E and F are graded by the authors during the data analysis, but U and A are graded by the participants during the session. SP, TPA, and OS stands for *service provider*, *third-party app operator*, and *operating system*, respectively.

believe that such a solution might be perceived as useful, and multiple WAT users might be interested in accessing information about their data sharing. However, most of the users will probably not use it, as they would need to actively check a dedicated section in the service provider's mobile app, which is already quite complex. Indeed, previous research on online social networks and Android permissions has shown that most of the users never update or even check their privacy settings [36, 49].

4.3 Feature 3 - Centralization

Centralization is not a new feature but rather a solution that guarantees secure data sharing among users. Two different solutions were proposed. The first solution suggests that the main service provider should have its own TPA app store. Any TPA interested in offering services in the app store would first need to obtain approval from the main service provider. This approval would serve as a guarantee to users that the TPA will confidentially and securely process their data, assuring that their privacy will not be compromised. In a slightly different context, a known example of this feature is Google Play's privacy labels[4] (or data safety section), allowing developers to disclose information about their app's data collection, sharing, and security measures. The second proposed method is to eliminate the possibility of sharing users' data with TPAs and replace it with a plugin system directly integrated into the main application. This solution would guarantee that the users' data would not be stored on the TPA's server at any moment, as the main service provider would remain the data-processing entity. CENTRALIZATION was incorporated into three different designs. This solution would necessitate active participation from service providers and TPA companies.

[4]https://blog.google/products/google-play/data-safety/, Last accessed May 2024.

The positive aspect of this feature is that a dedicated store would force TPAs to be more transparent about what they do with the data. However, regarding the plugin solution, we highly doubt that such a solution can be put in place. We therefore gave this feature by far the lowest evaluation for feasibility (2.00), and the second-lowest score for effectiveness (2.67). As for adoption and usability, it received average scores (4.00, and 4.18, respectively).

4.4 Feature 4 - Reminders

REMINDER is designed to address the well-known problem of users forgetting to revoke access [99, 115] by proposing notification reminders. Such a system could simply remind users periodically that they are sharing their data with TPAs. Multiple designs propose further engaging features by directly asking the users to renew the previously granted access (i.e., to opt-in again) or by asking them if they want to revoke it (i.e., to opt-out). Similar reminder mechanisms were implemented in other contexts. For example, Facebook implemented a privacy checkup system [33] to periodically remind users about the app they share their data with and ask them if they want to revise the access authorizations. This feature could be implemented by service providers. REMINDER was present in seven solutions. Figure 12 in Appendix F depicts one of the examples.

Whereas this feature would not solve all privacy issues, it solves the problem of forgetting and is highly likely to be used, as already shown by previous research [115]. This feature received the second highest score for feasibility (4.75) and effectiveness (4.00), and even if the mean score for usability (4.03) is not one of the highest, it is greater than 4, which is a decent score. As the score of adoption (3.75) is slightly lower than 4, we would recommend implementing that feature with an option to disable it or choosing the reminder frequency to avoid bothering users who do not want to use it.

4.5 Feature 5 - Revocation Assistance

This feature assists users in revoking data access. Two of the related proposed solutions include features for directly asking the user if they want to revoke access to their data when they *uninstall* a TPA's mobile app from their phone. This feature is relevant because some users would be concerned about their data being deleted after uninstalling TPAs [115]. REVOCATION ASSISTANCE was present in three different designs. One of these designs also includes an automatic data-revocation option for when a TPA's mobile app is not used for a while. A similar technique was implemented by Google on Android phones called "Remove permissions for unused apps"[5] to automatically remove permissions for apps than you did not use for a certain amount of time. The third design implements an option for directly sending a message to the TPA's company to ask them to delete any related data that are stored on their servers. This feature is supported by Article 17 of the General Data Protection Regulation (GDPR) about the "right to be forgotten."[6] Figure 13 in Appendix F is one of the designs implementing a feature that would enable revoking access while uninstalling a TPA's mobile app on the phone. Service providers should implement this feature, and depending on the specific version of the feature, it may also require the involvement of the company that provides the OS of the phone (e.g., sending a revoking request when uninstalling the app). This feature is slightly similar to the option provided by Android to remove permission of unused apps [10]. However, implementing such automatic data access revocation for TPA would raise new privacy issues. Indeed, even if the service provider (e.g. Fitbit) has access to the API access logs, it does not have access to the mobile app usage logs, and thus can not precisely know which are or are not used. The operating systems of the smartphone should therefore allow the service provider (e.g. Fitbit) to have access to the data usage logs to verify which TPAs are no longer used. Furthermore, the option to automatically send a data removal request to the TPA company could also be imposed by law, as it refers to GDPR.

This feature is very promising as it would increase privacy overall without decreasing utility. This feature received the highest score for effectiveness (4.50) and a decent score for feasibility (4.50). It also received the highest mean scores for adoption (4.28) and usability (4.50). Except for feasibility (for which it still received a decent mean score), this feature is the best-rated one.

4.6 Feature 6 - Education & Sensitization

Participants proposed adding a tutorial or awareness-raising video during the data-sharing process. Such a video would serve as an educational tool to encourage users to be mindful and considerate about the consequences of WAT data sharing, hoping it can be more effective than the typical text-based "terms of services." Earlier literature showed that users usually would skip reading such text-based privacy notices [84]. REMINDER was present in four different designs. One of the designs proposes to show a short video to the user to explain how data-sharing works and what are the multiple related risks to their privacy. This design also specifies that after watching the video, the users would have to answer a short quiz, and if they fail, they could not share their data. The fourth design aims to implement an informative and interactive consent form, enabling the users to click on different links to obtain more information about how their data is processed. This feature should be implemented by the service provider or by the TPA's company. The use of educational videos as privacy-preserving interventions has been proposed in various contexts, such as for multiparty privacy conflicts on social media [108]. Also, trading apps usually offer brief training when users create an account.[7]

We believe forcing users to watch a video is challenging because they could be doing something else while the video is playing. Besides the possibility of refraining from watching enforced videos, we also think that such interventions harm the sense of gratification that users would perceive when using a new technology. Indeed, when users install a TPA, they usually want to test it immediately, and their interest in tutorial videos is probably modest. Despite a decent score in feasibility (4.75), REMINDER received the lowest score for effectiveness (2.50). Furthermore, it received the second-lowest score for adoption (3.55) and usability (3.82).

4.7 Feature 7 - TPAs Limit

This feature aims to limit the number of TPAs the users can share their data with. If a user wants to share their data with a new TPA and this number is already reached, they will first have to revoke a previously granted access. Only one design implements this feature. This feature should be implemented by the service provider. Such a limitation is implemented, for example, WhatsApp that permits linking an account to only four different devices at the same time (see Figure 10 in Appendix F).[8]

We believe that users would not like any feature that limits their choices. Thus, if that feature could be enabled or disabled, most of them would probably disable it the first time they get prevented from installing something. This feature received a low score for effectiveness (2.50). Indeed, even if the feature of having a limited number of TPAs with which users can share their data would certainly increase users' privacy, users would not like it and would not want such a feature to be implemented. Furthermore, users could simply revoke/grant access multiple times, which does not help them. Considering the simplicity of this feature, it received the highest mean score for feasibility (5.00). As for the evaluation by the participants, this feature also received the lowest mean score for adoption (2.83) and usability (3.17).

5 DISCUSSION ON PROPOSED FEATURES

We investigated the widespread problem of user data-sharing in the context of third-party applications (TPAs) and wearable activity trackers (WATs). Through participatory design sessions, our participants provided us with multiple designs to help users better manage their WAT-data sharing and protect their privacy. These proposed solutions offer novel insights into the future design and development of privacy-enhancing technologies for WAT-data sharing with TPAs. In the following sections, we further discuss these

[5] https://support.google.com/android/answer/9431959?hl=en#zippy=%2Cautomatically-remove-permissions-for-unused-apps, Last accessed May 2024.

[6] https://gdpr.eu/right-to-be-forgotten/#:~:text=In%20Article%2017%2C%20the%20GDPR,originally%20collected%20or%20processed%20it, Last accessed May 2024.

[7] https://www.degiro.ch/helpdesk/en/trading-possibilities/why-do-i-have-complete-test-i-can-trade-product, Last accessed May 2024.

[8] https://faq.whatsapp.com/378279804439436/?helpref=uf_share, Last accessed May 2024.

findings, including their limitations and technical feasibility, and envision possible combinations of these solutions to build effective PETs.

Enabling the users to **share selectively based on context, or specific timeframes** (i.e., which data and activity type they want to share regarding the time it was collected or the corresponding activity) could address one major misunderstanding regarding data sharing. Users tend to think that they only share the data that was collected from the moment they granted access authorization. This is not the case; once a TPA has access to a user's given type of data (e.g., step-count, heart-rate), they can access all data corresponding to this type, regardless of when it was collected [115]. Furthermore, it could likely increase user privacy by substantially reducing the amount of personal data[9] that a potential adversary would have access to. As suggested during the evaluation by the authors, it could be particularly interesting to also limit the amount of shared information by allowing users to share aggregated data. Indeed, previous research already discussed options to share data aggregated over time (e.g., aggregating the data series by the day) [30] and showed that it is an effective technique for mitigating inference attacks [114] and is likely to be adopted by a large number of WAT users [115]. However, this study is, to our knowledge, the first the highlight the need for partial sharing regarding a specific context or timeframe, which was highlighted through the use of a user-centered approach.

Mechanisms such as **reminder notifications** and "opt-out" or "opt-in" access-authorization renewal were also evaluated as having high usability and effectiveness (especially according to the evaluation by the authors). An advantage of such solutions is their feasibility to develop them without many technical challenges. A similar feature was also proposed and evaluated in previous research [115], showing that WAT users are particularly inclined to use reminder notifications. However, we recommend implementing only "opt-out" renewal, as "opt-in" could cause utility issues because such a feature would revoke the access if the user ignores the message. The user should be able to choose the frequency of such notifications or disable them, for example, by checking a box that appears with the notification (e.g., "don't ask me again"). Furthermore, the design of reminder notifications could be utilized from statistics about the number of data requests for each TPA (i.e., how many times a particular TPA accesses their data, and what type of data). Such information is available to the service provider as a TPA generally accesses user data using a dedicated API. Using such statistics in the design could raise awareness among the users about the amount of data that they actually share. However, the risk of using statistics is that the TPAs may game the system and increase the number of data requests just to show that the user actively uses the service. This could undermine the feature's intended purpose.

The feature allowing users to **revoke data access** when uninstalling a TPA's mobile app or asking a TPA's company to remove data from their servers received the most positive feedback from the participants and us. Therefore, we find that such a protection mechanism should be implemented. Indeed, as multiple WAT service providers implement data access for TPAs by using API keys or access tokens (e.g., using protocols such as OAuth [21]), it might not be clear for users that the access authorization is not necessarily revoked when they delete a TPA's mobile app from their phone and that the TPA can still access their data from server to server. Solutions in REVOCATION ASSISTANCE could not only remind the users to revoke the access but also teach them that they must do it if they want to stop sharing their data with a given TPA. Furthermore, a feature to help WAT users ask a TPA's company to remove data from their servers is not only a particularly good feature for increasing privacy but a means of complying with Article 17 of the GDPR: *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have an obligation to erase personal data without undue delay [...]"* [100]. However, simple notifications, as suggested in REMINDER, would be preferable to automatic revocation, as the former could cause utility issues (e.g., an access authorization being removed without the user noticing).

We would therefor propose a multi-dimensional approach comprising PARTIAL SHARING, REMINDER, and REVOCATION ASSISTANCE to help WAT users better manage data sharing. It implements partial sharing (i.e., timeframe, context, and temporal aggregation), periodical reminders with "opt-out" renewal (i.e., the user has to revoke the access actively) as well as a disabling option, and an option to revoke access authorization when uninstalling the TPA's mobile app from the phone as well as the option to send an automatic data removal request to the corresponding company. Figure 2 illustrates the workflow of WAT-data sharing and outlines the distinct features that we recommend. The workflow, informed by prior literature on WATs, encompasses three primary phases in the utilization of TPAs (and consequently the data exchange with them): (1) adoption (i.e., when users initiate the use of WATs) [31, 81], (2) adherence (i.e., the period during which users continue using WATs) [97], and (3) abandonment (i.e., when users cease using WATs) [19, 34]. During the adoption step, a given user contemplates using a TPA, usually installing the corresponding mobile app on their phone, and sharing their data with the TPA. To do so, the user usually can select the type of data they want to share (e.g., step count, heart rate, activities) and has to agree to share their data, generally by tapping/clicking on an "accept" button. In that step, we propose partial sharing (i.e., PARTIAL SHARING), offering the user a different option to share more specific data regarding context and timeframe, and to only share aggregated data. Implementing such a feature early in the process is important as the TPA will have access to all data for a given type as soon as the user accepts to share. The user interface of such a multi-aspect partial sharing feature is out of the scope of our work and should be investigated in future studies. During the adherence step of the data-sharing process, the user passively shares their data to a given TPA by just wearing the TPA and potentially using the corresponding mobile app. We still propose partial sharing, in this step, as the user may want to modify them, either to share more or less data and adjust the privacy risks. Additionally, we suggest reminding the user, helping them not forget about the previously granted access to their data, and the fact that they can revoke this authorization. In the abandonment step, REVOCATION ASSISTANCE assists the user in revoking previously granted access when they uninstall or remove the TPA mobile app from their phone, and reminds the user that they can request the

[9]Following the concept of data minimization: https://edps.europa.eu/data-protection/data-protection/glossary/d_en, Last accessed May 2024.

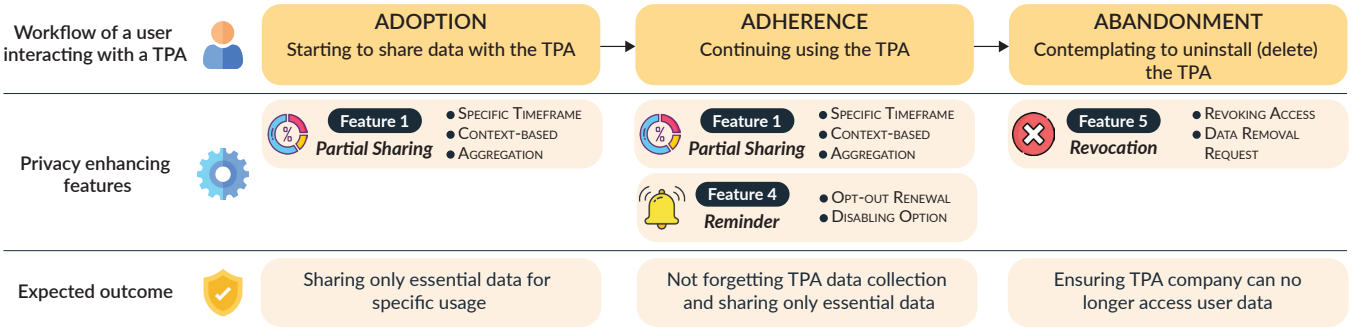


Figure 2: An example of meta-solution for TPA privacy – Top: A typical workflow of a user interacting with a TPA; Middle: Privacy-enhancing features; Bottom: Expected outcomes

corresponding company to delete their data, including personally identifiable information and WAT data, according to the GDPR.

This proposition of meta-solution corresponds to a privacy-by-control approach in the sense that it offers the users more options to decide which data they want to share, which they do not, and to which they no longer want the TPA company to have access. We believe that this solution would be highly effective in giving users more control over what data they do or do not want to share (and with whom), and that it would go a long way in reducing the risks to their privacy (particularly related to the inference of other sensitive data [74, 112, 114]), but also to reduce their concerns about using WATs. Furthermore, even if this specific study is focused on WAT data sharing, the solution we propose can be implemented, at least partially, in every type of API-based data-sharing system. Indeed, features such as time-framed partial sharing or reminders are not specific to WAT data. However, this solution cannot help the user in case of a data breach, once their data is shared, they can have no (technical) guarantee that any third parties will not keep, share, or use the data without their consent.

Such a more global solution requires almost exclusively the service provider to be involved, which makes them the primary stakeholder, allowing users to increase their privacy. This is an advantage for users or any other party (e.g., a legal authority), as they would not need to request new features from multiple third parties, but only from a single entity (the service provider), requiring less effort on their end. Recognizing that the presented solution is just one manifestation of the diverse set of potential design configurations is essential. The participatory approach we took uncovered a range of innovative design features, each with the potential to enhance user privacy in distinct ways. Thus, other combinations and arrangements of these features have the potential to produce equally effective solutions. Having said that, some of the proposed ideas require more consideration. For example, a particularly drastic one would be to store data directly only on the WAT or the smartphone and block any transmission of the data. However, this could lead to severe drawbacks for utility, as these devices (especially the WAT) have very limited computing and storage capacities.

Finally, it is essential to note that multiple proposed solutions have similar already existing solutions in other contexts, e.g., Facebook Privacy-Checkup [33] or Android run-time permission [11], as discussed in Sections 2 and 4. However, this does not constitute a problem in terms of the novelty and relevance of the design proposition; it may even have been a source of inspiration for participants. Furthermore, the fact that there are similar solutions for other types of technology can only increase the necessity of their implementation in the context of WAT and additionally show their feasibility. In this context, developing such solutions would require additional work as the data types are different (e.g., time series). Furthermore, as WATs consist of particular devices and data environments, users' needs in terms of usability and utility could also be different, hence the importance of user-centered approaches as ours.

6 EVALUATION OF SELECTED FEATURES

After classifying and evaluating the various proposed features, we found that a general solution combining PARTIAL SHARING, REMINDER, and REVOCATION ASSISTANCE would constitute a promising tool to help WAT users effectively protect their privacy. Indeed, all three have at least three of the four evaluated aspects (either by the participants or by us) that receive a score of at least 4 (the other features have only two or less).

6.1 Survey Methodology

To better understand users' assessment of these features, we deployed an online survey with WAT users. This evaluation serves two purposes: First, it facilitates the understanding of the potential effectiveness and usability of such features; Second, it complements the results of our participatory design study with the perspective of a more diverse sample, in terms of age and educational background.

We recruited the respondents through Prolific. We first deployed a screener survey (with four questions) to 1000 respondents, asking them about the brand of their WAT, the frequency of using WAT (per week), and the experience of sharing data with TPA. Next, we contacted 454 respondents who were (1) fluent in English, (2) owned an Apple Watch, Fitbit, or Garmin, (3) wore their WAT at least five days per week, (4) shared their data with at least one TPA, and (5) had an approval rate of at least 95% in Prolific (indicating they were reliable respondents). The respondents were paid 0.1 GBP (~ 0.13 USD) for answering the screener survey.

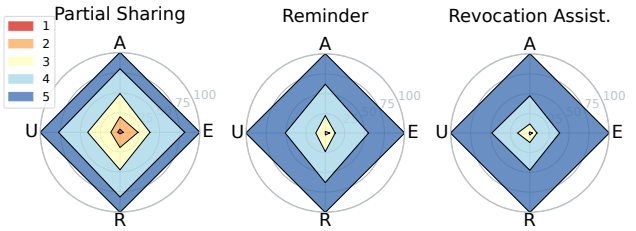


Figure 3: Distribution (in %) of the five-point Likert scale evaluation for reported Adoption (A), Effectiveness (E), Recommendation likelihood (R), and Usability (U) by survey respondents. For example, for E, red and dark blue corresponds to *"not at all effective"* and *"extremely effective"*, respectively.

The questionnaire was designed to take around 20 minutes to complete.[10] The survey started with a consent form. In the next section, the respondents were asked about their WAT usage behavior. The main part of the survey included descriptions of the three best-evaluated features in Section 4 (PARTIAL SHARING, REMINDER, and REVOCATION ASSISTANCE) and their mock-ups as examples (i.e., available in the OSF repository). For each of the three features, we asked respondents to report *usage likelihood* (adoption), *perceived effectiveness* for privacy improvement, potential *ease of use* (usability), and *recommendation* potential (a.k.a. net promoter score or NPS) of this feature, using a five-point Likert scale. However, unlike previous evaluations, we did not assess feasibility, as it would be more for developers or experts than for the users to evaluate such an aspect. Furthermore, for each feature, we asked a general open-ended question to gather additional comments or suggestions (including pros and cons).

Our IRB approved the study. Before launching the survey, we performed in-person cognitive pretests to identify any issues with its designs. We invited two non-project researchers from the first author's institution who were WAT users. During the test, we slightly improved the phrasing of the descriptions and revised the open-ended questions. We also used two attention-check questions in the survey and used the open-ended questions as a proxy to evaluate the quality of the respondents's answers [73]. To compensate for the respondents' effort, each received 4 GBP (~ 5.1 USD).

6.1.1 General Statistics. Initially, we collected 209 responses. We excluded eight responses due to being incomplete or failing to respond to attention checks and open-ended questions. In total, we report the answer of $N = 201$ WAT users including 55.7% of men, 43.8% of women, and 0.5% (1 individual) who preferred not to answer. They were aged from 19 to 73 with a mean of 40 ($SD = 12$). As for their device usage, 43% were Apple users, 36% Fitbit users, and 21% Garmin users. Only 1.9% were using their device for less than one month, while 20.4% used it for one month to one year, 28.9% used it from one to three years, 26.4% from three to five years, and 22.4% for more than five years. Finally, they wear their devices for an average of 6.7 days a week ($SD = 0.8$).

6.2 Survey Findings and Discussion

We used the affinity diagramming method[11] to inductively analyze the open-ended answers. The rest of the answers are reported using descriptive statistics. In addition to the mean scores reported hereafter, Figure 3 illustrates the distribution of the five-point Likert scale evaluations for the three features. Overall, REVOCATION ASSISTANCE and REMINDER features received more favorable scores than PARTIAL SHARING. Interestingly, the evaluations across all features showed remarkable consistency, with each feature receiving similar scores for their respective metrics. We will now provide a detailed elaboration on the findings for each feature. According to the survey's respondents evaluation, REVOCATION ASSISTANCE received the best feedback for adoption ($M = 4.5$), effectiveness ($M = 4.4$), and recommendation ($M = 4.4$). As for usability, it received a slightly lower score ($M = 4.3$). The majority of respondents discussed the perceived benefits of REVOCATION ASSISTANCE, particularly emphasizing its ability to highlight a common **misunderstanding** that uninstalling an app does not automatically revoke data access. A 26-year-old woman, Apple user, captured this sentiment, stating, *"I didn't realize that this happened so this feature would be incredible!"* This **realization** was seen as the main advantage of the feature, ensuring users are informed and can prevent unintentional sharing after TPA uninstallation. Other highlighted benefits included the feature's ability to facilitate seamless data deletion, save time, and provide an extra layer of protection, which contributes to a sense of confidence in sharing, and control. However, there were calls for **further assurances** that data deletion requests are indeed executed, with some respondents expressing the need for regulatory monitoring to ensure compliance. Additionally, the feature was recognized as useful for users **transitioning to new devices**, ensuring continuity of data and access (i.e., by not revoking access when uninstalling TPA in the old device). The respondents also noted the importance of clear communication about the implications of data deletion on service continuity. Lastly, some respondents found the feature easy to find as it is **integrated into the uninstallation process**, simplifying its use. Same as REVOCATION ASSISTANCE, REMINDER also received overall high scores (i.e., both greater than 4 for all measured aspects) for adoption ($M = 4.3$), effectiveness ($M = 4.1$), usability ($M = 4.4$), and recommendation ($M = 4.1$). Respondents acknowledged the usefulness of reminder notifications in **effortlessly monitoring** TPA permissions. They also highlighted their impact in **mitigating forgetfulness** and adapting to changes in user preferences over time. The **familiarity** of notifications was also seen as a positive aspect, providing an easy and recognizable way to stay informed. However, there was a concern about becoming **habituated** to frequent reminders, with some noting the risk of missing important alerts due to the many notifications they receive. Respondents suggested the option to **customize the frequency** of reminders to address this issue. A 34-year-old man, Garmin user, stated, *"This is good, but some people may find it annoying - having the option to set how regularly this appears would be helpful here."* Beyond the notifications, there were calls for a more actionable approach, with suggestions for notifications to include direct links

[10] The script of the survey questionnaire is available in https://dx.doi.org/10.17605/OSF.IO/UEC85.
[11] https://www.nngroup.com/articles/affinity-diagram/, Last accessed May 2024.

to a detailed and user-friendly interface for revoking TPA access and for the content of the reminders to list the relevant TPAs. As for PARTIAL SHARING, it globally received lower scores for adoption ($M = 3.5$), effectiveness ($M = 3.5$), usability ($M = 3.7$), and recommendation ($M = 3.5$). Many respondents appreciated the **control** PARTIAL SHARING offers, emphasizing its value in selective sharing based on context and time, reducing uncertainty and enhancing trust. However, several respondents highlighted the **complexity of configuring** PARTIAL SHARING, noting that deciding what data to share requires significant cognitive effort. A 32-year-old woman, Fitbit user, remarked, *"This looks a bit more complex to use, not sure if I would go in and specifically use this to change features. I would prefer to just have a blanket approach."* Also, some discussed the potential for this privacy focus to **compromise the utility** of TPAs, indicating a challenging balance. To ease usability, respondents suggested introducing **predefined data sharing levels**—basic, moderate, and extreme—with explanations about the risks of sharing particular data types. They also proposed a **renewal** option to allow users to adjust their preferences over time, thus making the feature more user-friendly and straightforward. Lastly, several respondents recognized the benefits of combining the features to create a unified privacy management system. This aligns with our earlier proposal (see Figure 2). Some users suggested merging REMINDER with PARTIAL SHARING or REVOCATION ASSISTANCE to receive timely alerts during the adherence phase to enhance their awareness of data sharing before deciding to delete a TPA (i.e., abandonment phase). A 51-year-old woman, Fitbit user, highlighted, *"This is useful, but not as useful as the previous reminder - I would value being reminded that I am sharing data well before the point where I delete an app."* Such an **integrated** approach would ensure users are continually informed and can make proactive decisions about their privacy throughout the TPA's lifecycle.

7 LIMITATIONS AND FUTURE WORK

This work has certain limitations. First, the sample of the participatory design study is not representative of WAT users in terms of age, educational background, and WAT brand. For example, Fitbit is known for being more permissive regarding TPAs, whereas Apple users are accustomed to a more closed environment. In particular, Apple Health does not have a web API, only a local API. Therefore, recruiting more participants who use devices from other brands and with more representative demographics would likely have resulted in more diverse design proposals. We attempted to compensate for this limitation by designing the online survey to be highly diverse, which validates results for a representative sample. Secondly, participants evaluated each design as a whole rather than evaluating the design features or individual proposed features separately. Multiple designs included various features but were assessed as holistic solutions. Therefore, while this approach allowed us to draw general conclusions, the participants' evaluations do not precisely reflect how they would have evaluated each category individually. In contrast, with the authors, evaluations were conducted for each category individually. Additionally, aspects such as usability or adoption require more comprehensive investigations. In this work, we only assessed users' *perceptions* of the potential usability and adoption of each solution. Thirdly, as we conducted multiple participatory design sessions, not all participants evaluated all designs. Fourthly, we lack qualitative feedback from the participants. Although we encouraged them to engage in discussion after each presentation, they primarily asked questions to ensure they correctly understood the design. Very few participants offered remarks about their appreciation of the presented design. Lastly, we do not propose highly technical solutions and focus mainly on user-centered solutions. However, the main goal of the study is to ensure diversity among the proposed solutions and increase the chances of finding ideas that developers or people with a more technical background would not necessarily have thought of and at the same time guarantee high acceptability of the proposed solutions among the general public. For that purpose, it was also important to us that the users come with their technical background related to PETs as is, that is why we only educated them about the data-sharing ecosystem and not about information security. Advanced technical solutions are therefore outside of the scope of this study. Also, we can note that the most technical proposed solution (e.g., PARTIAL SHARING) received the lowest scores in our survey evaluation as it was perceived as too complex by respondents.

For future work, we plan to further develop the proposed solutions, and evaluate their effectiveness through in-the-lab user studies. We also intend to implement and deploy such tools to test their effectiveness in longitudinal in-the-wild user environments. Such a study could help us understand how users can adopt and use such a solution to protect WAT users' privacy. Another interesting study could be conducted on WAT companion-app developers and/or companies to better understand their motivations and to what extent they would consider implementing such functionalities. Finally, we should actively follow the new data-sharing trends in the WAT market, as well as the corresponding functionalities, to observe if new privacy-enhancing technologies are indeed implemented and to study potential new data-sharing behaviors that could be harmful to privacy.

8 CONCLUSION

In this article, we report a participatory design study conducted with $N = 26$ WAT users to design new features that could help WAT users better manage data sharing and thereby, increase their privacy. We have classified the 19 different designs proposed by the participants into seven different feature categories. We have described and evaluated these categories, combining our evaluations with the participants' evaluations. We have used this information along with other protection mechanism ideas previously proposed in research [30, 102, 114, 115], to formulate a comprehensive solution that, in our opinion, would be highly effective in enhancing WAT users' privacy while maintaining a decent level of feasibility, usability, and adoption. We then conducted a survey study with $N = 201$ WAT users to evaluate the potential of these solutions. We suggest combining three of the seven previously designed features: PARTIAL SHARING, REMINDER, and REVOCATION ASSISTANCE, along with an additional feature of temporal aggregation informed by previous research [30, 114, 115]. Our work contributes to the privacy field related to WATs by describing and evaluating efficient solutions to help WAT users better manage their data sharing with TPAs and provide them with new functionalities for fine-grained sharing.

Such a solution would increase WAT privacy while maintaining a decent level of utility.

ACKNOWLEDGMENTS

This work was partially funded by the Swiss National Science Foundation with Grant #200021_178978 (PrivateLife) and by an HEC Research Fund. We thank Holly Cogliati and Vincent Vandersluis for proofreading this article and Lahari Goswami for providing valuable comments on the writing. We also thank Alpha Diallo, Yamane El Zein, Neele Roch, and Lorin Schöni for participating in the cognitive pre-tests for the design sessions and the survey. Finally, we thank Arnaud Bonvin for his support in facilitating the design sessions.

REFERENCES

[1] Reem Abdel-Salam, Rana Mostafa, and Mayada Hadhood. 2021. Human Activity Recognition Using Wearable Sensors: Review, Challenges, Evaluation Benchmark. *Deep Learning for Human Activity Recognition* (2021), 1–15. https://doi.org/10.1007/978-981-16-0575-8_1

[2] Daniel A. Adler, Vincent W.-S. Tseng, Gengmo Qi, Joseph Scarpa, Srijan Sen, and Tanzeem Choudhury. 2021. Identifying Mobile Sensing Indicators of Stress-Resilience. In *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, Vol. 5. 1–32. https://doi.org/10.1145/3463528

[3] Seyed Hossein Ahmadinejad, Philip W.L. Fong, and Reihaneh Safavi-Naini. 2016. Privacy and Utility of Inference Control Mechanisms for Social Computing Applications. In *Proc. of the ACM on Asia Conf. on Computer and Communications Security (AsiaCCS)*. ACM, 829–840. https://doi.org/10.1145/2897845.2897878

[4] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. 2017. Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proc. of the Multimedia Privacy and Security (MPS)*. ACM, 1–11. https://doi.org/10.1145/3137616.3137617

[5] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. In *Proc. of the ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 787–796. https://doi.org/10.1145/2702123.2702210

[6] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. 421–434. https://www.usenix.org/conference/soups2019/presentation/alqhatani

[7] Abdulmajeed Alqhatani and Heather R Lipford. 2021. Exploring The Design Space of Sharing and Privacy Mechanisms in Wearable Fitness Platforms. In *NDSS Workshop on Usable Security and Privacy*.

[8] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J. Wisniewski. 2022. Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI) (CHI '22)*. ACM, 1–18. https://doi.org/10.1145/3491102.3517652

[9] Sarah L. Alvarez, Stephanie L. Baller, and Anthony Walton. 2021. Who Owns Your Health Data? Two Interventions Addressing Data of Wearable Health Devices among Young Adults and Future Health Clinicians. *Journal of Consumer Health on the Internet* 25, 1 (Jan. 2021), 35–49. https://doi.org/10.1080/15398285.2020.1852386

[10] Android. 2023. Android 12. https://www.android.com/android-12/

[11] Android. 2023. Request runtime permissions. https://developer.android.com/training/permissions/requesting

[12] Pauline Anthonysamy, Awais Rashid, James Walkerdine, Phil Greenwood, and Georgios Larkou. 2012. Collaborative privacy management for third-party applications in online social networks. In *Proc. of the workshop on Privacy and Security in Online Social Media (PSOSM)*. ACM, 1–4. https://doi.org/10.1145/2185354.2185359

[13] Patricia Arias-Cabarcos, Saina Khalili, and Thorsten Strufe. 2022. 'Surprised, Shocked, Worried': User Reactions to Facebook Data Collection from Third Parties. https://doi.org/10.48550/arXiv.2209.08048

[14] Raquel Benbunan-Fich. 2017. Usability of Wearables without Affordances. *Americas Conference on Information Systems* (2017).

[15] Joan-Isaac Biel, Nathalie Martin, David Labbe, and Daniel Gatica-Perez. 2018. Bites'n'Bits: Inferring Eating Behavior from Contextual Mobile Data. In *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, Vol. 1. 125:1–125:33. https://doi.org/10.1145/3161161

[16] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. 2017. Exploring decision making with Android's runtime permission dialogs using in-context surveys. 195–210. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bonne

[17] Weicheng Cao, Chunqiu Xia, Sai Teja Peddinti, David Lie, Nina Taft, and Lisa M. Austin. 2021. A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. In *Proc. of the USENIX Security Symp.* 803–820. https://www.usenix.org/conference/usenixsecurity21/presentation/cao-weicheng

[18] Yuan Cheng, Jaehong Park, and Ravi Sandhu. 2013. Preserving user privacy from third-party applications in online social networks. In *Proc. of the Int'l Conf. on World Wide Web - WWW Companion*. ACM Press, 723–728. https://doi.org/10.1145/2487788.2488032

[19] James Clawson, Jessica A. Pater, Andrew D. Miller, Elizabeth D. Mynatt, and Lena Mamykina. 2015. No longer wearing: investigating the abandonment of personal health-tracking technologies on craigslist. In *Conference on Pervasive and Ubiquitous Computing (UbiComp)*. ACM, 647–658. https://doi.org/10.1145/2750858.2807554

[20] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1–13. https://doi.org/10.1145/3313831.3376389

[21] Blaine Cook and Chris Messina. 2012. OAuth 2.0 — OAuth. https://oauth.net/2/

[22] SR Davis, D Peters, RA Calvo, SM Sawyer, JM Foster, and L Smith. 2018. "Kiss myAsthma": Using a participatory design approach to develop a self-management app with young people with asthma. *Journal of Asthma* 55, 9 (Sept. 2018), 1018–1027. https://doi.org/10.1080/02770903.2017.1388391

[23] Jaime Delgado, Eva Rodríguez, and Silvia Llorente. 2010. User's privacy in applications provided through social networks. In *Proc. of the SIGMM workshop on Social media (WSM)*. ACM, 39. https://doi.org/10.1145/1878151.1878163

[24] Michalis Diamantaris, Elias P. Papadopoulos, Evangelos P. Markatos, Sotiris Ioannidis, and Jason Polakis. 2019. REAPER: Real-time App Analysis for Augmenting the Android Permission System. In *Proc. of the Conf. on Data and Application Security and Privacy*. ACM, 37–48. https://doi.org/10.1145/3292006.3300027

[25] Jaco du Toit. 2020. PAUDIT: A Distributed Data Architecture for Fitness Data. In *Information and Cyber Security (Communications in Computer and Information Science)*, Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, and Jan Eloff (Eds.). Springer International Publishing, 43–56. https://doi.org/10.1007/978-3-030-43276-8_4

[26] Simon Eberz, Giulio Lovisotto, Andrea Patane, Marta Kwiatkowska, Vincent Lenders, and Ivan Martinovic. 2018. When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts. In *S&P*. IEEE, 889–905. https://doi.org/10.1109/SP.2018.00053

[27] Melanie Ehrenkranz. 2019. The Plan to Use Fitbit Data to Stop Mass Shootings Is One of the Scariest Proposals Yet. https://gizmodo.com/the-plan-to-use-fitbit-data-to-stop-mass-shootings-is-o-1837710691

[28] Haroon Elahi and Guojun Wang. 2019. A Participatory Privacy Protection Framework for Smart-Phone Application Default Settings. In *Security in Computing and Communications*. Springer, 168–182. https://doi.org/10.1007/978-981-13-5826-5_13

[29] Haroon Elahi, Guojun Wang, and Dongqing Xie. 2017. Assessing privacy behaviors of smartphone users in the context of data over-collection problem: An exploratory study. In *Proc. of the IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 1–8. https://doi.org/10.1109/UIC-ATC.2017.8397613

[30] Daniel A. Epstein, Alan Borning, and James Fogarty. 2013. Fine-grained sharing of sensed physical activity: a value sensitive approach. In *Conference on Pervasive and Ubiquitous Computing (UbiComp)*. ACM, 489–498. https://doi.org/10.1145/2493432.2493433

[31] Daniel A. Epstein, An Ping, James Fogarty, and Sean A. Munson. 2015. A lived informatics model of personal informatics. In *Conference on Pervasive and Ubiquitous Computing (UbiComp)*. Association for Computing Machinery, 731–742. https://doi.org/10.1145/2750858.2804250

[32] Emre Ertin, Nathan Stohs, Santosh Kumar, Andrew Raij, Mustafa al'Absi, and Siddharth Shah. 2011. AutoSense: unobtrusively wearable sensor suite for inferring the onset, causality, and consequences of stress in the field. In *Proc. of the Conf. on Embedded Networked Sensor Systems (SenSys)*. ACM, 274. https://doi.org/10.1145/2070942.2070970

[33] Facebook. 2023. Facebook Privacy Checkup | Facebook Help Centre. https://www.facebook.com/help/443357099140264

[34] Louis Faust, Priscilla Jiménez-Pazmino, James K. Holland, Omar Lizardo, David Hachen, and Nitesh V. Chawla. 2019. What 30 Days Tells Us About 3 Years: Identifying Early Signs of User Abandonment and Non-Adherence. In *Proc. of the Conf. on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*. ACM, 216–224. https://doi.org/10.1145/3329189.3329196

[35] Johannes Feichtner and Stefan Gruber. 2020. Understanding Privacy Awareness in Android App Descriptions Using Deep Learning. In *Proc. of the Conf. on*

Data and Application Security and Privacy (CODASPY). ACM, 203–214. https://doi.org/10.1145/3374664.3375730

[36] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*. 1–14. https://doi.org/10.1145/2335356.2335360

[37] fitcoin. 2023. Fitcoin | Much more than just a fitness cryptocurrency. https://fitcoin.io/

[38] Scott Freeman, Sarah L. Eddy, Miles McDonough, Michelle K. Smith, Nnadozie Okoroafor, Hannah Jordt, and Mary Pat Wenderoth. 2014. Active learning increases student performance in science, engineering, and mathematics. *Proc. of the National Academy of Sciences of the United States of America* 111, 23 (2014), 8410–8415. https://doi.org/10.1073/pnas.1319030111

[39] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *CHI Conference on Human Factors in Computing Systems*. ACM, 1–24. https://doi.org/10.1145/3491102.3517504

[40] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. Can IoT Wearable Devices Feed Frugal Innovation?. In *Proc. of the Workshop on Experiences with the Design and Implementation of Frugal Smart Objects (FRUGALTHINGS)*. ACM, 1–6. https://doi.org/10.1145/3410670.3410861

[41] Sandra Gabriele and Sonia Chiasson. 2020. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1–12. https://doi.org/10.1145/3313831.3376651

[42] Andrew Garbett, David Chatting, Gerard Wilkinson, Clement Lee, and Ahmed Kharrufa. 2018. ThinkActive: Designing for Pseudonymous Activity Tracking in the Classroom. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1–13. https://doi.org/10.1145/3173574.3173581

[43] Kambiz Ghazinour, Emil Shirima, Vijayasimha Reddy Parne, and Abhilash BhoomReddy. 2017. A Model to Protect Sharing Sensitive Information in Smart Watches. *Procedia Computer Science* 113 (2017), 105–112. https://doi.org/10.1016/j.procs.2017.08.322

[44] Yanmin Gong, Yuguang Fang, and Yuanxiong Guo. 2016. Private data analytics on biomedical sensing data via distributed computation. *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 13, 3 (2016), 431–444. https://doi.org/10.1109/TCBB.2016.2515610

[45] Peter Leo Gorski, Yasemin Acar, Luigi Lo Iacono, and Sascha Fahl. 2020. Listen to Developers! A Participatory Design Study on Security Warnings for Cryptographic APIs. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1–13. https://doi.org/10.1145/3313831.3376142

[46] Lahari Goswami, Thibault Estier, Pegah Sadat Zeinoddin, and Mauro Cherubini. 2023. Supporting Collaboration in Introductory Programming Classes Taught in Hybrid Mode: A Participatory Design Study. *Designing Interactive Systems Conference (DIS)* (2023). https://doi.org/10.1145/3563657.3596042

[47] Saul Greenberg, Sheelagh Carpendale, Nicolai Marquardt, and Bill Buxton. 2012. The narrative storyboard: telling a story about use and context over time. *ACM Interactions* 19, 1 (2012), 64–69. https://doi.org/10.1145/2065327.2065340

[48] Xinning Gui, Yu Chen, Clara Caldeira, Dan Xiao, and Yunan Chen. 2017. When Fitness Meets Social Networks: Investigating Fitness Tracking and Social Practices on WeRun. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1647–1659. https://doi.org/10.1145/3025453.3025654

[49] Shumin Guo and Keke Chen. 2012. Mining Privacy Settings to Find Optimal Privacy-Utility Tradeoffs for Social Network Services. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. IEEE, 656–665. https://doi.org/10.1109/SocialCom-PASSAT.2012.22

[50] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An Interactive Tool for Visualizing Privacy Policies. In *Proc. of the Workshop on Privacy in the Electronic Society (WPES)*. ACM, 57–71. https://doi.org/10.1145/3411497.3420221

[51] Mario A. Gutierrez, Michelle L. Fast, Anne H. Ngu, and Byron J. Gao. 2016. Real-Time Prediction of Blood Alcohol Content Using Smartwatch Sensor Data. In *Smart Health*, Xiaolong Zheng, Daniel Dajun Zeng, Hsinchun Chen, and Scott J. Leischow (Eds.). Springer, 175–186.

[52] Yangyang He. 2019. Recommending privacy settings for IoT. In *Proc. of the Conf. on Intelligent User Interfaces: Companion (IUI)*. ACM, 157–158. https://doi.org/10.1145/3308557.3308732

[53] Alex Hern. 2018. Fitness tracking app Strava gives away location of secret US army bases. *The Guardian* (Jan. 2018). https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[54] Robert P Hirten, Matteo Danieletto, Lewis Tomalin, Katie Hyewon Choi, Eddye Golden, Sparshdeep Kaur, Drew Helmus, Anthony Biello, Alexander Charney, Riccardo Miotto, Benjamin S Glicksberg, Ismail Nabeel, Judith Aberg, David Reich, Dennis Charney, Laurie Keefer, Mayte Suarez-Farinas, Girish N Nadkarni, and Zahi A Fayad. 2021. Physiological Data from a Wearable Device Identifies SARS-CoV-2 Infection and Symptoms and Predicts COVID-19 Diagnosis: Observational Study. *Journal of Medical Internet Research* (2021), 36.

[55] Yangyu Hu, Haoyu Wang, Tiantong Ji, Xusheng Xiao, Xiapu Luo, Peng Gao, and Yao Guo. 2021. CHAMP: Characterizing Undesired App Behaviors from User Comments based on Market Policies. In *Proc. of the Conf. on Software Engineering (ICSE '21)*. IEEE Press, 933–945. https://doi.org/10.1109/ICSE43902.2021.00089

[56] Huawei. 2021. Account Kit-OAuth 2.0-based Authentication. https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides-V5/open-platform-oauth-0000001053629189-V5

[57] Alethia Hume, Nicolás Ferreira, and Luca Cernuzzi. 2021. The design of a privacy dashboard for an academic environment based on participatory design. In *Latin American Computing Conf. (CLEI)*. 1–10. https://doi.org/10.1109/CLEI53233.2021.9640155

[58] IDC. 2020. Shipments of Wearable Devices Leap to 125 Million Units, Up 35.1% in the Third Quarter, According to IDC. https://www.idc.com/getdoc.jsp?containerId=prUS47067820

[59] Qatrunnada Ismail, Tousif Ahmed, Kelly Caine, Apu Kapadia, and Michael Reiter. 2017. To Permit or Not to Permit, That is the Usability Question: Crowdsourcing Mobile Apps' Privacy Permission Settings. In *Proc. on Privacy Enhancing Technologies (PoPETs)*, Vol. 2017. 119–137. https://doi.org/10.1515/popets-2017-0041

[60] Ayanga Imesha Kumari Kalupahana, Ananta Narayanan Balaji, Xiaokui Xiao, and Li-Shiuan Peh. 2023. SeRaNDiP - Leveraging Inherent Sensor Random Noise for Differential Privacy Preservation in Wearable Community Sensing Applications. In *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, Vol. 7.

[61] Andrei Kazlouski, Thomas Marchioro, and Evangelos Markatos. 2023. I just wanted to track my steps! Blocking unwanted traffic of Fitbit devices. In *Proc. of the Conf. on the Internet of Things (IoT '22)*. ACM, 96–103. https://doi.org/10.1145/3567445.3567457

[62] Finn Kensing and Andreas Munk-Madsen. 1993. PD: structure in the toolbox. *Commun. ACM* 36, 6 (1993), 78–85. https://doi.org/10.1145/153571.163278

[63] Jennifer King, Airi Lampinen, and Alex Smolen. 2011. Privacy: is there an app for that?. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. ACM, 1. https://doi.org/10.1145/2078827.2078843

[64] Georgios Kontaxis, Michalis Polychronakis, and Evangelos P. Markatos. 2012. Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security* 11, 5 (2012), 321–332. https://doi.org/10.1007/s10207-012-0173-6

[65] Hanna Krasnova, Nicole Eling, Oleg Schneider, Helena Wenninger, Thomas Widjaja, and Peter Buxmann. 2013. Does This App Ask For Too Much Data? The Role Of Privacy Perceptions In User Behavior Towards Facebook Applications And Permission Dialogs. *Proc of the European Conf. of Information Systems* (2013), 14.

[66] Hyeokhyen Kwon, Gregory D. Abowd, and Thomas Plötz. 2018. Adding structural characteristics to distribution-based accelerometer representations for activity recognition using wearables. In *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*. ACM, 72–75. https://doi.org/10.1145/3267242.3267258

[67] Federica Laricchia. 2021. Number of connected wearable devices worldwide from 2016 to 2022. https://www.statista.com/statistics/487291/global-connected-wearable-devices/

[68] Chantal Lidynia, Philipp Brauner, and Martina Ziefle. 2018. A Step in the Right Direction – Understanding Privacy Concerns and Perceived Sensitivity of Fitness Trackers. In *Advances in Human Factors in Wearable Technologies and Game Design*, Tareq Ahram and Christianne Falcão (Eds.). Springer, 42–53. https://doi.org/10.1007/978-3-319-60639-2_5

[69] Stephen Lindsay, Daniel Jackson, Guy Schofield, and Patrick Olivier. 2012. Engaging older people using participatory design. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 1199–1208. https://doi.org/10.1145/2207676.2208570

[70] Xiao Liu, Bonan Gao, Basem Suleiman, Han You, Zisu Ma, Yu Liu, and Ali Anaissi. 2023. Privacy-Preserving Personalized Fitness Recommender System P3FitRec: A Multi-level Deep Learning Approach. *ACM Transactions on Knowledge Discovery from Data* 17, 6 (2023), 76:1–76:24. https://doi.org/10.1145/3572899

[71] Deborah Lupton. 2021. "Sharing Is Caring:" Australian Self-Trackers' Concepts and Practices of Personal Data Sharing and Privacy. *Frontiers in Digital Health* 3 (2021). https://doi.org/10.3389/fdgth.2021.649275

[72] Meethu Malu and Leah Findlater. 2016. Toward Accessible Health and Fitness Tracking for People with Mobility Impairments. In *Proc. of the Conf. on Pervasive Computing Technologies for Healthcare*. ACM. https://doi.org/10.4108/eai.16-5-2016.2263329

[73] Tenga Matsuura, Ayako A. Hasegawa, Mitsuaki Akiyama, and Tatsuya Mori. 2021. Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods. In *European Symp. on Usable Security*. ACM, 36–47. https://doi.org/10.1145/3481357.3481515

[74] Ulku Meteriz, Necip Fazil Yildiran, Joongheon Kim, and David Mohaisen. 2020. Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In *Proc. of the Conf. on Distributed Computing Systems (ICDCS)*. IEEE, 464–473. https://doi.org/10.1109/ICDCS47774.2020.00063

[75] Jochen Meyer, Merlin Wasmann, Wilko Heuten, Abdallah El Ali, and Susanne C.J. Boll. 2017. Identification and Classification of Usage Patterns in Long-Term Activity Tracking. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 667–678. https://doi.org/10.1145/3025453.3025690

[76] Vishvak S. Murahari and Thomas Plötz. 2018. On attention models for human activity recognition. In *Proc.of the Symp. on Wearable Computers (ISWC)*. ACM, 100–103. https://doi.org/10.1145/3267242.3267287

[77] Patrick Murmann, Matthias Beckerle, Simone Fischer-Hübner, and Delphine Reinhardt. 2021. Reconciling the what, when and how of privacy notifications in fitness tracking scenarios. *Pervasive and Mobile Computing* 77 (Oct. 2021), 101480. https://doi.org/10.1016/j.pmcj.2021.101480

[78] Annamalai Natarajan, Abhinav Parate, Edward Gaiser, Gustavo Angarita, Robert Malison, Benjamin Marlin, and Deepak Ganesan. 2013. Detecting cocaine use with wearable electrocardiogram sensors. In *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*. ACM, 123–132. https://doi.org/10.1145/2493432.2493496

[79] Kavous Salehzadeh Niksirat, Lev Velykoivanenko, Noé Zufferey, Mauro Cherubini, Kévin Huguenin, and Mathias Humbert. 2024. Wearable Activity Trackers: A Survey on Utility, Privacy, and Security. *Comput. Surveys* (2024). https://doi.org/10.1145/3645091

[80] Mehdi Nobakht, Yulei Sui, Aruna Seneviratne, and Wen Hu. 2020. PGFit: Static permission analysis of health and fitness apps in IoT programming frameworks. *Journal of Network and Computer Applications* 152 (2020), 102509. https://doi.org/10.1016/j.jnca.2019.102509

[81] Jourdan Owen, Delano Archibald, and Damith Wickramanayake. 2019. The Willingness to Adopt Fitness Wearables in Jamaica: A Study on Wearable Fitness Trackers in Kingston and St. Andrew. *International Journal of Internet of Things* 8, 2 (2019), 36–45. https://doi.org/10.5923/j.ijit.20190802.02

[82] Pooja Parameshwarappa, Zhiyuan Chen, and Gunes Koru. 2020. An Effective and Computationally Efficient Approach for Anonymizing Large-Scale Physical Activity Data: Multi-Level Clustering-Based Anonymization. *International Journal of Information Security and Privacy (IJISP)* 14, 3 (2020), 72–94. https://doi.org/10.4018/IJISP.2020070105

[83] Jamie Pinchot and Donna Cellante. 2021. Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers. *Journal of Information Systems Applied Research* 14, 2 (2021), 4–13. http://jisar.org/2021-14/n2/JISARv14n2p4.html

[84] Zablon Pingo and Bhuva Narayan. 2018. Users' Responses to Privacy Issues with the Connected Information Ecologies Created by Fitness Trackers. In *Maturity and Innovation in Digital Libraries*, Milena Dobreva, Annika Hinze, and Maja Žumer (Eds.). Springer, 240–255. https://doi.org/10.1007/978-3-030-04257-8_25

[85] Karen Renaud and Judy van Biljon. 2008. Predicting Technology Acceptance and Adoption by the Elderly: A Qualitative study. *South African Institute of Computer Scientists & Information Technologists (SAICSIT)* (2008).

[86] Christopher Rowl. 2019. With fitness trackers in the workplace, bosses can monitor your every step - and possibly more. https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html

[87] Johnny Saldana. 2021. *The Coding Manual for Qualitative Researchers* (4th ed ed.). SAGE Publishing.

[88] Kavous Salehzadeh Niksirat, Evanne Anthoine-Milhomme, Samuel Randin, Kévin Huguenin, and Mauro Cherubini. 2021. "I thought you were okay": Participatory Design with Young Adults to Fight Multiparty Privacy Conflicts in Online Social Networks. In *Designing Interactive Systems Conf.* ACM, 104–124. https://doi.org/10.1145/3461778.3462040

[89] Kavous Salehzadeh Niksirat, Fitra Rahmamuliani, Xiangshi Ren, and Pearl Pu. 2022. Understanding intergenerational fitness tracking practices: 12 suggestions for design. *CCF Transactions on Pervasive Computing and Interaction* 4, 1 (March 2022), 13–31. https://doi.org/10.1007/s42486-021-00082-2

[90] Odnan Ref Sanchez, Ilaria Torre, Yangyang He, and Bart P. Knijnenburg. 2020. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction* 30, 3 (2020), 513–565. https://doi.org/10.1007/s11257-019-09246-3

[91] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proc. of the Asia Conf. on Computer and Communications Security (Asia CCS)*. ACM, 340–351. https://doi.org/10.1145/3321705.3329806

[92] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. 2019. Understanding the Impact of Information Representation on Willingness to Share Information. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 1–6. https://doi.org/10.1145/3290605.3300753

[93] Mohamed Shehab, Said Marouf, and Christopher Hudel. 2011. ROAuth: recommendation based open authorization. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. ACM Press, 1. https://doi.org/10.1145/2078827.2078842

[94] Daniel Smullen, Yuanyuan Feng, Shikun Aerin Zhang, and Norman Sadeh. 2020. The Best of Both Worlds: Mitigating Trade-offs Between Accuracy and User Burden in Capturing Mobile App Privacy Preferences. In *Proc. on Privacy Enhancing Technologies (PoPETs)*, Vol. 2020. 195–215. https://doi.org/10.2478/popets-2020-0011

[95] Alina Stöver, Sara Hahn, Felix Kretschmer, and Nina Gerber. 2023. Investigating how Users Imagine their Personal Privacy Assistant. *Proc. on Privacy Enhancing Technologies (PoPETs)* 2023, 2 (2023), 384–402. https://doi.org/10.56553/popets-2023-0059

[96] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2022. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI) (CHI '23)*. ACM, 1–24. https://doi.org/10.1145/3544548.3581060

[97] Lie Ming Tang, Jochen Meyer, Daniel A. Epstein, Kevin Bragg, Lina Engelen, Adrian Bauman, and Judy Kay. 2018. Defining Adherence: Making Sense of Physical Activity Tracker Data. *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2, 1 (2018), 37:1–37:22. https://doi.org/10.1145/3191769

[98] Rina Torchinsky. 2022. How period tracking apps and data privacy fit into a post-Roe v. Wade climate. *NPR* (June 2022). https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

[99] Ilaria Torre, Odnan Ref Sanchez, Frosina Koceva, and Giovanni Adorni. 2018. Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing* 22, 2 (2018), 345–364. https://doi.org/10.1007/s00779-017-1068-3

[100] European Union. 2016. Art. 17 GDPR – Right to erasure ('right to be forgotten'). https://gdpr-info.eu/art-17-gdpr/

[101] Christie van Diggele, Annette Burgess, and Craig Mellis. 2020. Planning, preparing and structuring a small group teaching session. *BMC Medical Education* 20, 2 (2020), 462. https://doi.org/10.1186/s12909-020-02281-4

[102] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2021. Are Those Steps Worth Your Privacy?: Fitness-Tracker Users' Perceptions of Privacy and Utility. *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 5, 4 (2021), 1–41. https://doi.org/10.1145/3494960

[103] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2018. Privacy Attitudes and Data Valuation Among Fitness Tracker Users. In *Transforming Digital Worlds*, Gobinda Chowdhury, Julie McLeod, Val Gillet, and Peter Willett (Eds.). Springer, 229–239. https://doi.org/10.1007/978-3-319-78105-1_27

[104] Jing Wang, Na Wang, and Hongxia Jin. 2016. Context Matters? How Adding the Obfuscation Option Affects End Users' Data Disclosure Decisions. In *Proc. of the Conf. on Intelligent User Interfaces (IUI)*. ACM, 299–304. https://doi.org/10.1145/2856767.2856817

[105] Na Wang. 2012. Third-party applications' data practices on facebook. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1399–1404. https://doi.org/10.1145/2212776.2212462

[106] Na Wang, Heng Xu, and Jens Grossklags. 2011. Third-party apps on Facebook: privacy and the illusion of control. In *Proc. of the Symp. on Computer Human Interaction for Management of Information Technology (CHIMIT)*. ACM, 1–10. https://doi.org/10.1145/2076444.2076448

[107] Rui Wang, Weichen Wang, Alex daSilva, Jeremy F. Huckins, William M. Kelley, Todd F. Heatherton, and Andrew T. Campbell. 2018. Tracking Depression Dynamics in College Students Using Mobile Phone and Wearable Sensing. *Proc. of the conf. on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2, 1 (2018), 1–26. https://doi.org/10.1145/3191775

[108] Renita Washburn, Tangila Islam Tanni, Yan Solihin, Apu Kapadia, and Mary Jean Amon. 2023. Bottom-up psychosocial interventions for interdependent privacy: Effectiveness based on individual and content differences. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, 1–20. https://doi.org/10.1145/3544548.3581117

[109] Susanne Weber, Marian Harbach, and Matthew Smith. 2015. Participatory Design for Security-Related User Interfaces. In *Proc. Workshop on Usable Security*. Internet Society. https://doi.org/10.14722/usec.2015.23011

[110] WeWard. 2023. WeWard - The mobile app that motivates you to walk. https://www.wewardapp.com/

[111] Pamela Wisniewski, Heng Xu, Heather Lipford, and Emmanuel Bello-Ogunu. 2015. Facebook apps and tagging: The trade-off between personal privacy and engaging with friends: Facebook Apps and Tagging: The Trade-off Between Personal Privacy and Engaging with Friends. *Journal of the Association for Information Science and Technology* 66, 9 (2015), 1883–1896. https://doi.org/10.1002/asi.23299

[112] Daniel R. Witt, Ryan A. Kellogg, Michael P. Snyder, and Jessilyn Dunn. 2019. Windows into human health through wearables data analytics. *Current Opinion in Biomedical Engineering* 9 (2019), 28–46. https://doi.org/10.1016/j.cobme.2019.01.001

[113] Verena M. Wottrich, Eva A. van Reijmersdal, and Edith G. Smit. 2018. The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness,

and privacy concerns. *Decision Support Systems* 106 (2018), 44–52. https://doi.org/10.1016/j.dss.2017.12.003

[114] Noé Zufferey, Mathias Humbert, Romain Tavenard, and Kévin Huguenin. 2023. Watch your Watch: Inferring Personality Traits from Wearable Activity Trackers. In *Proc. of the USENIX Security Symp.* USENIX Association, 193–210. https://www.usenix.org/conference/usenixsecurity23/presentation/zufferey

[115] Noé Zufferey, Kavous Salehzadeh Niksirat, Mathias Humbert, and Kévin Huguenin. 2023. "Revoked just now!" Users' Behaviors Toward Fitness-Data Sharing with Third-Party Applications. *Proc. on Privacy Enhancing Technologies (PoPETs)* 2023, 1 (2023), 47–67. https://doi.org/10.56553/popets-2023-0004

[116] Douglas Zytko, Pamela J. Wisniewski, Shion Guha, Eric P. S. Baumer, and Min Kyung Lee. 2022. Participatory Design of AI Systems: Opportunities and Challenges Across Diverse Users, Relationships, and Application Domains. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, 1–4. https://doi.org/10.1145/3491101.3516506

A TPA REGISTRATION FORM

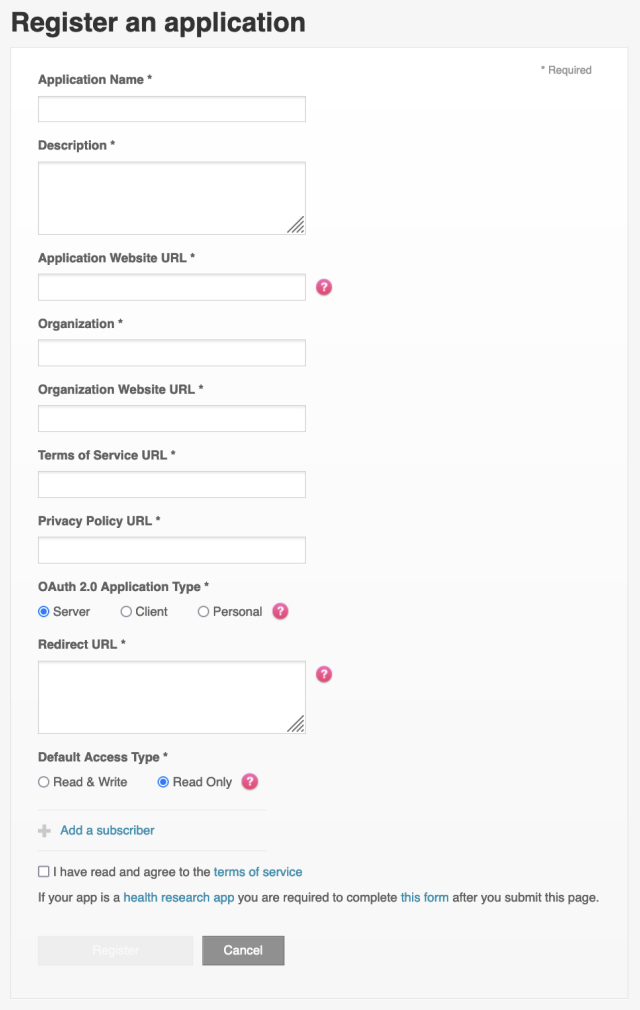


Figure 4: A screenshot of the form to register a TPA on the Fitbit developer platform (May 2024).

B SESSION TIMELINE

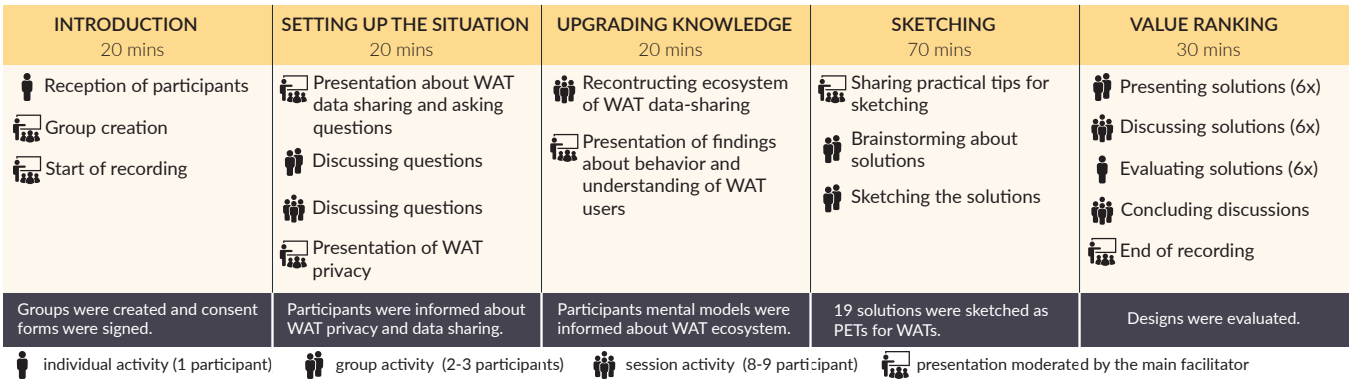


Figure 5: Session timeline. This figure summarizes the activities (top), detailed steps (middle), and outcomes (bottom) of each participatory design session.

C SESSION ROOM LAYOUT

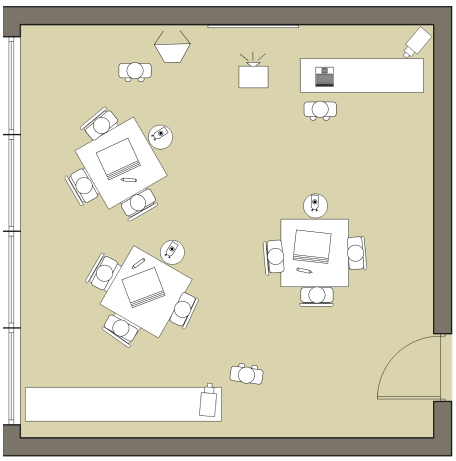


Figure 6: Layout of the room where all the participatory design sessions were conducted. Three tables, three chairs each, drawing material (e.g., paper sheets, pens), a flipchart, and a video projector (and a connected laptop) were used. Also, three audio recorders (one per table) and two video cameras were used to record the sessions. The facilitators stood up and could freely move around while participants sat in groups around the tables.

D DETAILS ABOUT THE PARTICIPANTS

DS	G	Gender	Age	Days	Hours	Nb TPAs	Device
1	1	woman	23	6	13-18	1	Garmin
		man	30	7	13-18	10+	Apple
		man	20	7	13-18	1	Apple
	2	woman	22	7	19-24	2-5	Fitbit
		man	22	4	7-12	2-5	Garmin
	3	woman	19	7	7-12	2-5	Apple
		man	22	7	19-24	1	Apple
		man	20	7	19-24	6-9	Apple
2	4	man	25	4	7-12	2-5	Garmin
		woman	22	7	19-24	1	Fitbit
		woman	19	5	19-24	2-5	Garmin
	5	woman	24	6	13-18	2-5	Apple
		man	19	5	13-18	2-5	Apple
		man	20	5	19-24	1	Garmin
	6	woman	23	5	19-24	1	Other
		man	21	7	13-18	1	Apple
		woman	20	7	13-18	2-5	Apple
3	7	man	21	7	7-12	2-5	Apple
		woman	20	5	19-24	1	Apple
		woman	21	5	7-12	1	Apple
	8	woman	18	7	7-12	1	Apple
		man	20	7	7-12	1	Apple
		man	20	3	7-12	2-5	Apple
	9	man	20	7	19-24	1	Apple
		man	19	7	19-24	2-5	Fitbit
		woman	19	3	7-12	1	Apple

Table 1: Details of participants for each participatory design session and group. For each participant, we indicate which design session (DS) and group (G) they were attributed to, their gender, their age, how many days a week and how many hours per day they usually wear their WAT, how many TPAs they share their data with, and their WAT brand.

E PHOTOS OF THE SESSIONS

Figure 7: A participant sketching

Figure 8: A group of participants discussing their sketched solutions

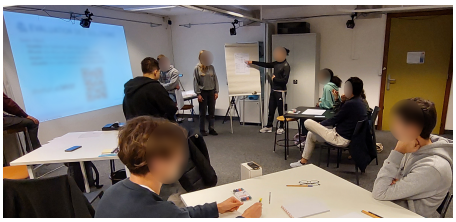


Figure 9: A group presenting their design

F FEATURE EXAMPLES

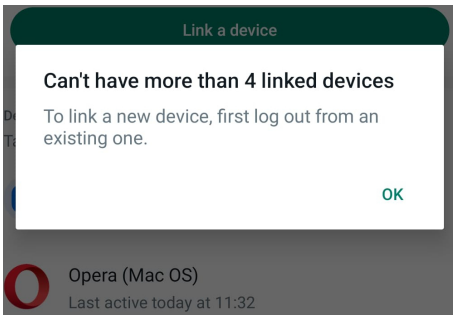


Figure 10: Screenshot of the WhatsApp linked devices panel. The user cannot link their account with more than four different devices at a time.

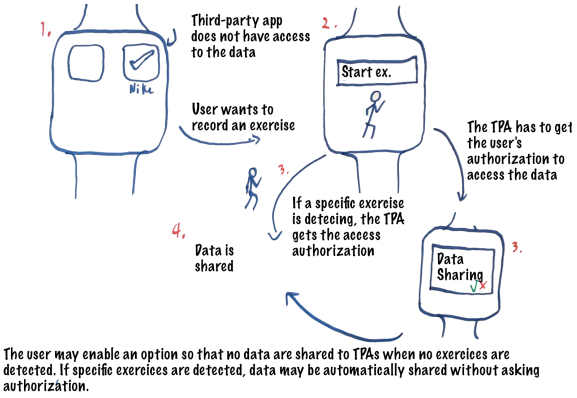


Figure 11: Translated version of the design that proposes PARTIAL SHARING regarding specific contexts (exercises) and/or time frames (only the data collected during this context/time frame will be shared). In this version of the design, we replaced all the text (written in French) with an English translation.

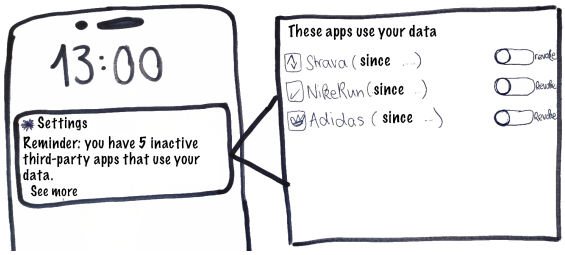


Figure 12: Translated version of a design that implements a reminder notification feature (REMINDER).

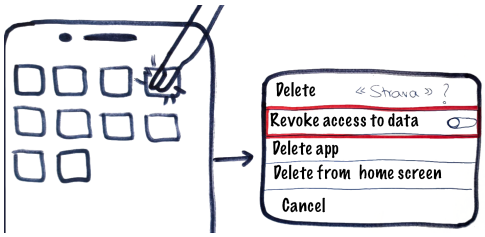
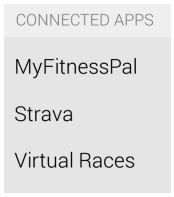
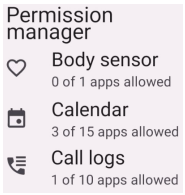


Figure 13: A translated example of design implementing REVOCATION ASSISTANCE enabling revoking access while uninstalling a TPA's mobile app on the phone.



(a) Garmin companion app showing the TPAs list. When the user taps on one of the TPAs, it opens a panel showing all types of data that is shared with that TPA. The colors have been inverted for readability.



(b) Permission management panel on Android. When the user taps on one of the data types, it opens a panel showing all applications having access to that data/sensor.

Figure 14: Screenshots of the Garmin TPAs list (left) and of the Android permission manager (right).

G DESIGN FEATURE CODING

Code / Group	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	8	9	9
Feature 1 - Partial sharing	✓									✓							✓		
Code 1.1 - Sharing regarding the context	✓																		
Code 1.2 - Sharing regarding a specific timeframe	✓									✓							✓		
Feature 2 - Visualization		✓								✓	✓			✓				✓	
Code 2.1- Interactive tool for exploring shared data / data flow		✓									✓							✓	
Code 2.2- Data sharing logs (history)										✓									
Code 2.3 - TPA usage Statistics														✓					
Feature 3 - Centralization				✓				✓				✓							
Code 3.1 - Specific app store				✓															
Code 3.2 - Plugins								✓				✓							
Feature 4 - Reminders			✓		✓	✓	✓							✓	✓				✓
Code 4.1 - "Opt-in" data access renewal			✓		✓														✓
Code 4.2 - "Opt-out" data access renewal															✓				
Code 4.3 - Only information			✓			✓	✓							✓	✓				
Feature 5 -Revocation Assistance																✓		✓	✓
Code 5.1 - Assistance for access revocation when uninstalling TPA's service																✓			✓
Code 5.2 - Assistance for asking TPA to remove the user's data from their servers																		✓	
Code 5.3 - Automatic revocation																			✓
Feature 6 - Sensitization, Education					✓		✓		✓				✓						
Code 6.1 - Video					✓				✓				✓						
Code 6.2 - Informative and Interactive consent form					✓		✓												
Feature 7 - TPAs limit			✓																

Table 2: Coding table. Each column corresponds to one specific design. For each design, we display the ID of the group who designed it, this ID corresponds to the group IDs in Table 1.