Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility

Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, Mauro Cherubini

Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility

LEV VELYKOIVANENKO, University of Lausanne, Switzerland
KAVOUS SALEHZADEH NIKSIRAT, University of Lausanne, Switzerland
NOÉ ZUFFEREY, University of Lausanne, Switzerland
MATHIAS HUMBERT, University of Lausanne, Switzerland
KÉVIN HUGUENIN, University of Lausanne, Switzerland
MAURO CHERUBINI, University of Lausanne, Switzerland

Fitness trackers are increasingly popular. The data they collect provides substantial benefits to their users, but it also creates privacy risks. In this work, we investigate how fitness-tracker users perceive the utility of the features they provide and the associated privacy-inference risks. We conduct a longitudinal study composed of a four-month period of fitness-tracker use ($N = 227$), followed by an online survey ($N = 227$) and interviews ($N = 19$). We assess the users' knowledge of concrete privacy threats that fitness-tracker users are exposed to (as demonstrated by previous work), possible privacy-preserving actions users can take, and perceptions of utility of the features provided by the fitness trackers. We study the potential for data minimization and the users' mental models of how the fitness tracking ecosystem works. Our findings show that the participants are aware that some types of information might be inferred from the data collected by the fitness trackers. For instance, the participants correctly guessed that sexual activity could be inferred from heart-rate data. However, the participants did not realize that also the non-physiological information could be inferred from the data. Our findings demonstrate a high potential for data minimization, either by processing data locally or by decreasing the temporal granularity of the data sent to the service provider. Furthermore, we identify the participants' lack of understanding and common misconceptions about how the Fitbit ecosystem works.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; *Privacy protections*; • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**.

Additional Key Words and Phrases: fitness trackers, utility, privacy, mental models, wearable activity trackers.

ACM Reference Format:
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. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 4, Article 181 (December 2021), 41 pages. https://doi.org/10.1145/3494960

Authors' addresses: Lev Velykoivanenko, lev.velykoivanenko@unil.ch, University of Lausanne, Lausanne, Switzerland; Kavous Salehzadeh Niksirat, kavous.niksirat@unil.ch, University of Lausanne, Lausanne, Switzerland; Noé Zufferey, noe.zufferey@unil.ch, University of Lausanne, Lausanne, Switzerland; Mathias Humbert, mathias.humbert@armasuisse.ch, University of Lausanne, Lausanne, Switzerland; Kévin Huguenin, kevin.huguenin@unil.ch, University of Lausanne, Lausanne, Switzerland; Mauro Cherubini, mauro.cherubini@unil.ch, University of Lausanne, Lausanne, Switzerland.

2474-9567/2021/12-ART181
https://doi.org/10.1145/3494960

1 INTRODUCTION

Wearable devices, such as fitness trackers,[1] were among the top worldwide fitness trends from 2016 to 2020 [101]. In recent years, fitness tracker brands such as Fitbit have attracted much attention from both users [96] and technology giants such as Google [108]. Fitness trackers enable users to continuously collect large amounts of physiological data, ranging from step counts to heart rate. The first generation of users who started benefiting from wearable devices were 'self-quantifiers': technology-savvy individuals who use wearable devices to log their physiological data and behaviors to learn more about themselves [15, 64]. Today, wearable devices are more pervasive, easier to use, and more affordable than ever before. As a result, individuals who are not technologically savvy can also reap the aforementioned benefits of fitness trackers. These users can self-reflect on their data [54], and set goals [75] to maintain a healthy lifestyle and to improve their well-being.

Despite the enormous benefits fitness trackers offer, their use can involve privacy risks [3, 40, 87]. First, a user may choose to share their data with their tracker's manufacturer and/or the manufacturer's affiliates [102]. Users can also compromise their privacy for the benefits provided by third-party organizations (e.g., giving access to insurance providers in exchange for lower premiums [22, 97]). Furthermore, users can also expose their fitness data on online social networks for self-presentation [6]. In addition to data leakages, earlier studies showed that the existing machine-learning techniques are capable of inferring users' sensitive information from their fitness tracker data (e.g., drug consumption) [7, 10, 20, 66–68, 83, 93, 105]. Although in some cases these inferences could benefit users (e.g., diagnosing COVID-19 [41, 82]), the mainstream media have reported several privacy and security incidents involving fitness trackers [40, 87].

Earlier research showed that fitness-tracker users perceive their devices as being mostly beneficial [6, 63, 109]. However, most users are not well-informed about the privacy risks associated with their device [6, 34, 91, 109]. Hence, users have an overall low level of privacy concerns [63, 109]. Users also do not take sufficient actions to protect their privacy [4, 34, 63, 109]. Despite this previous body of research, we have a limited understanding of the utility that users associate with these devices and the most common privacy concerns that could arise after repeated use of this technology. In this work, we assess users' perceptions of the utility of their fitness trackers, as some user behaviors related to utility might have further implications for privacy. In particular, we evaluate the potential for data minimization [14, 58], i.e., preventing the collection and transfer of data that does not contribute to a feature considered significantly useful by the users. While studying users' perceptions of fitness-tracker's utility, we also assessed their knowledge of privacy threats about different types of information that can be inferred from data collected by fitness trackers. Additionally, as users' awareness of privacy risks is closely related to their understanding of how the fitness tracker ecosystem functions (see Appendix A), we investigate their mental models [70] regarding how fitness tracker data is transmitted between, and processed by, different entities (e.g., fitness tracker, smartphone, servers, *etc.*). This is indeed in line with the definition of privacy by Nissenbaum [78] that privacy is adopted by appropriate flows of information. The appropriateness of information flow is defined by established contextual norms between different entities (i.e., senders, recipients, and data subjects), information type, and transmission principles (i.e., the constraints that control information flow). Lastly, we are interested in learning more about the reasons for the privacy-preserving actions that fitness tracker users take. To this end, we pose the following research questions:

RQ1. How do users value the utility of features, types of data, and platforms in the fitness-tracker ecosystem? In particular, how much loss of detail would users be willing to accept to protect their privacy?

RQ2. How do users perceive privacy in the context of fitness trackers? In particular, which types of sensitive information do users think can be inferred and with what accuracy?

[1] 'Fitness trackers' refers to any wrist-worn wearable devices that can collect fitness data. For instance, Fitbit, Garmin, and Jawbone are the most common types of fitness tracker [39, 44, 62].

RQ3. How well do users understand the information flow among the devices, the companion app, and the supporting online services?
RQ4. Which behaviors would users engage in to protect their privacy?

In order to answer our research questions, we conducted a longitudinal study with young university students ($N = 227$). We provided all of our participants with fitness trackers and asked them to use the trackers for four months. At the end of the four months, we asked these individuals to complete an online survey (followed by an interview with some of the respondents, $N = 19$). The survey included questions about fitness-tracker users' privacy-risk awareness, privacy-preserving actions, and their perceptions of utility of their devices. To assess our participants' mental models, we also asked them to make a drawing of how they think the data collected by their tracker is transferred and processed.

Our findings showed a high potential for data minimization without affecting the perceived utility of the fitness trackers. Most notably, we found that most of the features that users find significantly useful could be implemented by *only* storing the data locally on the users' smartphone (i.e., without sending it to Fitbit's servers by default), as very few participants reported accessing their data through Fitbit's website or with other connected devices. We found that the participants showed concerns about sensitive information being inferred from their fitness tracker data. However, their level of concern did not match their perception of how precisely different types of information could be inferred. Moreover, the vast majority of our participants showed a limited understanding of how the Fitbit ecosystem works. This could partially explain why participants did not think that it was possible to infer various types of sensitive information that are –in fact– possible to infer, as demonstrated by prior studies.

In this work, we provide an empirical contribution about how users of fitness trackers evaluate the utility of their device. Also, we contribute to a better understanding of the privacy risks (and functioning) typically understood by the users of this technology. Our findings can inform the design of new privacy-preserving strategies and data-minimization techniques for fitness trackers.

2 RELATED WORK

In this section, we review earlier studies on fitness-tracker users' perceptions of the utility of their devices, and we discuss the effect of the perceived utility on users' privacy decisions and possible implications for data minimization. Next, we look at prior studies about data inference and fitness-tracker users' perceptions of privacy. Last, we review the actions users take to protect their privacy. Prior work in this area is vast, so literature surveys have been compiled to support researchers [19, 21, 23, 39, 48, 80, 89, 92, 94]. In the following sections, we will refer to the individual studies and not to the surveys.

2.1 Utility Perceptions, Privacy Calculus, and Data Minimization

Utility perceptions of fitness trackers vary among users [12, 88]. The type of device they own, their technical expertise, values, and attitudes can influence their perceptions of the utility of the devices. An earlier study shows that users value functional factors more highly than hedonic attributes [45]. Prior research found that users of this type of device consider fitness and health-oriented data more important than social features such as messaging or sharing functions [95, 109]. Fitness-tracker users also have concerns that are related to their perceptions of the utility of their devices. Users can worry about how to present themselves by using fitness information, and they can be unsure about what the acceptable norms for sharing fitness information are [6, p. 429]. Prior research has found that these users are typically concerned about the type of fitness data that could be interesting to share [102], and users are often unsure about who would be interested in seeing their fitness data [75, 77].

Earlier research [12] found that users can be categorized into three general types: *benefit maximizers* (i.e., those who have utility preferences), *fact enthusiasts* (i.e., those who are interested in the motivational aspects of the fitness trackers), and *data protectors* (i.e., those who prioritize privacy). While using their trackers, users not only consider the utility aspects but also usually perform risk-benefit analyses (i.e., the so-called privacy calculus) [38, 60]. Users consider the trade-off between receiving relevant and personalized health information, the sensitivity of this information, and the existence of legislative data-protection mechanisms [60]. However, some users might not be sufficiently aware of the potential privacy risks that are involved in using fitness trackers [9]. Therefore, some users are not able to properly make informed decisions [63]. Research shows that fitness-tracker users usually give more weight to the utility rather than the privacy aspects [12, 106]. Users could be willing to sacrifice their privacy for utility, especially if they are ensured that the tracker provides considerable benefits [109]. In contrast, in other contexts users could be willing to compromise utility for privacy. For example, in the context of location check-ins, Bilogrevic et al. [11] studied how privacy-preserving techniques, such as obfuscating location information at the semantic and geographical levels, affect the perceived utility of the users and found that obfuscating geographical information had a less negative effect on users' utility than obfuscating semantic information did.

To the best of our knowledge, no existing work has investigated the *opportunities* for increasing fitness-tracker users' privacy, without affecting their perceived (or the concrete) utility of the technology. In particular, we are interested in studying this from a data-minimization perspective.[2] To elaborate, we aim to discover which *platforms* (e.g., the tracker itself, companion app, website) are less frequently used to view the fitness data, and which *forms of data representations* (e.g., different intervals and aggregations) could be perceived as sufficient for most fitness-tracker users.

2.2 Information Inference and Knowledge of Privacy Threats

Information inference is feasible with different types of data [2, 17, 42, 107]. But one particularly threatening case of inference attacks is related to fitness trackers [3, 40, 87], as they continuously collect users' physiological data that can reveal sensitive information related to their habits, behaviors, and beliefs. Inferences can be made by attackers by using machine-learning algorithms [7, 10, 20, 66–68, 83, 93, 105], and manually, wherein users could simply reflect on their peers' activity data and infer their sensitive information such as their lifestyles [37, p. 1653] or health conditions [36, p. 4317]. The former, however, is more concerning, as it can be done by malicious users and with higher accuracy. Research showed that attackers can precisely infer users' sensitive information such as smoking cigarettes [93], alcohol intoxication [7], illegal drug consumption [83], smartphone keystrokes (e.g., passwords) [66], and mechanical padlock codes [68].

With regard to inferences of sensitive information from other sources of data, Zimmer et al. [109] found that users are usually not aware of potential threats. More specifically related to the domain of fitness trackers, Schneegass et al. [91] found that non-expert fitness-tracker users could not distinguish between raw data and derived data. Consequently, users are more likely to underestimate potential inference threats. Furthermore, Gabriele and Chiasson [34] found that fitness-tracker users think that data inference is technically possible but unlikely to occur. For example, 61% of their participants found that it is possible to reject job applicants because of their poor mental health, as inferred from their sleep data, but only 21% of the respondents thought that such a scenario would be likely to occur [34, p. 5].

Overall, fitness-tracker users show a low level of concern regarding privacy [63, 109]. A significant portion of these users think no one would be interested in their data [109], and others fully trust the service providers

[2]Note that data minimization is one of the core principles of the *privacy-by-design approach* [14, 58]. For instance, if a participant looks only at their step data and does so only on the tracker itself, there is no need to send this data to the fitness tracker company's servers. Also, if a participant is not interested in their sleep data, then this data should not be collected in the first place.

to keep their data secure [6, 109]. The lack of privacy concerns can be attributed to a lack of understanding about inference attacks, as explained previously, or to the lack of awareness about how their data is collected and how it can be used [4, 63, 102]. Specifically, some functionalities offered by the service provider might create additional vulnerabilities for attackers to exploit (e.g., step counts sharing). Users are more or less concerned, depending on which type of data (e.g., step counts, sleep graphs, average active hours, etc.) would be shared and with whom (e.g., friends, employers, advertisement companies, etc.) [34, 76]. Users primarily worry about location data [53, 74]. Weight and sleep data are considered sensitive [61, 81]. Users are less comfortable sharing graph data (e.g., weight graphs) as compared to sharing aggregated statistical data (e.g., lifetime floors climbed) or personal data (e.g., birthday) [34]. Additionally, users would be more concerned if they thought that some of their data could be used to identify them [4, 36, 109]. For example, in recent research, users expressed higher levels of concern about situations where they noticed that their step-count data can reveal vital information about their daily activities [4, 36]. Furthermore, considering the recipients of the data being shared, users are concerned about 3rd parties, such as insurance companies [6, 34, 97], employers [6, 34, 36, 63], and advertising agencies [34], more than about other users of the same service.

While a previous work [34] studied the likelihood and plausibility of privacy breaches and information inference in different scenarios, in this work, we essentially focus on the *information type*. We seek to understand whether users think that different types of sensitive information (e.g., political views or personality traits) could be inferred accurately from their fitness data, and how they would rank the risks connected with these types of sensitive information being inferred accurately. Also, despite the vast literature on fitness tracker users' knowledge [4, 34, 63, 91, 102, 109], it is unclear how much users understand about the *architecture of the fitness-tracker ecosystem* and its associated risks. Therefore, our objective is also to study the mental models that fitness-tracker users have of these technical platforms [70].

2.3 Privacy-Preserving Actions

Fitness-tracker users usually take limited actions to preserve their privacy [4]. Most of the time, privacy-preserving actions are only limited to the first-time setup [109]. Prior research found that users typically do not change the default settings, and they do not read the privacy policy or the terms and conditions agreements [34]. Gabriele and Chiasson [34] found that only half of the users, in their sample, set their data sharing preferences. Prior research suggests that fitness trackers have limited privacy controls and that users of fitness trackers want more granular controls [13, 63]. Concerning the sharing of this type of data, a recent study found that users might agree to share their fitness data with their employers, but only if they could delete certain parts of their data before sharing [52]. Similarly, Klasnja et al. [53] reported that users would share their location data if they could be assured that it would be deleted after some time.[3] In this context, we are interested in knowing *what actions* users might take to protect their privacy. Given prior research in this area, we posit two hypothetical sets of actions: *i. not wearing* the tracker, to stop data collection during specific times; *ii. reducing the granularity* of the information being collected by the device (i.e., selecting limited information and recording only that information) instead of coarse recording (i.e., recording everything).[4] Given that granular recording is limited in current off-the-shelf (Fitbit) fitness trackers, understanding users' perceptions could inform novel and usable privacy-preserving strategies for designers.

[3]Note that this would not guarantee the users' privacy, as the data could be leaked during the time it would be available to the service provider or the users.

[4]Note that the ability to reduce the granularity of the recorded data is available in some fitness tracker models. For example, the Fitbit Inspire HR enables disabling heart-rate recording, but not other sensors [26, p. 17]. These settings could be hidden in the Fitbit tracker software, hence most users are likely not aware of their existence.

3 METHODOLOGY

To answer our research questions, we organized a longitudinal study involving $N = 227$ individuals. Our study was based on another study conducted over a four-month period, from May 2020 until September 2020.[5] This other study had another research goal (not reported in this paper). It was designed to evaluate whether personality traits could be inferred from step counts collected by fitness trackers. Building on this other study, we had access to a group of participants who used the same wearable-device model and the same companion app. This choice ensured that the participants had been exposed to the same type of technology for a similar amount of time. We deployed an online survey and conducted semi-structured interviews with a sub-sample that demonstrated interesting behaviors with regard to the use of the fitness trackers.

3.1 Apparatus

The purpose of the other study was to collect the fitness tracker data of a set of participants who use a specific model of fitness tracker, namely the Fitbit Inspire HR. We chose this specific tracker as Fitbit trackers have often been used in research [39] due to their reliability [5, 39]. Furthermore, Fitbit is one of the market leaders for life-style tracking devices for the general public [39, 43, 62], and Fitbit provides a convenient Web API to third parties for accessing user data (using OAuth[6]) [27, 28, 39]. Furthermore, the Fitbit Inspire HR was a *general* purpose fitness tracker with a large user base. It also collects a wide range of data types (including step count, activities, sleep, and heart rate). Each participant was provided with a Fitbit Inspire HR, which we purchased for the study. At the start of the study, our participants had to create a Fitbit account and grant us access to their data by using the Fitbit API; thus, we could retrieve their fitness data from Fitbit's servers through the provided APIs. For each participant, we collected the following information from their Fitbit accounts: the number of steps taken every minute, the average heart rate every minute, sleep related information (i.e., bedtime, wake-up time, and sleep phases), and the sports activities that are automatically detected by the device.

3.2 Participant Recruitment

The participants were recruited through LABEX, a dedicated structure at the University of Lausanne that organizes behavioral studies with a pool of around 8000 students. These students came from the University of Lausanne (UNIL) and the École Polytechnique Fédérale de Lausanne (EPFL), which are located in the same geographical region. The participants were contacted by e-mail and those who showed interest in the study had to fill a screener questionnaire. The screener allowed us to verify the eligibility of potential participants and to ensure some diversity in terms of gender and field of study. More specifically, the selection criteria were (1) to own a smartphone that is compatible with the Fitbit application, (2) to possess sufficient mastery of French,[7] and (3) to not be current users of fitness trackers to avoid that they use their own device instead of the one we provide.[8] A total of 981 individuals answered the screener questionnaire and 429 were eligible with respect to the aforementioned criteria. According to the number of devices at our disposal, and with one participant dropping out,[9] we finally collected data from 227 individuals.

[5]The effect of the COVID-19 pandemic on our participants' lives was limited as most venues (including shops and restaurants) were open and there was no lock-down in the region where the study was conducted. To verify this claim, we checked the participants' fitness data. On average, they walked 8523 steps per day ($STD = 2850$). These numbers are similar to statistics published by Fitbit [55] that show Swiss people walk around 9000 steps per day.
[6]https://oauth.net/2/, last visited: Feb. 2021.
[7]The surveys, which contain (official translations of) standardized questionnaires, and the interviews were conducted in French.
[8]We did not exclude participants who had used fitness trackers in the past.
[9]Due to having an allergic skin reaction to the wristband of the fitness tracker.

3.3 Procedure

The participants, one at a time, enrolled in the study and picked up their tracker. We explained the conditions of participation, the data that would be collected, the associated data-management plan, and the procedure for withdrawing from the study (in case they chose to do so). The participants could withdraw from the study at any point and, if they did so, the data we collected about them would be deleted. The participants had to sign a consent form with all the aforementioned information. The participants had to wear the tracker throughout the day, but could choose to wear it at night or not.

As a financial incentive the participants were paid 60 CHF (≈ 67 USD) at the end of the study and were allowed to keep the tracker. Our study was approved by our institutional review board (IRB).

At the end of the study, the participants had completed an exit questionnaire that we describe in Section 3.4. This exit questionnaire included a question asking the participants whether they would be interested in participating in a follow-up interview that we describe in Section 3.5. Interviewees were paid an additional 35 CHF (≈ 38 USD) for participating. These follow-up interviews were conducted three months after the end of the data-collection period.

3.4 Design of the Survey

The questionnaire was designed to collect information about various aspects of how fitness trackers are used. Specifically, we designed questions around the level of concerns that participants have with fitness trackers and the privacy risks that they could foresee. We also probed the participants' knowledge about the concept of information inference. The survey questions were designed collaboratively by all the research members to provide relevant data to the research questions. After an initial draft of the survey was ready, each team member iterated the document by providing comments, refining the language and the instructions, and by testing the logic of the questions. The survey comprised 25 items spread over 10 sections. An English transcript of the survey can be found in Appendix B.[10]

Sec. 1 This section contained demographic questions (e.g., gender and faculty in which the participants study) to characterize our sample and to configure the skip-logic of the rest of the survey questions.

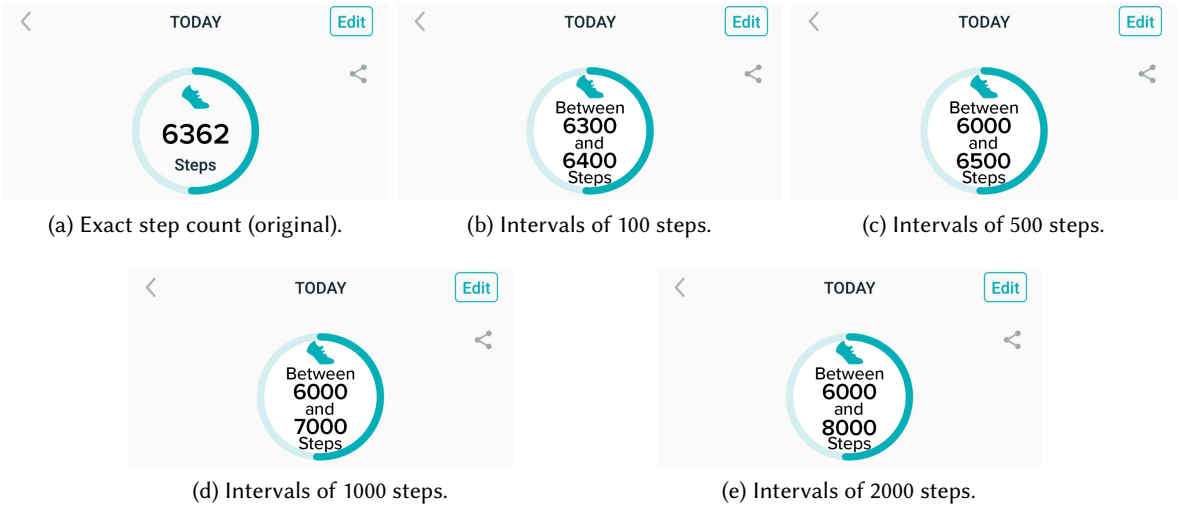
Sec. 2 This section focused on the participants' self-perceived privacy risks regarding the use of fitness trackers (cf. RQ2), and it sought to understand which privacy-related actions participants might have taken during the study (cf. RQ4). The privacy-related-actions question contained a predefined list of actions, including reading Fitbit's terms and conditions and changing the privacy settings in their Fitbit account. These actions were selected based on the options that can be found within the Fitbit app and website and were also informed by the results of a previous study [34].

Sec. 3 This section focused on the participants' knowledge about the hardware of the tracker (cf. RQ3) and about which sensors they would disable to protect their privacy (cf. RQ4). The sensors list consisted of all those *actually* embedded in the Fitbit Inspire HR and of several sensors embedded in *other* devices. We chose to include sensors that are not actually embedded in the device, in order to better gauge the participants' technical understanding.

Sec. 4 This section collected the participants' perceived likelihood of (and concerns about) certain types of information being inferred (cf. RQ2). The information types were selected either based on previous studies (e.g., alcohol consumption [7], illegal drug consumption [83]), or based on the EU General Data Protection Regulation (GDPR)[11] (e.g., religious beliefs, political opinions, sexual activity, and sexual orientation [100]).

[10] A transcript of the original survey in French is available on the Open Science Framework repository. See https://doi.org/10.17605/OSF.IO/56EXZ, last accessed October 2021.

[11] See https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed October 2021.



(a) Exact step count (original). (b) Intervals of 100 steps. (c) Intervals of 500 steps.

(d) Intervals of 1000 steps. (e) Intervals of 2000 steps.

Fig. 1. Alternative UIs for daily step counts (as would be seen in the Fitbit app). The participants had to rate the utility of the different levels of information shown in each variant, thus enabling us to evaluate the potential for data minimization by using ranges instead of precise values.

Sec. 5 This section sought to understand which data types collected by the tracker participants find useful (cf. RQ1), and to assess the frequency of use of each platform for viewing (1) step and heart-rate data, and (2) sleep data. We group step- and heart-rate data together, as they are calculated on the fitness tracker, whereas sleep data is calculated on Fitbit's servers. The purpose of these questions was to evaluate the potential for *data minimization* as a means of privacy protection.

Sec. 6 This section asked how many times per *day* the participants removed their tracker and why they did so (cf. RQ4). If participants selected that they removed the tracker for privacy reasons, they were given an additional question asking about which privacy related reasons they removed it. We identified the predefined options, before running the survey, by deploying a short survey with open-ended questions among 33 fitness-tracker users.

Sec. 7 This section focused on how often the participants wore their tracker at *night* and why they chose not to wear it (cf. RQ4).

Sec. 8 This section asked the participants for their preference in terms of how precise the data displayed in the Fitbit app should be (cf. RQ1). In Q20, the participants were presented with alternative UI designs (as would be seen in the Fitbit app) where, instead of a precise step count, they would be shown a step interval (see Figure 1). In Q21, the participants were asked about the time span of data that they like to review when looking at their historical data. In Q22, the participants were shown graphs representing different levels of aggregation of their number of steps made throughout the week. The purpose of this block of questions was to understand the potential for data minimization (cf. RQ1).

Sec. 9 This section asked respondents to make a drawing of how they thought their data was processed and transferred across the various components of the Fitbit ecosystem. We asked the participants to draw this by thinking about either step data or sleep data (cf. RQ3). Analyzing drawn mental models [70] has gained traction in security and privacy research [49, 57, 65, 79]. Mental models are instrumental for analyzing users' *tacit knowledge* (i.e., subjective and implicit assumptions) about how things work. Such knowledge

often cannot be easily verbalized [65]. To this end, we provided the respondents with a template (see the template figure in Q23) including example elements they could use in their drawings.

Sec. 10 This section contained the Internet Users' Information Privacy Concerns (IUIPC) [69], which measures the respondent's level of privacy concern (cf. RQ2).[12]

Sec. 11 This section asked respondents whether they would be willing to participate in a (paid) follow-up interview (see Section 3.5).

We initially designed the questions in English. Later, one of the authors translated them into French. Three authors checked and revised the questions in French. To further refine the questions before deploying the survey, we conducted two cognitive pre-tests with individuals outside our institution. Both individuals have used Fitbit fitness trackers for several years and are fluent in French. One of the authors created a meeting over Zoom with each participant and asked them to share their screens. Each participant was asked to rephrase each question in their own words, to explain what each question was asking, and how they would answer it. The feedback was used to clarify and improve the phrasing (e.g., for Q23 adjusting and clarifying the instructions for what participants have to do), to change the available answer options (e.g., for Q14, replacing semantic options such as 'Often', with concrete ranges like '1–2 times per day'), and to adjust the formatting (e.g., emphasizing keywords by making them bold and underlining them). The order of the answer options was randomized to avoid possible carryover and presentation effects. The order of questions was chosen to avoid priming the participants. The survey was developed and deployed using the Qualtrics online survey platform. Respondents filled the survey online.

3.5 Interview Protocol and Participants Selection

In order to better understand our participants' perception of Fitbit devices, we conducted semi-structured interviews with 19 participants who completed the exit survey. Our goal was to delve deeper into three topics: (i) their privacy concerns in general and with regard to the tracker, (ii) their views on the utility of the tracker, and (iii) their mental models regarding the functioning of the Fitbit ecosystem and, in particular, regarding data processing and transfer.

To develop the interview questions, we relied primarily on the exit-survey results. We identified the questions that we wanted to explore in greater depth. We reviewed the proposed questions internally and then conducted one cognitive pre-test with one of the individuals with whom we had done cognitive pre-tests for the exit survey. We created a customized interview script for each participant, based on how they answered the exit survey. During the interviews, for various questions, we showed the interviewees their answers to some questions in the exit survey and asked them to elaborate further. This enabled us to capture the participants' reasoning behind the answers they gave in the exit survey. As the interviews were semi-structured, we adapted the interviews to what the participant was saying during the conversation, we delved deeper where necessary and skipped questions that we felt were no longer relevant. The protocol for the interviews is available on the Open Science Framework repository.[13]

In order to increase the diversity of opinions about privacy issues relating to the trackers, we determined four categories of participants, based on their tracker-wearing habits, as follows. Participants who:

G1. *Frequently* removed the tracker during the day and who *rarely or never* wore it at night.
G2. *Frequently* removed the tracker during the day and who *often or always* wore it at night.
G3. *Rarely or never* removed the tracker during the day and who *rarely or never* wore the tracker at night.
G4. *Rarely or never* removed the tracker during the day and who *often or always* wore it at night.

[12] We used only items (2), (3), and (6) to calculate the score, as suggested by the IUIPC developers [69, p. 353].
[13] See https://doi.org/10.17605/OSF.IO/56EXZ, last accessed October 2021.

We aimed to recruit two men and three women per group, thus roughly matching the gender distribution of our entire pool of participants (see Section 3.7). However, not enough people from each group agreed to be interviewed. We randomly sampled the participants from those who indicated they would be interested in participating in follow-up interviews; we grouped them into the four aforementioned categories; and we looked at their answers for Q10 to ensure a diversity of privacy concerns relating to fitness trackers.

We interviewed each participant individually. We conducted 14 in-person interviews and 5 Zoom interviews. Some of our questions were related to the mental models that participants had drawn during the exit survey. The interviews lasted ~ 40 minutes on average for each participant.

3.6 Coding Processes

3.6.1 Interviews. To analyze the interview data, we first transcribed the audio records. We read the transcripts and selected the relevant quotes from the participants. Next, two authors developed the codebook with open coding [90], thus labeling the selected quotes. Using the main topics arisen from our survey data (e.g., respondents' concerns about data inference), we searched for individual narratives or anecdotes that could explain our survey findings.

3.6.2 Mental Models. To analyze the mental-model data, we chose to focus on three aspects in order to gauge how well the participants understand how information flows through the fitness tracker ecosystem. We phrased these aspects as the following questions:

(1) Does the data go through the smartphone, tablet, or computer (i.e., henceforth a 'connected device')?
(2) Does the data go through the connected device to the server, then back to the connected device?
(3) Does the tracker receive non-relevant data?

Using these questions, we categorized the participants' mental models into three main types: (i) correct models, (ii) incomplete models, and (iii) incorrect models. These three categories were derived from previous studies on mental models (for examples in various contexts see: computer security [103], cryptocurrency [65], HTTPS [57], and secure communication [1]). We will further explain these three categories in Section 4.3.

3.7 General Participant Statistics

The survey took an average of 32 minutes to complete. A total of 227 participants completed the exit survey. Table 2 in Appendix C shows the participants' distribution by age range and gender. Given that prior research identified gender differences on users' self-tracking practices [85] and their online privacy concerns [8, 86], it is necessary to collect data from all genders. The distribution by gender was 63.0% female, 36.6% male, 0.4% prefer not to answer. Women are over-represented in our sample, compared to the general population. Note that our sample is consistent with the market trend of women being the majority of fitness-tracker users [85]. The ages of the participants ranged from 18 to 33, with an average of 21.62 and a standard deviation of 2.57. The distribution of the major fields of studies was quite diverse, as can be seen in Figure 14 (see Appendix C).

With regard to the privacy concern (IUIPC) scale, the average score was 3.19, with a standard deviation of 1.22 (the score could range between 0 and 6).[14] We fitted the distribution of the IUIPC scores. We found it to be closest to a Truncated Normal distribution ($\mu = 3.21$,$\sigma = 1.31$, $a = -0.01$, and $b = 6.01$). The μ and σ values are the estimated expected mean value and the estimated standard deviation, respectively. The a and b values represent the lower and upper, respectively, cutoff bounds for the distribution. This means that most of our participants' privacy concerns were close to the average level. Figure 2 shows the histogram of the averaged IUIPC scores, together with the fitted distribution.

[14] In the IUIPC 0 is the lowest level of concern, and 6 is the highest level of concern.

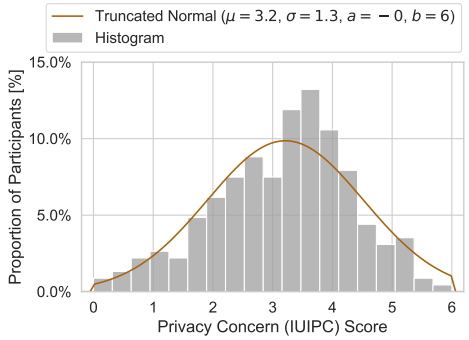


Fig. 2. Privacy concern (IUIPC), with fit.

In the exit survey, 119 participants agreed to participate in a follow-up interview. We interviewed 19 of those participants. Table 3 in Appendix C shows the participants' gender distribution per interview group. We did not achieve our desired quotas per group.

Of our 227 participants, 220 of them submitted their drawings after answering the survey. We first made a quality check and discarded four items because the photos that the participants sent us were not clear or because the participants did not understand the drawing task correctly. Finally, we had 216 drawings to analyze.

4 RESULTS

In this section, we report the analysis of the data collected through our surveys and interviews. We organized the findings according to the main themes of our study.

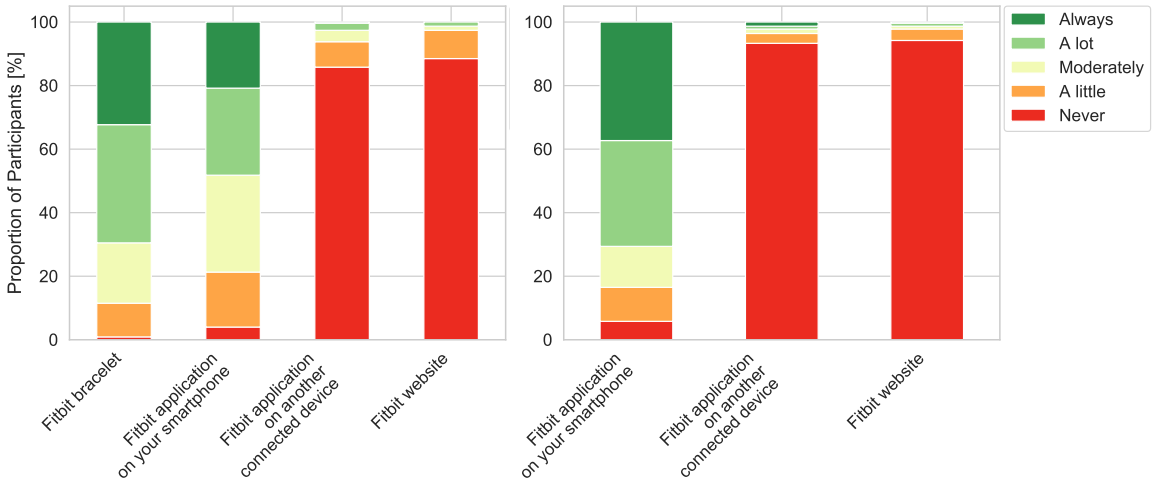
4.1 Participants' Perceptions of the Utility of Fitness Trackers and Potential Privacy Protection Mechanisms

We investigated users' perceptions of the utility of fitness trackers to find potential areas for applying privacy-protection mechanisms. In particular, we looked at applying data minimization by keeping data stored *only* locally on users' connected devices (e.g., smartphones). To do this, we asked participants about which interfaces they used to browse their step or heart-rate data (Figure 3a), and sleep data (Figure 3b). The participants used primarily their tracker and their smartphone to browse their step- and heart-rate data. A vast majority of participants never used other[15] connected devices (85.8%) or Fitbit's website (88.5%). The same trend can be observed with the sleep data in Figure 3b.

During the interviews, we asked participants how they would respond to removing the synchronization feature if it would improve their privacy. One interviewee said that they would not want to lose the synchronization feature, whereas all the other interviewees said that they would either not be affected by it or would even prefer to not have it.

To further our investigation for opportunities of data minimization, we looked at reducing the precision of the collected data. We asked participants how useful they would find the fitness tracker if it showed less precise information. Figure 4a shows how receptive participants are to being shown their step count in intervals rather than having a precise number. From our participants, 31.7% would find 100-step intervals to be useless compared with having the precise number. Furthermore, 55.1% and 74.4% of the participants would find intervals of 1,000 steps and 2,000 steps to be useless compared to the precise number. During the interviews, most participants

[15]Other than the device used for synchronizing the tracker.



(a) Step or heart rate (b) Sleep

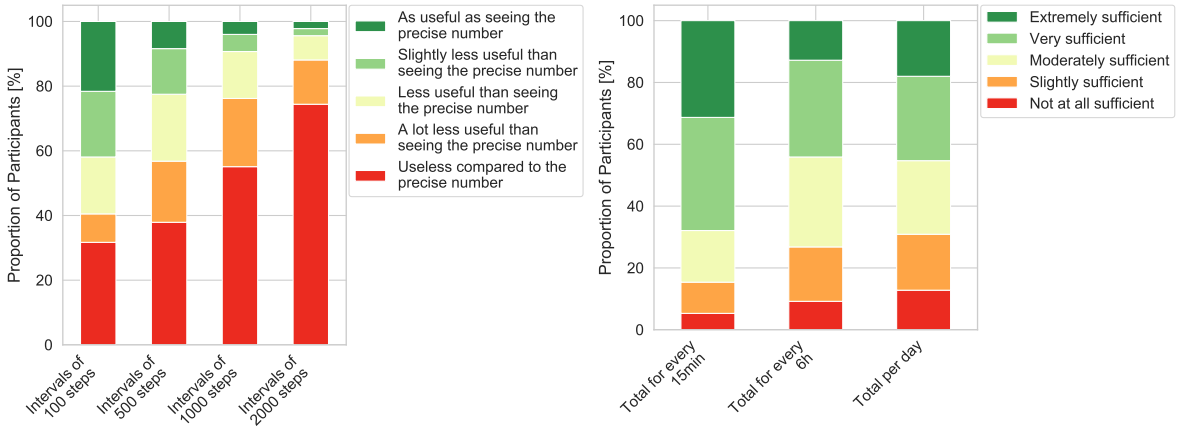
Fig. 3. Frequency of use of each interface to checking step or heart rate (left) and sleep (right) data ($N = 227$). Sleep data cannot be checked directly on the tracker.

explained that having step intervals makes them feel like they are missing out on information and that they would have a hard time tracking their fitness progress. [female, 20 y.o.]: "*I want the precise result at the end of the day, I would feel like I was missing something if it was an interval, because I would have a poor understanding of my step counts.*"

We also asked our participants if they would prefer to have aggregated daily totals, or be able to see them broken down into blocks of steps over time counts. Figure 4b shows that overall participants are indifferent between the options we provided, as they responded positively to each one. During the interviews, 21.1% of the interviewees said that they look mainly at the total steps per hour, 73.7% said that they look mainly at the total per day, and 5.3% said that they do not look at the step count rather at the total distance traveled and the number of active minutes. When we asked them to elaborate on their preferences, the participants who preferred more detailed information said that they like having as much information as possible. [male, 20 y.o.]: "*The more details the better. I like stats, I'm interested in seeing that, comparing my different activity levels.*" The participants who preferred aggregated data explained this by saying that they just wanted to know if they had been sufficiently active during the day. [female, 25 y.o.]: "*I mostly look at the total number of steps per day, per weekend, and per week. I like to compare the days with each other. I have little interest in more detail.*" In summary, we found that, overall, data aggregation is a well received strategy for data minimization. However, some fitness-tracker users (e.g., self-quantifiers) might still want granular data.

4.2 Awareness, Beliefs, and Concerns Regarding Privacy Risks

We investigate the privacy perceptions of the participants. Figure 5 depicts the proportions of participants for each level of self-reported privacy awareness. We observed that more than half of the participants (58.1%) think that they are at least slightly aware of the privacy risks associated with fitness-trackers.



(a) Step counts intervals

(b) Aggregated step counts

Fig. 4. Relative utility of less precise fitness data ($N = 227$).

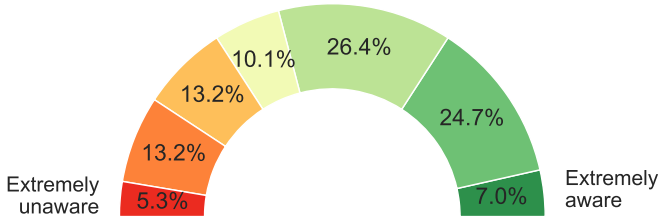
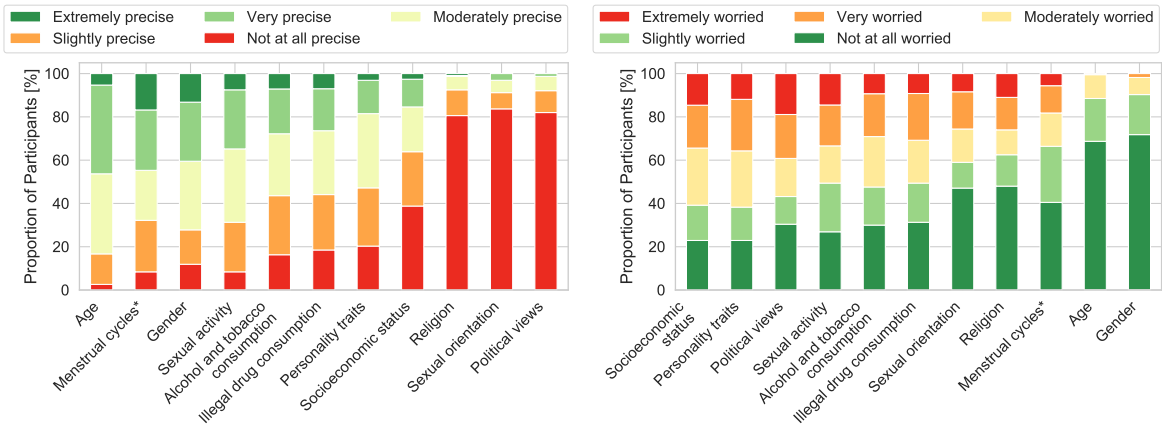


Fig. 5. Participant self-reported awareness of privacy risks associated with fitness trackers ($N = 227$).

In order to understand the beliefs of the participants about the personal information that can be inferred, we asked them to report the precision that they think several types of sensitive information could be inferred from fitness tracker data. As shown in Figure 6a, a large majority of the participants realized and indicated that age, sexual activity, menstrual cycles, and drug consumption could be inferred from fitness tracker data with a moderate (or higher) precision. The participants' opinions diverged regarding personality traits. Almost all participants thought that religion, political views, and sexual orientation could not be inferred from fitness tracker data.

When we asked the participants to explain their intuitions about the privacy inferences, one of them mentioned, [female, 21 y.o.]: "*[Age, Illegal drug consumption, etc.] are inferable because they are physiological data types.*" Whereas, the participants saw no link between their fitness data and non-physiological types of information such as 'religion' and 'political views'. Furthermore, several participants think certain types of information can be inferred accurately. [female, 21 y.o.]: "*... because they can be entered in the app.*" This indicates that there could have been a misunderstanding of what 'inference' is, as compared to having access to the data directly.



(a) Participants perceived precision of inferring various types of sensitive information from their fitness data (N = 227).

(b) Level of worry if certain types of sensitive information could be inferred accurately from fitness tracker data (N = 227).

Fig. 6. Participants perceived precision of inferring various types of sensitive information and their level of worry if those types of information could be inferred accurately. *The results for menstrual cycles were calculated only for participants who reported their gender as female.

Figure 6b depicts the levels of concern regarding privacy inferences of different types of information. The types of information that a majority of participants were concerned (i.e., for which participants reported being at least 'moderately worried') about are personality traits (61.7%),[16] Socioeconomic status (60.8%), political views (56.8%), alcohol and tobacco consumption (52.4%), sexual activity (50.7%), and illegal drug consumption (50.7%).

During the interviews, the most often cited reasons for worrying about these types of information were related to avoiding targeted advertising (e.g., [male, 21 y.o.]: "*... being manipulated by targeted advertising.*") and fearing social rejection by peers or family members (e.g., [female, 20 y.o.]: "*... my family would not approve if they knew I did that [alcohol and drug consumption].*").

Age and gender were the attributes that participants were the least worried about, wherein 68.7% of the participants said they were not at all worried about their age being inferred and 71.8% said they were not worried about their gender being inferred. In the interviews, some participants reported that they were typically not worried about these types of information as they can be easily observed. Age and gender need to be provided when creating a Fitbit account. Hence, the participants' willingness to create one to participate in the study is another indicator that they are not worried about them.

Surprisingly, many participants reported not being worried about if their sexual orientation or religion could be inferred. During the interviews participants told us that they were not worried because they live in a "...safe country." (mentioned by [male, 25 y.o.], [male, 21 y.o.], [male, 20 y.o.]). However, if they were to live in a country where they could be subject to persecution, then they would be very concerned. For example, a Muslim participant said [male, 20 y.o.]: "*... if I lived in [redacted], I would be very concerned about my religion being inferred.*" In conclusion, our findings showed that the users' concerns about the inference of certain types of information (e.g., religion and sexual orientation) are highly dependent on the conditions in their country of residence.

[16]This is consistent with [52].

4.3 Understanding of the Information Flow in the Fitness-Tracker Ecosystem

We analyzed the mental-model drawings based on the aforementioned criteria (cf. Section 3.6.2). In terms of the elements used in the mental-model drawings, 40.3% of the participants depicted only the three essential elements in their drawings, including a tracker, a smartphone (or a tablet), and a Fitbit server. The remaining 59.7% used additional elements, including personal computers or laptops (86.3%), items related to the Internet (18.3%, e.g., other servers, Wi-Fi routers, data centers, or ISPs), and others (3.1%, e.g., satellites[17] and third-party apps).

Our findings showed that only 20.8% of the participants have the correct mental model. The correct model should contain at least a tracker, a connected device, and Fitbit servers (cf. Appendix A). The correct flow of information is where information flows from the tracker to the connected device, from the connected device to the servers, and finally, from the servers back to the connected device in order to visualize the analyzed data (see an example in Figure 7a). Note that the tracker could not receive the processed data (e.g., sleep graph), and could only receive limited information from the connected device. For instance, the tracker receives information for configuration and status updates (e.g., during the synchronization process, to update the time and calendar, or to receive notifications on the tracker).

The remaining 79.2% of the participants drew either incomplete or incorrect mental models. For the incomplete mental models (24.6%), we found three types of minor mistakes in the participants' drawings:[18] (i) 16.2% of the participants think that the flow of information between their tracker and smartphone is one-sided (e.g., Figure 7b). This is incorrect because the tracker can also receive information from connected devices such as notifications, as mentioned above (cf. explanation of the correct model). (ii) 6.5% of the participants think that their tracker can receive the processed data from a connected device. The trackers do not receive processed data (e.g., sleep graphs); and such data is visualized on a connected device (via the Fitbit app) or on the Fitbit website. (iii) 1.9% of the participants think that information always flows from their smartphone to the Fitbit servers and that no information is sent back to their smartphone. In other words, the participants think all the processing of their data occurs on their smartphone and not on the Fitbit servers.

For the incorrect mental models (54.6%), we distinguish four types of technical misunderstandings: (i) The most common misunderstanding (28.7%) was for participants thinking that their tracker can directly contact the Fitbit servers without passing through their smartphone, by using Bluetooth, WiFi, or satellites (e.g., Figure 7c).[19] (ii) The second most common misunderstanding (19.4%) was related to the participants who thought their trackers receive the processed data directly from the Fitbit servers. (iii) The least common misunderstanding (1.9%) was from the participants who think their fitness data goes from their tracker to their smartphone, from their smartphone to their computer, and then from their computer to the Fitbit servers. But in fact, smartphones or computers can directly connect to both the trackers and the Fitbit servers; and they cannot exchange the information with each other.[20] Last, the remaining 4.6% of the mental models included combinations of the mistakes mentioned above.

We also considered if participants illustrated any recipients or third-party elements in their drawings. Such elements can reflect the participants' privacy concerns and their perceptions regarding potential threats. Roughly 1 out of every 10 (11.1%) participants reflected their privacy concerns in their drawings. Among these participants, 33.3% drew third-party organizations that, such as giant tech companies, could utilize their data without obtaining their consent. 29.2% of the participants mentioned that the fitness company could sell their data to their business partners. Participants also suspect that advertising agencies (12.5%) or insurance companies (4.2%) are buying their data. 8.3% of the participants drew intelligence agencies (e.g., the CIA) that could exploit fitness data for

[17] Note that three drawings had the satellite element. Only one of them used a satellite for sending fitness data. The other two were for positioning (i.e., GPS).
[18] We designated the models with only one minor mistake as incomplete.
[19] Interestingly, one participant (0.5%) thought the tracker and the Fitbit server connect via satellites (e.g., Figure 7d).
[20] Note that a computer with Bluetooth technology can directly connect to the tracker without requiring a USB dongle.

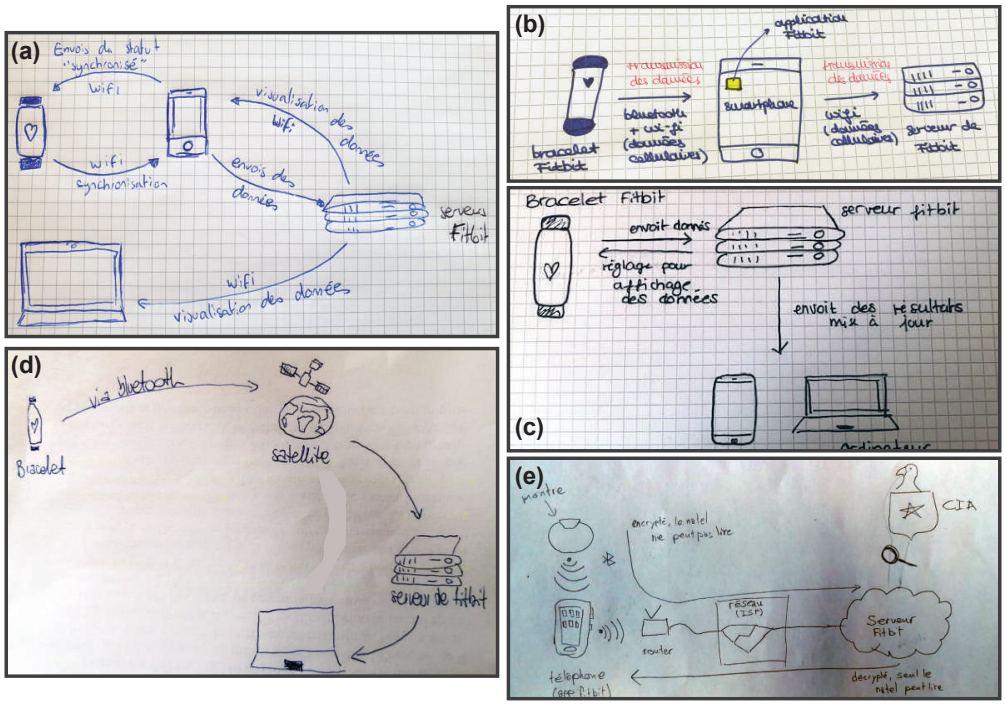


Fig. 7. Samples of the participants' mental models: (a) a correct model, (b) an incomplete model, (c) an incorrect model, (d) an interesting mistake, (e) an (incomplete) model depicting third-party threats.

their benefit (e.g., Figure 7e). The remaining 16.7% believe that their data was used for research purposes, to collect statistics by governments (e.g., census), and was shared on online social networks.

During the follow-up interviews, we showed participants their own drawings and asked which part(s) of their drawing they think can cause privacy risks and why. More than half of the interview participants (52.6%) mentioned Fitbit servers as the vulnerable part in their drawing. Most of these participants mentioned security issues, in which Fitbit servers could be penetrated by hackers. The second most reported reason was the lack of trust in the fitness-tracker company, as it could sell users' fitness data to third parties. The participants also mentioned a lack of control over their data. [female, 25 y.o.]: "*I have no control over my data on the Fitbit server, I will never know what has really been done with my data there.*" One participant also mentioned that wearing fitness trackers could have some implications in totalitarian countries, as the government could access the servers and track some users.

26.3% of the participants had concerns about how their data is communicated from their tracker to their smartphone, and subsequently to the Fitbit servers. Some participants think that Bluetooth is not a secure connection and can be attacked. [male, 21 y.o.]: "*The Bluetooth version used with the tracker is not secure, it is not encrypted and is easy to hack, especially because it is always activated.*" Some others mentioned that there are security issues with Wi-Fi connections. [female, 19 y.o.]: "*When data is sent from my smartphone to the server using Wi-Fi. If that [Wi-Fi] is hacked by someone they could get my information [the participant drew a man in the middle].*" Some participants pointed to the Internet, in general, as being insecure; but they could not give a concrete example of threats. [female, 20 y.o.]: "*My information can be hacked when it is exchanged between the*

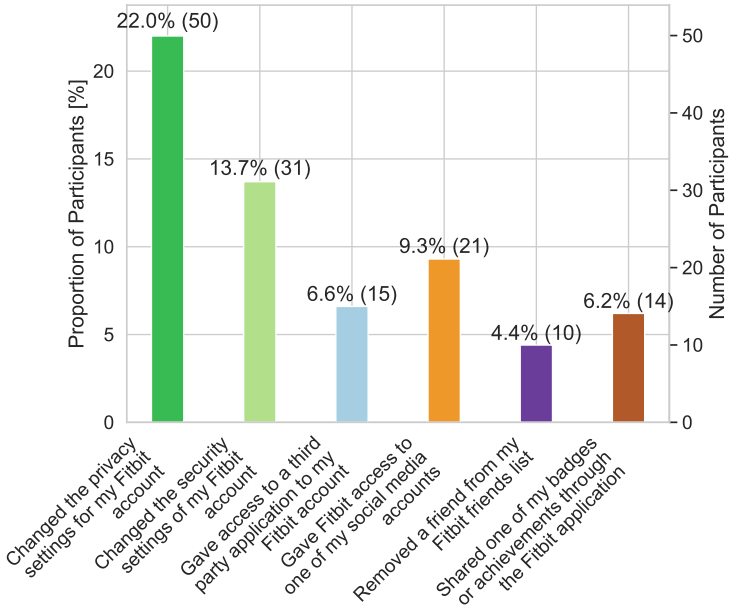


Fig. 8. Various actions that participants had taken that can either preserve or reduce their privacy ($N = 227$).

server and my smartphone because the server location is far, and [I'm] not sure where compared to the smartphone or tracker."

Some participants said that their own devices were the vulnerable parts in their drawings, including their trackers (10.6%), smartphones (26.3%), and computers (15.8%). Overall, these participants thought that adversaries could attack these devices because they collect or store their data. Last, one participant (5.3%) mentioned that every single point in the drawing is a potential source of risk. We also observed that most of the participants were not able to give concrete examples of threats.

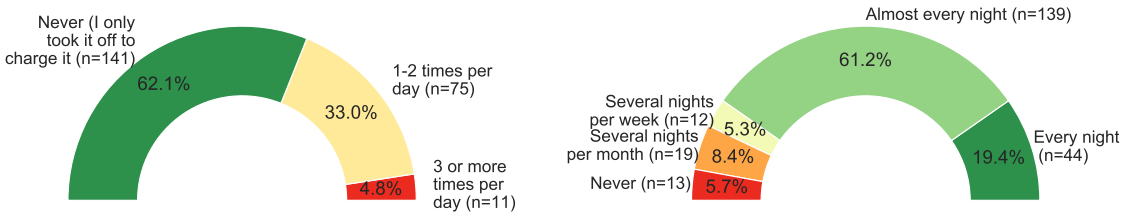
In conclusion, our findings show that (i) most of the fitness-tracker users have either incomplete or incorrect mental models, (ii) only a small portion of the fitness-tracker users reflected privacy concerns or security threats in their drawings, and (iii) although the interview participants mentioned many points in their drawings, they perceived fitness-tracker servers as the most vulnerable and concerning part. We will discuss these findings and the potential implications for design in Section 5.3.

4.4 Privacy-Preserving Actions

We further analyze whether the participants took various privacy-related actions, and more specifically whether they removed their fitness trackers throughout the day and whether they wore them at night.

Figure 8 shows the number of participants that performed each type of privacy-related action. A minority of participants performed these actions. The two most common actions were changing the privacy settings in their accounts (22.0%) and changing the security settings in their accounts (13.7%).

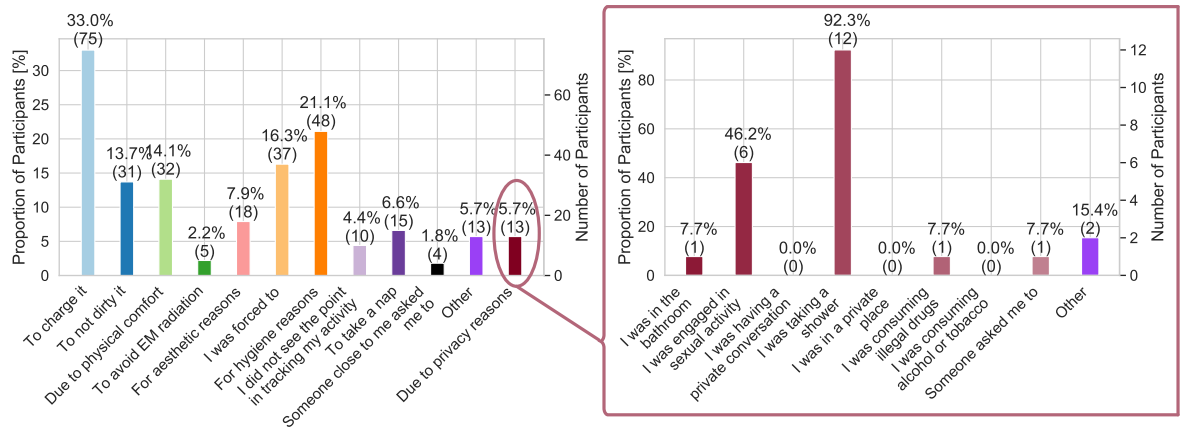
During the interviews, we asked participants whether they were aware of the existence of such options within the Fitbit app and/or website. Most of them said that they were not aware of the existence of the options/functions



(a) Frequency of **removal** of the fitness tracker throughout a typical **day** ☼.

(b) Frequency of **wearing** the fitness tracker at **night** ☾.

Fig. 9. Participants' self-reported fitness tracker removal during the day and wearing frequency at night (N = 227).



(a) General reasons for removing the tracker during the day ☼ (N = 227).

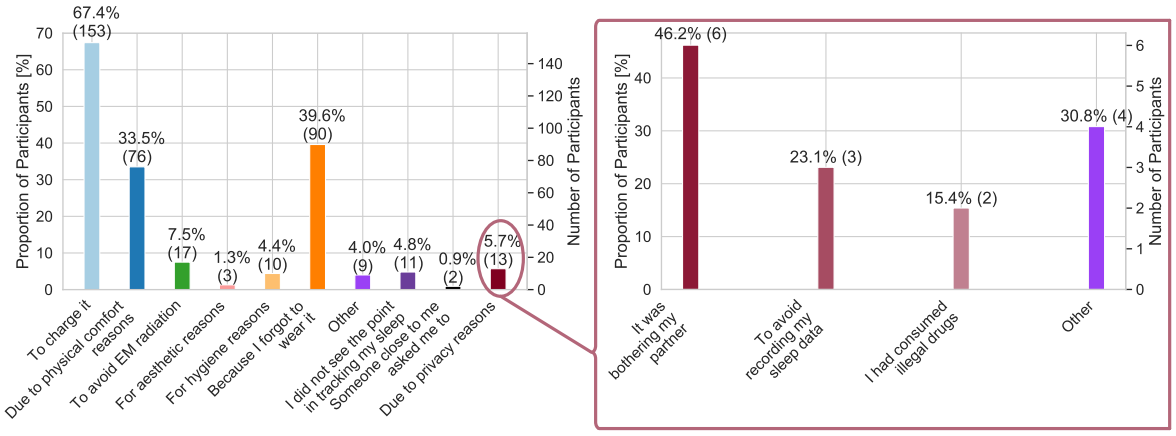
(b) Privacy-related reasons for removing the tracker during the day ☼ (N=13).

Fig. 10. General and privacy-related reasons for removing the fitness tracker during the day ☼.

(e.g., [female, 25 y.o.]: "*I didn't know that you could do that [change your privacy settings].*"); others said they were not interested in using them (e.g., [male, 24 y.o.]: "*I did not see the point in doing that [giving access to a third party application].*").

Figure 9a shows how often participants reported removing their Fitbit tracker during the day. A majority of participants (62.1%) reported removing the tracker only to recharge it. One third of the participants reported removing their trackers once or twice per day. Few participants (4.9%) removed their tracker three or more times per day.

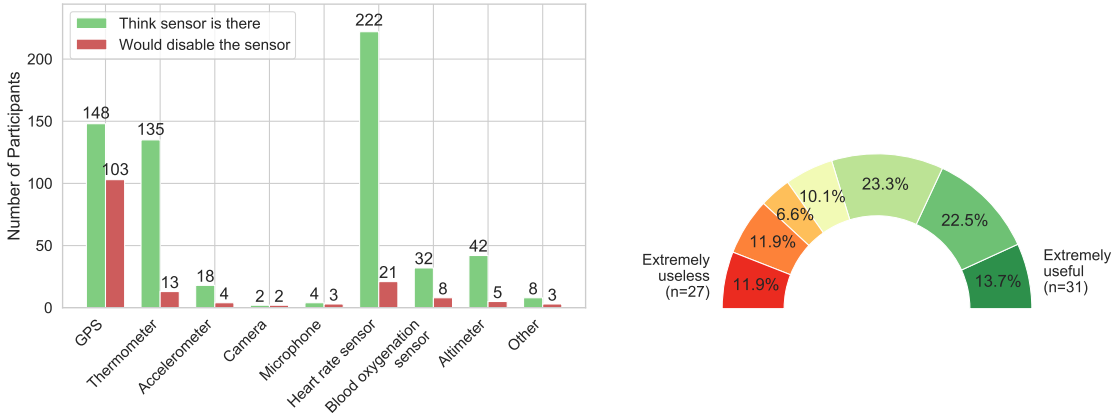
Figure 10a shows the general reasons, and Figure 10b shows the privacy-related reasons for removing the tracker during the day. Most of the participants reported that they removed their trackers for reasons other than privacy. For example, 33.0% of the participants reported removing their trackers to recharge them, 21.1%



(a) General reasons for not wearing the fitness trackers at night ☾ (N = 227).

(b) Privacy-related reasons for not wearing the fitness trackers at night ☾ (N=13).

Fig. 11. General and privacy-related reasons for not wearing the tracker at night ☾.



(a) Participants' perception of which sensors are embedded in the fitness tracker and which ones they would disable to protect their privacy.

(b) Perceived effectiveness of disabling sensors as a means of protecting their privacy.

Fig. 12. Participants' perception regarding the sensors embedded in the fitness tracker and privacy protection (N = 227).

removed the device for hygiene reasons, and 16.3% removed their device because they were "forced" to (e.g., for security checks at airports). Only 5.7% of the participants said they removed the tracker for privacy reasons.

Out of those who reported removing the tracker for privacy reasons, 92.3% mentioned taking a shower.[21] The second most common privacy-related reason was engaging in sexual activity (46.2%), e.g., one participant wrote in the free text field, [male, 24 y.o.]: "*... because I was masturbating.*" During the interviews, the participants who removed the tracker frequently told us that it was mainly to recharge it, to avoid getting it wet, or because it was uncomfortable. This is inline with the survey results.

We analyze how frequently participants wore their fitness tracker at night.[22] Figure 9b shows the participants' self-reported the frequency of wearing at night. The results show that more than half of the participants wore the tracker almost every night during the study. Furthermore, only 5.7% of the participants reported 'never' wearing the tracker at night.

We asked the participants for which reasons they did not wear their trackers at night. Figure 11a shows that the majority (67.4%) of the users reported recharging the fitness tracker as one of the reasons they did not wear it. The other two most often mentioned reasons were forgetting to wear it (39.6%) and finding it physically uncomfortable (33.5%). As with the daytime removal results, only 5.7% of the participants reported removing the trackers for privacy reasons. From these participants, 46.2% reported not wearing it to avoid bothering their partner, 23.1% said that they did not want to have their sleep data recorded, and 15.4% reported that they had consumed illegal drugs (see Figure 11b). Almost one third of the participants (30.8%) wrote in the text field sexual activity, or to hide that they were staying up all night, or going out with friends. During the interviews, several participants mentioned being concerned if other people could find out about their nocturnal activities. One participant did not want to have her fitness tracker data recorded when she attended a rave party at night. [female, 20 y.o.]: "*I took it off because I went to a rave [at night] and I didn't want any data to be collected at that time, any type of data, about me but also about others*"

Next, we asked our participants which sensors they believe are present in the fitness tracker, and which sensors they would disable to protect their privacy (see Figure 12a). Correctly, almost all participants (97.8%) reported that the fitness tracker has a heart-rate sensor. In contrast, only 7.9% participants mentioned that the fitness tracker has an accelerometer which is used to detect physical movements (e.g., step count, running) [26]. Erroneously, a majority of participants believe that their fitness tracker has an embedded GPS (65.2%) and/or a thermometer (59.5%) sensor. Surprisingly, a few participants reported that they believe their tracker has a camera (0.9% participants) and/or a microphone (1.8% participants)[23]. Almost half of the participants (45.4% participants) expressed their desire to disable the GPS sensor on their tracker. Roughly one in ten participants (9.3% participants) mentioned that they would disable their heart-rate sensor.

We asked the participants how useful an option to disable sensors would be in terms of preserving their privacy. Figure 12b shows that more than half of the participants (59.9%) would find such option 'slightly' to 'extremely' useful.

5 DISCUSSION

In this section, we discuss our findings about users' perceptions of the utility of their fitness trackers, and we highlight opportunities for designing privacy-preserving techniques in the context of data minimization. We also discuss the results that shed light on fitness-tracker users' perception about personal-data inference, and their understanding of the fitness-tracker ecosystem.

[21]There could be some overlap between the participants reporting removing the tracker for hygiene reasons in the general reasons and showering in the privacy reasons. Although showering in and of itself might not be a private activity, the participants can engage in private activities while showering (e.g., sexual activities).

[22]Note that we did not instruct participants to wear the trackers at night.

[23]Note that even though the fitness tracker we provided did not have a microphone, some new Fitbit smartwatches (e.g., Versa 3) indeed have built-in microphones. The results show that some participants were not aware of the differences between fitness trackers and smartwatches. But it is likely that in the future, fitness trackers will also be equipped with microphones.

5.1 Opportunities for Data Minimization — RQ1

Our findings show that, to browse any of their fitness data, most participants do not use the website or *additional* connected devices other than their main mobile phone. Hence, there is a high potential for data minimization by removing the online synchronization feature (i.e., not sending the fitness data to Fitbit servers). Note, however, that online synchronization is also used for data backup and some data processing. Removing the online synchronization functionality without a large effect on the utility of fitness trackers for users would be possible only for step and heart-rate data, as it seems that sleep data is processed on Fitbit's servers and not locally on the tracker or smartphone. Hence, users who perceive much utility from recording their sleep data could be unwilling to exchange utility for privacy. An alternative solution could be modular synchronization, wherein a user can select which data is synchronized. This could be implemented in the privacy-settings section of the companion app/Fitbit website, where a user would be presented with an list describing which data would be synchronized and why, and next to it there would be a toggle button to enable or disable synchronization for that data.

Furthermore, fitness tracker companies usually have a vested interest in not reducing the data flow from their users. For example, having the capacity to collect more user data is part of Fitbit's value proposition for business-to-business (B2B) customers [31].[24] Fitbit uses this data to improve its own products and services. Furthermore, it provides services and access to user data to third parties (such as employee-health monitoring for employers [29]). Therefore, the most likely way to enforce such a change would be via government regulations, such as the GDPR. For instance, new legislation could force fitness-tracker companies to make centralized data collection an 'opt-in' option. This would enable privacy-concerned users to still use the device without affecting their utility.[25]

We found that it could be acceptable to only offer the largest level of data aggregation for step counts (i.e., the total per day) without negatively affecting the participants' perceptions of the tracker's utility. Hence, an alternative approach to data minimization could be to store only the users' aggregated step data on the servers. However, Fitbit might not want to reduce their data flow. But as the data flow is not cut-off entirely, Fitbit might be more willing to accept such a change. This could be implemented as either a standard for all users, or as an opt-in option available in the privacy settings.

Our findings indicate that adopting step intervals, instead of the precise number of steps, would not be an acceptable data-minimization strategy, as it would greatly harm the users' perception of the tracker's utility. Even though the precise number would be still available on the bracelet, our participants were not willing to accept a reduction in the accuracy of the reported step data in the connected fitness app installed on their mobile phone. Their reticence towards step intervals could be explained by the endowment effect [46], or more broadly by Prospect Theory [47]. The participants can view the loss of accuracy as a loss from their current reference point, hence they do not want to accept it without any apparent gain.

In conclusion, the overall best solution to protect users' privacy in terms of data minimization would be to stop the centralized data collection. Government regulation would be beneficial for enforcing fitness tracker companies to no longer collect all their users' data. As for more granular-data minimization, users do not want to have obfuscated step counts, hence this is likely not the best avenue for protecting users' privacy. However, users could be open to having only their aggregated daily total-step counts stored on the companies' servers.

[24] 'Business-to-business' refers to when a given company sells their products and/or services to other companies, rather than directly to consumers [56, pp. 20–21].

[25] N.B. some fitness-tracker manufacturers offer the option to enable/disable specific or all online synchronization and data-processing features (e.g., Garmin Connect offers the option to disable all or some data synchronization and processing features). Some of those manufacturers' devices even process all of the data on the tracker/smartwatch (e.g., Garmin's Venu 2 smartwatch performs sleep analysis on the device itself). Hence making this be an industry standard should be feasible.

5.2 Beliefs and Concerns Regarding Privacy — RQ2

Our participants thought that physiological types of information can be inferred with at least moderate precision, whereas non-physiological types of information such as religion cannot be inferred precisely. Our participants' beliefs could be related to their knowledge of the sensors embedded in the device and of the links between the personal information and the data collected by these sensors. Our interview participants mentioned that they tend to identify more direct and concrete links between *personal* characteristics and *physiological* data. For instance, it is well-known that age is correlated with heart rate, which can be captured by the embedded optical heart-rate sensor. Similarly, sexual activity, and to some extent drug consumption (which is known to influence gait [7, 71, 98]), is directly linked to movement, which can be captured by the embedded accelerometer. This could explain the relatively large proportion of participants who realized that these two pieces of information (i.e., age and sexual activity) could be inferred with high precision.

However, for religion, participants might have followed the reasoning that "there is no sensor for religion" and that there is no physiological difference between two individuals with different religions. Yet, what the participants failed to realize is that physiological data (e.g., movement) contains behavioral information (e.g., wake-up time), which is affected by personal aspects such as religion. Previous studies demonstrated that a person's religion could be inferred with a reasonable accuracy from the electric consumption profile of their household, which reveals their activity: for instance, Muslims would wake up earlier for breakfast during Ramadan [59, 99, 104].

Our participants showed little to no concern with regard to age and gender being inferred. However, for all other types of information we presented, the participants showed varying degrees of concern. The participants' general lack of concern about age and gender being inferred accurately is in line with findings in a previous study where participants reported being comfortable sharing these types of information [34]. However, the participants' lack of concern with regard to religion and sexual orientation was surprising. This can be explained by two factors. Firstly, the country in which the study took place has a low crime rate and few violations against sexual and religious minorities. Consequently, the negative repercussions of such information being disclosed could be limited. Secondly, the participants did not believe that these two types of sensitive information (i.e., religion and sexual orientation) can be inferred from fitness tracker data. The participants underestimate the potential for discrimination based on the types of sensitive information we presented them with [24].

Our participants' lack of understanding of potential threats implies that there is a need for privacy education. Privacy education could be given inside of the companion app, such as having simple and clear descriptions in the privacy settings that explain what sort of privacy risks a person would be exposed to if a given feature were to be enabled [4]. Beyond this, including privacy education in school and university curricula could be another way to inform people of privacy issues beyond only fitness trackers. Furthermore, the participants' underlying assumption that they are currently not at risk, does not mean that in the future the social or political climate will not change to where they would be at risk. Therefore, it is important to provide a perspective that the situation will not always remain the same.

5.3 Mental Models and Implications — RQ3

Our findings revealed that only one-fifth of the participants had the *correct* mental model of how the fitness tracker ecosystem functions. These participants had the essential understanding, hence they might be more knowledgeable about the privacy consequences of their device use. However, the vast majority of the participants had either *incorrect* or *incomplete* mental models. We found that half of our participants had *incorrect* mental models. This finding confirms related work about how fitness-tracker users lack awareness [4, 6, 63, 102, 109]. However, our paper sheds light on users' technical misunderstandings and how some of these misunderstandings can imply potential privacy misconceptions and dangerous behavior. For instance, most of the participants with the *incorrect* mental models erroneously thought that their fitness tracker can communicate directly and

bilaterally with Fitbit's servers, without requiring any connected device. Such beliefs have potential risks, as these participants could underestimate the privacy and security risks associated with their connected devices: for example, users could use their smartphone to provide access to malicious third-party apps without considering the associated risks. This finding might explain why more than half of the interview participants mentioned Fitbit's servers as the most vulnerable element in the fitness-tracker ecosystem, neglecting the potential risks associated with their connected devices.[26]

Considering the *incomplete* mental models, most of these participants had misunderstandings about the information flow between their trackers and connected devices (e.g., trackers can receive processed fitness data). This could be explained by earlier findings [91] that most of the users cannot distinguish the differences between raw and processed data. It is noteworthy to mention that we did not find any potential privacy-threatening scenarios associated with the *incomplete* mental models.

On a different note, our interview participants recognized different elements as vulnerable points in the fitness-tracker ecosystem. Most of these participants mentioned the fitness tracker company servers because they think the servers are not secure enough or simply because the users do not trust the company, and/or they think the companies might provide their fitness data to third-party organizations (e.g., advertisement agencies, insurance companies, intelligence agencies) for monetary benefits. This result contradicts with some recent findings [6, 109] that users trust the fitness tracker companies.[27] The participants also mentioned that different connection protocols (e.g., Bluetooth) are vulnerable and they can be penetrated by attackers. This conception is supported by earlier literature [18] that shows that Bluetooth traffic of the fitness trackers can be used to infer the users' activity levels thus to identify them. Our participants also mentioned that their smartphones could be hacked by attackers. However, the participants never mentioned themselves (i.e., *users*) as responsible parties, in the sense that they might take wrong privacy decisions. Indeed, users' voluntary behaviors [6, 102], such as sharing fitness data in social network platforms or granting access to other fitness applications, are important risk factors. Our participants also never mentioned anything about how they would manage their previously provided access (e.g., revoking access after using a third-party application). Only one-tenth of the participants used visual elements to illustrate any third-party organizations in the fitness-tracker ecosystem, thus showing that they have a limited understanding of the existing threats in the fitness-tracker ecosystem [4, 6, 109].

We believe that better media coverage, such as more tech news and educational video tutorials, could be helpful to enhance fitness-tracker users' mental models. However, we also suggest redesigning the existing interfaces (e.g., mobile apps) so that they inform the users with incorrect mental models about the potential privacy and security risks. One example could be redesigning fitness apps to visualize how fitness information flows across different devices and that the potential privacy risks are associated with any user action. Such a design could empower users with incorrect mental models to make informed privacy decisions [103].

5.4 Removing the Tracker or Disabling a Sensor for Privacy Protection — RQ4

Our findings showed that, surprisingly, the majority of our participants did not view the removal of their trackers as being a privacy-preserving action. The reasons for removing the tracker during the *day* were rarely privacy-related. However, a few participants did attempt to remove their trackers specifically to protect their privacy. This is indicative of the privacy concerns being sufficiently high that the participants were willing to forgo any utility gained from using the fitness tracker. Based on the *privacy calculus* theory, the perceived privacy loss can greatly outweigh the perceived utility gain of using the fitness tracker [35]. Our findings also showed that, in general, the participants did not seem to remove their trackers at *night* for privacy reasons. Instead, we observed

[26]Earlier studies assessed the security vulnerabilities in the fitness-tracker ecosystem [16, 25, 72]. As a result, we could conclude that our participants mistakenly thought that their smartphone is more secure than the fitness-tracker company servers and that their vulnerability assessment is not realistic.

[27]Users might trust the companies' honesty, but not their ability to protect the servers.

that the participants have a clear preference for recharging their trackers at night when they sleep. In conclusion, we speculate that, for several reasons, most our participants did not consider removing their fitness trackers for privacy protection: (i) they were not sufficiently concerned with their privacy, (ii) they might be overly confident in their understanding of the privacy risks associated with wearing their tracker all the time, or (iii) they might not realize the benefits that such actions can have on their privacy.

With regard to disabling sensors in the Fitbit Inspire HR for privacy protection, many participants mentioned that they would disable the GPS sensor. This implies that most of the participants have concerns about their location being tracked, nevertheless, they have limited understanding about the embedded sensors in their trackers.[28] This is in line with earlier studies showing that fitness-tracker users usually consider their location data to be sensitive [53, 74] and that they could perform a privacy-preserving action to hide their location. Although most of the participants would use the option of disabling the GPS, a minority of participants would use such an option for other sensors (e.g., to disable the accelerometer to hide the step count). We should also note that our participants' lack of ability to identify some sensors in the tracker could be related to the use of technical language. For instance, 'accelerometer' is not a commonly used word in the daily language.

In conclusion, the participants showed a desire to disable (certain) sensors in their trackers, yet most of them were not interested in removing the entire tracker for privacy protection. Perhaps our participants thought that the privacy-utility trade-off would be more reasonable when disabling some sensors, compared with removing the tracker. In particular, as the participants were mainly concerned about their location being tracked, they were interested in disabling the GPS sensor in their tracker to protect their privacy. For trackers that would contain a GPS sensor, having the option to disable it would be useful in order to enable users to be able to use the device as they choose.

5.5 Limitations and Future Work

Our study has some limitations. First, given that we used our university's participant pool, we recruited only young participants. Fitness-tracker users from other age groups might have different requirements and perceptions. For example, older adults have different attitudes toward adopting the fitness trackers [51], and they might also have different privacy attitudes [50]. The over-representation of young people in our sample could limit the external validity of the study. Thus, our findings must be interpreted with caution and should not be generalized to other age groups. Future studies can include a broader age range. For example, it could be interesting to study the mental models of older users of fitness trackers to better understand the similarities and differences between older and younger users.

Some of our participants mentioned during the interviews that they had their own fitness tracker before the study, and they stopped using it to participate in our study. Whereas, others mentioned they had never used a fitness tracker before the study. Unfortunately, we did not collect participants' fitness-tracker experiences before the study, so we are not able to observe a relationship between their previous fitness tracker usage and its perceived utility, and their privacy attitudes and mental models. However, we believe that the four-month period is a relatively fair amount of time for the novice participants to adopt the trackers and reflect on their daily experiences (e.g., an earlier study [84] showed that after one month of using fitness trackers, users master their devices and begin perceiving benefits from them). In the future, it would be interesting to study how the experiences of participants with fitness trackers and their technical background would lead to different types of mental models. Although such research has been done in other domains (e.g., the comparison between the mental models of Internet administrators and end-users [57]), it has yet to be studied in the context of fitness tracking.

[28] Fitbit Inspire HR does not include a GPS sensor, and it uses the connected GPS feature, in which it utilizes from the GPS sensor of a connected device.

Our participants were given the tracker devices to participate in a data-collection study. This deliberate participation in the study might have slightly influenced their fitness-tracking practices and utility/privacy perceptions. However, we think such an effect is negligible, as the length of the study was sufficiently long that the participants were able to become accustomed to the conditions of the study. An alternative approach to minimizing such effects would be to conduct a cross-sectional study by observing a population that already uses their 'personal' fitness trackers. However, such a data collection method has ethical issues and privacy implications for the study participants.

6 CONCLUSION

In this paper, we have presented a study wherein we distributed fitness trackers to more than two hundred participants and recorded their fitness data over a period of four months. At the end of the four-month period, we performed an exit survey with 227 participants; we asked questions related to users' perceptions of privacy, utility, and fitness-tracker functioning. To better contextualize and understand the reasoning behind the answers to the exit survey, we interviewed 19 survey respondents. During the interviews, we asked questions to explore the participants' privacy concerns, the perceived utility of fitness trackers, and their mental models of the fitness-tracker ecosystem. Our work provides an empirical contribution about how fitness-tracker users perceive the utility of their device. Our findings show a high potential for implementing data minimization that would enable certain privacy risks related to fitness trackers to be avoided. Nonetheless, this would be subject to fitness-tracker companies willingness to implement such changes and to accept the reduced data-flow by removing features such as synchronization with company servers. We contribute to furthering the comprehension of how users understand the privacy risks of fitness trackers and their functioning. We have shown that, overall, fitness-tracker users think that sensitive information cannot be inferred from their fitness tracker data. In particular, the participants thought that only information that is directly linked with the sensors that they believe to be present in their tracker (i.e., information related to physiological data) could be inferred. Our mental-model analysis shows that most of the participants have an incomplete or incorrect understanding of how the fitness-tracker ecosystem functions, and some of their misconceptions could have further privacy implications.

ACKNOWLEDGMENTS

This work was partially funded by the Swiss National Science Foundation with Grant #200021_178978 (PrivateLife) and by armasuisse S+T with Grant #CYD-C-2020007. We sincerely thank Laura Mauzurik for her help in conducting the interviews. We thank Rita Abi Akl for her help in designing the first draft of the survey. We also thank Holly Cogliati for proofreading this article. Last but not least, we thank Lyubov Velykoivanenko and Oleksandr Velykoivanenko for participating in the cognitive pre-tests for the survey and interviews.

REFERENCES

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Symp. on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 137–153. https://doi.org/10.1109/SP.2017.65

[2] A. Acquisti and R. Gross. 2009. Predicting Social Security Numbers from Public Data. *Proc. of the National Academy of Sciences* 106, 27 (July 2009), 10975–10980. https://doi.org/10.1073/pnas.0904891106

[3] Adam Satariano. 2014. Wear This Device So the Boss Knows You're Losing Weight. http://www.bloomberg.com/news/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.html

[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 Conf. on Multimedia Privacy and Security (MPS)*. ACM, Dallas, Texas, USA, 1–11. https://doi.org/10.1145/3137616.3137617

[5] Muaddi Alharbi, Adrian Bauman, Lis Neubeck, and Robyn Gallagher. 2016. Validation of Fitbit-Flex as a Measure of Free-Living Physical Activity in a Community-Based Phase III Cardiac Rehabilitation Population. *European Journal of Preventive Cardiology* 23, 14

(Sept. 2016), 1476–1485. https://doi.org/10.1177/2047487316634883
[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 Conf. on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, USA, 421–434. https://dl.acm.org/doi/abs/10.5555/3361476.3361508
[7] Z. Arnold, D. Larose, and E. Agu. 2015. Smartphone Inference of Alcohol Consumption Levels from Gait. In *Int. Conf. on Healthcare Informatics (ICHI)*. IEEE, Dallas, TX, USA, 417–426. https://doi.org/10.1109/ICHI.2015.59
[8] Kim Bartel Sheehan. 1999. An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors. *Journal of Interactive Marketing* 13, 4 (Jan. 1999), 24–38. https://doi.org/10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O
[9] Krutheeka Baskaran and Saji K. Mathew. 2020. Danger vs Fear: An Empirical Study on Wearable Users' Privacy Coping. In *Proc. of the Conf. on Computers and People Research (SIGMIS-CPR)*. ACM, Nuremberg, Germany, 123–132. https://doi.org/10.1145/3378539.3393856
[10] Tony Beltramelli and Sebastian Risi. 2015. Deep-Spying: Spying Using Smartwatch and Deep Learning. *arXiv:1512.05616 [cs]* (Dec. 2015). arXiv:1512.05616 [cs] http://arxiv.org/abs/1512.05616
[11] Igor Bilogrevic, Kévin Huguenin, Stefan Mihaila, Reza Shokri, and Jean-Pierre Hubaux. 2015. Predicting Users' Motivations behind Location Check-Ins and Utility Implications of Privacy Protection Mechanisms. In *Symp. of the Network and Distributed System Security (NDSS)*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2015.23032
[12] Laura Burbach, Chantal Lidynia, Philipp Brauner, and Martina Ziefle. 2019. Data Protectors, Benefit Maximizers, or Facts Enthusiasts: Identifying User Profiles for Life-Logging Technologies. *Computers in Human Behavior* 99 (Oct. 2019), 9–21. https://doi.org/10.1016/j.chb.2019.05.004
[13] Kelly Caine and Rima Hanania. 2013. Patients Want Granular Privacy Control over Health Information in Electronic Medical Records. *Journal of the American Medical Informatics Association* 20, 1 (Jan. 2013), 7–15. https://doi.org/10.1136/amiajnl-2012-001023
[14] Ann Cavoukian, Scott Taylor, and Martin E. Abrams. 2010. Privacy by Design: Essential for Organizational Accountability and Strong Business Practices. *Identity in the Information Society* 3, 2 (Aug. 2010), 405–413. https://doi.org/10.1007/s12394-010-0053-z
[15] Eun Kyoung Choe, Nicole B Lee, Bongshin Lee, Wanda Pratt, and Julie A Kientz. 2014. Understanding Quantified-Selfers' Practices in Collecting and Exploring Personal Data. In *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*. ACM, Toronto Ontario Canada, 1143–1152. https://doi.org/10.1145/2556288.2557372
[16] Jiska Classen, Daniel Wegemer, Paul Patras, Tom Spink, and Matthias Hollick. 2018. Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 1 (March 2018), 5:1–5:24. https://doi.org/10.1145/3191737
[17] Bogdan Copos, Karl Levitt, Matt Bishop, and Jeff Rowe. 2016. Is Anybody Home? Inferring Activity From Smart Home Network Traffic. In *IEEE Security and Privacy Workshops (SPW)*. IEEE, San Jose, CA, 245–251. https://doi.org/10.1109/SPW.2016.48
[18] Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah, and Prasant Mohapatra. 2016. Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers. In *Proc. of the ACM Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM, New York, NY, USA, 99–104. https://doi.org/10.1145/2873587.2873594
[19] Prerit Datta, Akbar Siami Namin, and Moitrayee Chatterjee. 2018. A Survey of Privacy Concerns in Wearable Devices. In *IEEE Int. Conf. on Big Data (Big Data)*. IEEE, Seattle, WA, USA, 4549–4553. https://doi.org/10.1109/BigData.2018.8622110
[20] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2015. Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics. In *Network and Distributed System Security Symp. (NDSS)*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2015.23203
[21] Kelly R. Evenson, Michelle M. Goto, and Robert D. Furberg. 2015. Systematic Review of the Validity and Reliability of Consumer-Wearable Activity Trackers. *International Journal of Behavioral Nutrition and Physical Activity* 12, 1 (Dec. 2015), 159. https://doi.org/10.1186/s12966-015-0314-1
[22] Christina Farr. 2015. Weighing Privacy Vs. Rewards Of Letting Insurers Track Your Fitness. https://www.npr.org/sections/alltechconsidered/2015/04/09/398416513/weighing-privacy-vs-rewards-of-letting-insurers-track-your-fitness
[23] Alireza Farrokhi, Reza Farahbakhsh, Javad Rezazadeh, and Roberto Minerva. 2021. Application of Internet of Things and Artificial Intelligence for Smart Fitness: A Survey. *Computer Networks* 189 (April 2021), 107859. https://doi.org/10.1016/j.comnet.2021.107859
[24] Federal Statistical Office. 2021. Experience of Discrimination. https://www.bfs.admin.ch/bfs/en/home/statistiken/bevoelkerung/migration-integration/zusammenleben-schweiz/diskriminierung.html
[25] Hossein Fereidooni, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, and Mauro Conti. 2017. Fitness Trackers: Fit for Health but Unfit for Security and Privacy. In *IEEE/ACM Int. Conf. on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. IEEE, Philadelphia, PA, USA, 19–24. https://doi.org/10.1109/CHASE.2017.54
[26] Fitbit. 2019. Fitbit Inspire HR User Manual. https://staticcs.fitbit.com/content/assets/help/manuals/manual_inspire_hr_en_US.pdf
[27] Fitbit. 2020. Fitbit SDK. https://dev.fitbit.com/
[28] Fitbit. 2020. Web API Reference. https://dev.fitbit.com/build/reference/web-api/
[29] Fitbit. 2021. Employers. https://healthsolutions.fitbit.com/employers/
[30] Fitbit. 2021. How Do Fitbit Devices Sync Their Data? https://help.fitbit.com/articles/en_US/Help_article/1877.htm

[31] Fitbit. 2021. Why Fitbit? http://healthsolutions.fitbit.com/whyfitbit/
[32] Fitbit. 2021. Why Is the Fitbit App Prompting Me to Turn on Location Services? https://help.fitbit.com/articles/en_US/Help_article/2134.htm?Highlight=syncing
[33] Fitbit. 2021. Why Won't My Fitbit Device Sync? https://help.fitbit.com/articles/en_US/Help_article/1866.htm
[34] 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, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376651
[35] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security* 77 (Aug. 2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002
[36] Nanna Gorm and Irina Shklovski. 2016. Sharing Steps in the Workplace: Changing Privacy Concerns Over Time. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, San Jose, California, USA, 4315–4319. https://doi.org/10.1145/2858036.2858352
[37] 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)*. Association for Computing Machinery, Denver, Colorado, USA, 1647–1659. https://doi.org/10.1145/3025453.3025654
[38] Cory Hallam and Gianluca Zanella. 2016. Wearable Device Data and Privacy: A Study of Perception and Behavior. *World Journal of Management* 7, 1 (March 2016), 82–91. https://doi.org/10.21102/wjm.2016.03.71.06
[39] André Henriksen, Martin Haugen Mikalsen, Ashenafi Zebene Woldaregay, Miroslav Muzny, Gunnar Hartvigsen, Laila Arnesdatter Hopstock, and Sameline Grimsgaard. 2018. Using Fitness Trackers and Smartwatches to Measure Physical Activity in Research: Analysis of Consumer Wrist-Worn Wearables. *Journal of Medical Internet Research* 20, 3 (March 2018), e110. https://doi.org/10.2196/jmir.9157
[40] 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
[41] Robert P Hirten, Matteo Danieletto, Lewis Tomalin, Katie Hyewon Choi, Micol Zweig, Eddye Golden, Sparshdeep Kaur, Drew Helmus, Anthony Biello, Renata Pyzik, Alexander Charney, Riccardo Miotto, Benjamin S Glicksberg, Matthew Levin, Ismail Nabeel, Judith Aberg, David Reich, Dennis Charney, Erwin P Bottinger, Laurie Keefer, Mayte Suarez-Farinas, Girish N Nadkarni, and Zahi A Fayad. 2021. Use of Physiological Data From a Wearable Device to Identify SARS-CoV-2 Infection and Symptoms and Predict COVID-19 Diagnosis: Observational Study. *Journal of Medical Internet Research* 23, 2 (Feb. 2021), e26107. https://doi.org/10.2196/26107
[42] Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti. 2013. Addressing the Concerns of the Lacks Family: Quantification of Kin Genomic Privacy. In *Proc. of the ACM SIGSAC Conf. on Computer & Communications Security (CCS)*. ACM Press, Berlin, Germany, 1141–1152. https://doi.org/10.1145/2508859.2516707
[43] 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
[44] Fortune Business Insights. 2021. Fitness Tracker Market Size, Share, Growth & Analysis. https://www.fortunebusinessinsights.com/fitness-tracker-market-103358
[45] Yoonhyuk Jung, Seongcheol Kim, and Boreum Choi. 2016. Consumer Valuation of the Wearables: The Case of Smartwatches. *Computers in Human Behavior* 63 (Oct. 2016), 899–905. https://doi.org/10.1016/j.chb.2016.06.040
[46] Daniel Kahneman, Jack L Knetsch, and Richard H Thaler. 1991. Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives* 5, 1 (Feb. 1991), 193–206. https://doi.org/10.1257/jep.5.1.193
[47] Daniel Kahneman and Amos Tversky. 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica* 47, 2 (March 1979), 263. https://doi.org/10.2307/1914185
[48] Mahdokht Kalantari. 2017. Consumers' Adoption of Wearable Technologies: Literature Review, Synthesis, and Future Research Agenda. *Internatinoal Journal of Technology Marketing* 12, 3 (Jan. 2017), 274–307. https://doi.org/10.1504/IJTMKT.2017.089665
[49] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proc. of the USENIX Conf. on Usable Privacy and Security (SOUPS)*. USENIX Association, Ottawa, Canada, 39–52. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang
[50] Murat Kezer, Barış Sevi, Zeynep Cemalcilar, and Lemi Baruh. 2016. Age Differences in Privacy Attitudes, Literacy and Privacy Management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1 (May 2016), 52–71. https://doi.org/10.5817/CP2016-1-2
[51] Sunyoung Kim and Abhishek Choudhury. 2020. Comparison of Older and Younger Adults' Attitudes Toward the Adoption and Use of Activity Trackers. *JMIR mHealth and uHealth* 8, 10 (Oct. 2020), e18312. https://doi.org/10.2196/18312
[52] Seoyoung Kim, Arti Thakur, and Juho Kim. 2020. Understanding Users' Perception Towards Automated Personality Detection with Group-Specific Behavioral Data. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. ACM, Honolulu, HI, USA, 1–12. https://doi.org/10.1145/3313831.3376250
[53] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring Privacy Concerns about Personal Sensing. In *Pervasive Computing*, Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito

Tobe (Eds.). Springer, Berlin, Heidelberg, 176–183. https://doi.org/10.1007/978-3-642-01516-8_13

[54] Rafal Kocielnik, Lillian Xiao, Daniel Avrahami, and Gary Hsieh. 2018. Reflection Companion: A Conversational System for Engaging Users in Reflection on Physical Activity. *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2, 2 (July 2018), 70:1–70:26. https://doi.org/10.1145/3214273

[55] Danielle Kosecki. 2017. Sláinte! Ireland Named Fitbit's Fittest Country. https://blog.fitbit.com/fittest-countries/

[56] Philip Kotler, Waldemar Pfoertsch, and Ines Michi. 2006. *B2B Brand Management.* Springer, Berlin ; New York.

[57] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *Proc. of the IEEE Symp. on Security and Privacy (S&P)*. IEEE, San Francisco, CA, USA, 1138–1155. https://doi.org/10.1109/SP.2019.00060

[58] Marc Langheinrich. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *UbiComp*, Gregory D. Abowd, Barry Brumitt, and Steven Shafer (Eds.), Vol. 2201. Springer Berlin Heidelberg, Berlin, Heidelberg, 273–291. https://doi.org/10.1007/3-540-45427-6_23

[59] Nader Lessan and Tomader Ali. 2019. Energy Metabolism and Intermittent Fasting: The Ramadan Perspective. *Nutrients* 11, 5 (May 2019), 1192. https://doi.org/10.3390/nu11051192

[60] He Li, Jing Wu, Yiwen Gao, and Yao Shi. 2016. Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective. *International Journal of Medical Informatics* 88 (April 2016), 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

[61] 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 (AHFE)*, Tareq Ahram and Christianne Falcão (Eds.), Vol. 608. Springer International Publishing, The Westin Bonaventure Hotel, Los Angeles, California, USA, 42–53. https://doi.org/10.1007/978-3-319-60639-2_5

[62] Ramon Llamas, Jitesh Ubrani, and Michael Shirer. 2017. Xiaomi and Apple Tie for the Top Position as the Wearables Market Swells 17.9% During the First Quarter, According to IDC. https://www.businesswire.com/news/home/20170605005391/en/Xiaomi-and-Apple-Tie-for-the-Top-Position-as-the-Wearables-Market-Swells-17.9-During-the-First-Quarter-According-to-IDC

[63] Byron Lowens, Vivian Genaro Motti, and Kelly Caine. 2017. Wearable Privacy: Skeletons in The Data Closet. In *IEEE Int. Conf. on Healthcare Informatics (ICHI)*. IEEE, Park City, UT, USA, 295–304. https://doi.org/10.1109/ICHI.2017.29

[64] Deborah Lupton. 2014. Self-Tracking Cultures: Towards a Sociology of Personal Informatics. In *Proc. of the Australian Computer-Human Interaction Conf. on Designing Futures: The Future of Design (OzCHI)*. Association for Computing Machinery, Sydney, New South Wales, Australia, 77–86. https://doi.org/10.1145/2686612.2686623

[65] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Proc. of the Sixteenth USENIX Conf. on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 341–358. https://www.usenix.org/conference/soups2020/presentation/mai

[66] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. 2016. Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms. In *Proc. of the ACM on Asia Conf. on Computer and Communications Security (ASIA CCS)*. ACM, Xi'an, China, 795–806. https://doi.org/10.1145/2897845.2897905

[67] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. 2015. (Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks Using Smartwatches. In *Proc. of the ACM Int. Symp. on Wearable Computers (ISWC)*. ACM, Osaka, Japan, 27–30. https://doi.org/10.1145/2802083.2808397

[68] Anindya Maiti, Murtuza Jadliwala, J. He, and I. Bilogrevic. 2018. Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Transactions on Mobile Computing* 17, 9 (Sept. 2018), 2180–2194. https://doi.org/10.1109/TMC.2018.2794984

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

[70] K. I. Manktelow and Man Cheung Chung (Eds.). 2004. *Psychology of Reasoning: Theoretical and Historical Perspectives* (first ed.). Psychology Press, Hove ; New York. https://www.taylorfrancis.com/books/9780203506936

[71] Maria De Marsico and Alessio Mecca. 2019. A Survey on Gait Recognition via Wearable Sensors. *Comput. Surveys* 52, 4 (Aug. 2019), 1–39. https://doi.org/10.1145/3340293

[72] Florina Mendoza, Lucía Alonso, Andrés López, and Daniel and Patricia Arias Cabarcos. 2018. Assessment of Fitness Tracker Security: A Case of Study. *Proceedings* 2, 19 (Oct. 2018), 1235. https://doi.org/10.3390/proceedings2191235

[73] Javan Mnjama, Greg Foster, and Barry Irwin. 2017. A Privacy and Security Threat Assessment Framework for Consumer Health Wearables. In *2017 Information Security for South Africa (ISSA)*. IEEE, Johannesburg, 66–73. https://doi.org/10.1109/ISSA.2017.8251776

[74] Vivian Genaro Motti and Kelly Caine. 2015. Users' Privacy Concerns About Wearables. In *Financial Cryptography and Data Security (FC)*, Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). Springer, San Juan, Puerto Rico, 231–244. https://doi.org/10.1007/978-3-662-48051-9_17

[75] S. A. Munson and S. Consolvo. 2012. Exploring Goal-Setting, Rewards, Self-Monitoring, and Sharing to Motivate Physical Activity. In *Int. Conf. on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*. IEEE, San Diego, United States, 25–32. https:

//doi.org/10.4108/icst.pervasivehealth.2012.248691

[76] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proc. of the Symp. on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, USA, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[77] Mark W. Newman, Debra Lauterbach, Sean A. Munson, Paul Resnick, and Margaret E. Morris. 2011. It's Not That i Don't Have Problems, i'm Just Not Putting Them on Facebook: Challenges and Opportunities in Using Online Social Networks for Health. In *Proc. of the ACM Conf. on Computer Supported Cooperative Work (CSCW)*. Association for Computing Machinery, Hangzhou, China, 341–350. https://doi.org/10.1145/1958824.1958876

[78] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *HeinOnline* 79 (2004), 119.

[79] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proc. on Privacy Enhancing Technologies (PoPETs)* 2018, 4 (Oct. 2018), 5–32. https://doi.org/10.1515/popets-2018-0029

[80] Greig Paul and James Irvine. 2014. Privacy Implications of Wearable Health Devices. In *Proc. of the Int. Conf. on Security of Information and Networks (SIN)*. ACM, Glasgow, Scotland, UK, 117–121. https://doi.org/10.1145/2659651.2659683

[81] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. 2012. Understanding Sharing Preferences and Behavior for MHealth Devices. In *Proc. of the ACM Workshop on Privacy in the Electronic Society (WPES)*. ACM, Raleigh, North Carolina, USA, 117–128. https://doi.org/10.1145/2381966.2381983

[82] Giorgio Quer, Jennifer M. Radin, Matteo Gadaleta, Katie Baca-Motes, Lauren Ariniello, Edward Ramos, Vik Kheterpal, Eric J. Topol, and Steven R. Steinhubl. 2021. Wearable Sensor Data and Self-Reported Symptoms for COVID-19 Detection. *Nature Medicine* 27, 1 (Jan. 2021), 73–77. https://doi.org/10.1038/s41591-020-1123-x

[83] Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. 2011. Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, Vancouver, BC, Canada, 11–20. https://doi.org/10.1145/1978942.1978945

[84] Mirana Randriambelonoro, Yu Chen, and Pearl Pu. 2017. Can Fitness Trackers Help Diabetic and Obese Users Make and Sustain Lifestyle Changes? *Computer* 50, 3 (March 2017), 20–29. https://doi.org/10.1109/MC.2017.92

[85] Rocket Fuel. 2014. *'Quantified Self' Digital Tools: A CPG Marketing Opportunity*. Technical Report. Rocket Fuel. http://rocketfuel.com/blog/quantified-self

[86] Mark Rowan and Josh Dehlinger. 2014. Observed Gender Differences in Privacy Concerns and Behaviors of Mobile Device End Users. *Procedia Computer Science* 37 (Jan. 2014), 340–347. https://doi.org/10.1016/j.procs.2014.08.050

[87] Christopher Rowl, closeChristopher Rowl, Business reporter focused on the health-care economy's effects on patient health, costs, and privacyEmailEmailBioBioFollowFollow. 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

[88] Michael A Rupp, Jessica R Michaelis, Daniel S McConnell, and Janan A Smither. 2018. The Role of Individual Differences on Perceptions of Wearable Fitness Device Trust, Usability, and Motivational Impact. *Applied ergonomics* 70 (2018), 77–87.

[89] Pablo Saa, Oswaldo Moscoso-Zea, and Sergio Lujan-Mora. 2018. Wearable Technology, Privacy Issues. In *Proc. of the Int. Conf. on Information Technology & Systems (ICITS)*, Álvaro Rocha and Teresa Guarda (Eds.), Vol. 721. Springer, Cham, Universidad Estatal Península de Santa Elena, Libertad City, Ecuador, 518–527. https://doi.org/10.1007/978-3-319-73450-7_49

[90] Johnny Saldana. 2021. *The Coding Manual for Qualitative Researchers* (4th ed ed.). SAGE Publishing, Thousand Oaks, California.

[91] 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)*. ACM, Glasgow, Scotland Uk, 1–6. https://doi.org/10.1145/3290605.3300753

[92] Grace Shin, Mohammad Hossein Jarrahi, Yu Fei, Amir Karami, Nicci Gafinowitz, Ahjung Byun, and Xiaopeng Lu. 2019. Wearable Activity Trackers, Accuracy, Adoption, Acceptance and Health Impact: A Systematic Literature Review. *Journal of Biomedical Informatics* 93 (May 2019), 103153. https://doi.org/10.1016/j.jbi.2019.103153

[93] Muhammad Shoaib, Ozlem Durmaz Incel, Hans Scholten, and Paul Havinga. 2018. SmokeSense: Online Activity Recognition Framework on Smartwatches. In *Mobile Computing, Applications, and Services*, Kazuya Murao, Ren Ohmura, Sozo Inoue, and Yusuke Gotoh (Eds.). Vol. 240. Springer International Publishing, Cham, 106–124. https://doi.org/10.1007/978-3-319-90740-6_7

[94] Prakash Shrestha and Nitesh Saxena. 2017. An Offensive and Defensive Exposition of Wearable Computing. *Comput. Surveys* 50, 6 (Nov. 2017), 92:1–92:39. https://doi.org/10.1145/3133837

[95] Ton Spil, Ali Sunyaev, Scott Thiebes, and Rolf van Baalen. 2017. The Adoption of Wearables for a Healthy Lifestyle: Can Gamification Help?. In *Proc. of the Hawaii Int. Conf. on System Sciences (HICSS)*, Vol. 2017. Hilton Waikoloa Village, Hawaii, 3617–3626. https://doi.org/10.24251/HICSS.2017.437

[96] Tailor Stanton. 2019. Earnings aside, over 60 Percent of Fitness Trackers Purchased Online Q1 Were Fitbits. https://www.rakutenintelligence.com/blog/2016/earnings-aside-over-60-percent-of-fitness-trackers-purchased-during-q1-were-fitbits

[97] Etye Steinberg. 2021. Run for Your Life: The Ethics of Behavioral Tracking in Insurance. *Journal of Business Ethics* (June 2021). https://doi.org/10.1007/s10551-021-04863-8

[98] Brian Suffoletto, Pritika Dasgupta, Ray Uymatiao, James Huber, Kate Flickinger, and Ervin Sejdic. 2020. A Preliminary Study Using Smartphone Accelerometers to Sense Gait Impairments Due to Alcohol Intoxication. *Journal of Studies on Alcohol and Drugs* 81, 4 (July 2020), 505–510. https://doi.org/10.15288/jsad.2020.81.505

[99] Sari Sultan. 2019. Privacy-Preserving Metering in Smart Grid for Billing, Operational Metering, and Incentive-Based Schemes: A Survey. *Computers & Security* 84 (July 2019), 148–165. https://doi.org/10.1016/j.cose.2019.03.014

[100] The European Parliament and the Council of The European Union. 2016. REGULATION (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *Official J. Eur. Union* 59 (April 2016), 1–88. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[101] Walter R. Thompson. November/December 2019. WORLDWIDE SURVEY OF FITNESS TRENDS FOR 2020. *ACSM's Health & Fitness Journal* 23, 6 (November/December 2019), 10–18. https://doi.org/10.1249/FIT.0000000000000526

[102] 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.). Vol. 10766. Springer International Publishing, Cham, 229–239. https://doi.org/10.1007/978-3-319-78105-1_27

[103] Rick Wash and Emilee Rader. 2011. Influencing Mental Models of Security: A Research Agenda. In *Proc. of the Conf. New Security Paradigms Workshop (NSPW)*. Association for Computing Machinery, Marin County, California, USA, 57–66. https://doi.org/10.1145/2073276.2073283

[104] Ellen Webborn and Tadj Oreszczyn. 2019. Champion the Energy Data Revolution. *Nature Energy* 4, 8 (Aug. 2019), 624–626. https://doi.org/10.1038/s41560-019-0432-0

[105] Gary M. Weiss, Jessica L. Timko, Catherine M. Gallagher, Kenichi Yoneda, and Andrew J. Schreiber. 2016. Smartwatch-Based Activity Recognition: A Machine Learning Approach. In *IEEE-EMBS Int. Conf. on Biomedical and Health Informatics (BHI)*. IEEE, Las Vegas, NV, USA, 426–429. https://doi.org/10.1109/BHI.2016.7455925

[106] Heetae Yang, Jieun Yu, Hangjung Zo, and Munkee Choi. 2016. User Acceptance of Wearable Devices: An Extended Perspective of Perceived Value. *Telematics and Informatics* 33, 2 (2016), 256–269.

[107] Jinxue Zhang, Xia Hu, Yanchao Zhang, and Huan Liu. 2016. Your Age Is No Secret: Inferring Microbloggers' Ages via Content and Interaction Analysis. In *Tenth Int. AAAI Conf. on Web and Social Media (ICWSM)*. The AAAI Press, Palo Alto, California, Cologne, Germany, 476–485. https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13076

[108] Paolo Zialcita. 2019. Google Buys Fitbit For $2.1 Billion, Pledges To Protect Health Data. https://www.npr.org/2019/11/01/775419131/google-buys-fitbit-for-2-1-billion-pledges-to-protect-health-data

[109] Michael Zimmer, Priya Kumar, Jessica Vitak, Yuting Liao, and Katie Chamberlain Kritikos. 2020. 'There's Nothing Really They Can Do with This Information': Unpacking How Users Manage Privacy Boundaries for Personal Fitness Information. *Information, Communication & Society* 23, 7 (June 2020), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442

A FITBIT ECOSYSTEM

Figure 13 shows a diagram of the Fitbit tracker functions. The Fitbit Inspire HR contains two sensors, viz., an optical heart rate and a 3-axis accelerometer used for motion pattern tracking [26, p. 42]. To synchronize, an Android phone or tablet, an iPhone or iPad, or a Windows 10 device must be used [30]. From here on 'connected device' will be used to refer to a device that can be used to synchronize. Synchronization can only begin if the user's connected device has an active internet connection [33]. In the case of Android phones, GPS location must also be enabled to synchronize [32]. The Fitbit tracker synchronizes with a user's connected device using Bluetooth [30]. The connected device then sends the data to Fitbit's servers [30]. Only recent data is cached on the connected device, hence, when the user wants to view older data on their connected device, the connected device will download the user's historical data from Fitbit's servers [73]. The same applies when displaying the data on another connected device. The connected device can also send data to the tracker. For example, it can send firmware updates [26, 73], notifications [26, p. 20], alarms [26, p. 23], and so on. If a user has allowed a 3rd party application to access their Fitbit account, then the 3rd party application's server will communicate with Fitbit's server and download the user's data [27, 28]. The user should then be able to view their Fitbit data in the 3rd party application. If a user allowed Fitbit to access their account on a 3rd party application, then Fitbit's server will access the 3rd party application's server and download the user's data from it. Depending on the type of 3rd party application, it could also upload data to a user's Fitbit account.

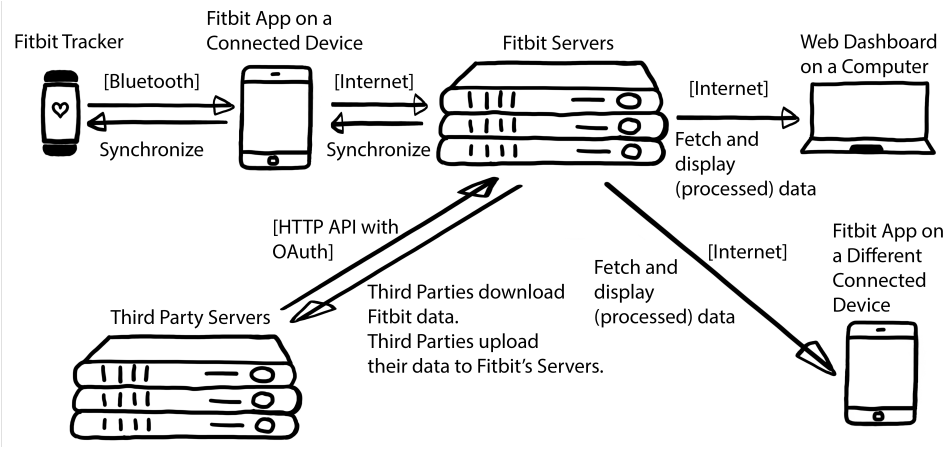


Fig. 13. Fitbit ecosystem functioning diagram.

B SURVEY TRANSCRIPT

Survey sections	Question numbers	Research questions
Sec. 1	Q1, Q2	Demographics
Sec. 2	Q3, Q4	RQ2 & RQ4
Sec. 3	Q5, Q6, Q7, Q8	RQ3 & RQ4
Sec. 4	Q9, Q10	RQ2
Sec. 5	Q11, Q12, Q13	RQ1
Sec. 6	Q14, Q15, Q16	RQ4
Sec. 7	Q17, Q18, Q19	RQ4
Sec. 8	Q20, Q21, Q22	RQ1
Sec. 9	Q23	RQ3
Sec. 10	Q24	RQ2
Sec. 11	Q25	Interview Participation

Table 1. Survey guide.

Note: Coding rules and section labels are colored in gray (they were not visible to respondents).

Sec. 1. Demographics

Q1. With which gender do you identify?
- ◯ Female
- ◯ Male
- ◯ Other [please specify] [ ] (text)
- ◯ Prefer not to answer

Q2. In which faculty/school are you studying?
- ◯ Faculty of Theology and Sciences of Religions (UNIL — FTSR)
- ◯ School of Law (UNIL)
- ◯ School of Criminal Justice (UNIL — ESC)
- ◯ School of Public Administration (UNIL — IDHEAP)
- ◯ Faculty of Arts (UNIL)
- ◯ Faculty of Social and Political Sciences (UNIL — SSP)
- ◯ Faculty of Business and Economics (UNIL — HEC)
- ◯ School of biology (UNIL — FBM)
- ◯ School of medicine (UNIL — FBM)
- ◯ Faculty of Geosciences and Environment (UNIL — GSE)
- ◯ Architecture (EPFL)
- ◯ Environmental Science and Engineering (EPFL)
- ◯ Civil Engineering (EPFL)
- ◯ School of Computer and Communication Sciences (EPFL)
- ◯ Chemistry and Chemical Engineering (EPFL)
- ◯ Mathematics (EPFL)
- ◯ Physics (EPFL)
- ◯ Electrical Engineering (EPFL)
- ◯ Mechanical Engineering (EPFL)
- ◯ Life Science Engineering (EPFL)
- ◯ Microengineering (EPFL)
- ◯ Materials Science and Engineering (EPFL)
- ◯ School of Life Sciences (EPFL)
- ◯ Other

Sec. 2. RQ2

Q3. To what extent do you think you **are aware of the privacy risks** associated with using a **fitness tracker**, such as the Fitbit Inspire HR tracker that you have worn during the study?
- ◯ Extremely unaware
- ◯ Moderately unaware
- ◯ Slightly unaware
- ◯ Neither unaware, nor aware
- ◯ Slightly aware
- ◯ Moderately aware
- ◯ Extremely aware

Q4. Which of the following actions have you carried out **over the course of the previous 4 months**?
(check all the options that apply)
*Without counting the ISPLab application used to collect your data in the context of this study.
- ☐ Read Fitbit's Terms of Service
- ☐ Read Fitbit's Privacy Policy
- ☐ Changed the privacy settings for my Fitbit account (for example, modifying the visibility of my personal data)
- ☐ Changed the security settings of my Fitbit account (for example, changing the password)
- ☐ Gave access to third party application (for example, Amazon Alexa or RunKeeper) to my Fitbit account
- ☐ Gave Fitbit access to one of my social media accounts
- ☐ Removed a friend from my Fitbit friends list
- ☐ Shared one of my badges or achievements through the Fitbit application

Sec. 3. RQ3 & RQ4

Q5. According to you, which **sensors** are present in the Fitbit Inspire HR tracker that you have worn during the study.
(check all the options that apply)
- ☐ GPS
- ☐ Thermometer
- ☐ Accelerometer
- ☐ Camera
- ☐ Microphone
- ☐ Heart rate sensor
- ☐ Blood oxygenation sensor
- ☐ Altimeter
- ☐ Other [please specify] [ ] (text)

Q6. Imagine that you have the possibility to **disable certain sensors** in your Fitbit tracker. Which ones would you disable?
(check all the options that apply)
[Only the items checked in Q5 are shown here.]
- ☐ GPS
- ☐ Thermometer
- ☐ Accelerometer
- ☐ Camera
- ☐ Microphone
- ☐ Heart rate sensor
- ☐ Blood oxygenation sensor
- ☐ Altimeter
- ☐ Other [please specify]

Q7. Could you briefly explain why you would deactivate certain sensors?
[ ] (text)

Q8. If **temporarily disabling certain sensors in your Fitbit tracker was possible**, how **useful** do you think it would be to protect your **privacy**?
- ◯ Extremely useless
- ◯ Moderately useless
- ◯ Slightly useless
- ◯ Neither useless, nor useful

- ◯ Slightly useful
- ◯ Moderately useful
- ◯ Extremely useful

Sec. 4. RQ2

Q9. **Imagine that you have not entered any personal information in your Fitbit profile.**

To what extent (that is, with what precision) can each of the following types of information be **inferred** based on **the data collected from your Fitbit tracker**?

Row options:
- Age
- Gender
- Religion
- Sexual orientation
- Personality traits
- Socioeconomic status (for example, revenue)
- Political views
- Menstrual cycles (for example, date of start, duration, absence, pregnancy)
- Illegal drug consumption (for example, cannabis, cocaine)
- Alcohol and tobacco consumption
- Sexual activity

Column options:
- ◯ Not at all precise
- ◯ Slightly precise
- ◯ Moderately precise
- ◯ Very precise
- ◯ Extremely precise

Q10. To what extent would you be **worried** if the following types of information **could** be **inferred accurately** based on **the data collected by your Fitbit tracker**?

Row options:
- Age
- Gender
- Religion
- Sexual orientation
- Personality traits
- Socioeconomic status (for example, revenue)
- Political views
- Menstrual cycles (for example, date of start, duration, absence, pregnancy)
- Illegal drug consumption (for example, cannabis, cocaine)
- Alcohol and tobacco consumption
- Sexual activity

Column options:
- ◯ Not at all worried
- ◯ Slightly worried
- ◯ Moderately worried
- ◯ Very worried
- ◯ Extremely worried

Sec. 5. RQ1

Q11. For each of the following **types of data**, indicate to what extent you find the data **useful** for your **self-tracking**.

*This data is not collected by the Fitbit Inspire HR tracker.

Row options:
- Number of steps
- Type and duration of exercise/activities (e.g., running, swimming)
- Heart rate

- Quality and duration of sleep
- Weight*
- Number of floors walked*
- Other [please specify] [ ] (text)

Column options:
- ◯ Extremely useless
- ◯ Moderately useless
- ◯ Slightly useless
- ◯ Neither useless, nor useful
- ◯ Slightly useful
- ◯ Moderately useful
- ◯ Extremely useful

Q12. With which **frequency** do you use the following devices/platforms to look at your **step count** and your **heart rate** collected by your Fitbit tracker?

Row options:
- Fitbit application on your smartphone
- Fitbit tracker
- Fitbit website
- Fitbit application on another connected device (e.g., tablet)
- Other [please specify] [ ] (text)

Column options:
- ◯ Never
- ◯ A little
- ◯ Moderately
- ◯ A lot
- ◯ Always

Q13. With which **frequency** do you use the following devices/platforms to look at the **sleep** data collected by your Fitbit tracker?

Row options:
- Fitbit application on your smartphone
- Fitbit website
- Fitbit application on another connected device
- Other [please specify] [ ] (text)

Column options:
- ◯ Never
- ◯ A little
- ◯ Moderately
- ◯ A lot
- ◯ Always

Sec. 6. RQ4

Q14. **Think about a typical day during the study.**

With what frequency have you **taken off** your Fitbit tracker over the course of a typical **day**?
- ◯ Never (I only took it off to charge it)
- ◯ 1–2 times per day
- ◯ 3–4 times per day
- ◯ 5–6 times per day
- ◯ More than 6 times per day

Q15. [Only shown if 'Never (I only took it off to charge it)' was not selected in Q14.]

Normally, for which **reasons** or in which **situations** did you **remove** your Fitbit tracker during the **day**?

(check all the options that apply)

I took it off:
- ☐ To charge it
- ☐ To not dirty it

- ☐ Due to physical comfort (it was bothering me)
- ☐ To avoid electromagnetic radiation (e.g., Bluetooth)
- ☐ For aesthetic reasons
- ☐ Because I was forced to (e.g., airport security, during an exam)
- ☐ For hygiene reasons
- ☐ To take a nap
- ☐ Because I did not see the point in tracking my activity at that point in time
- ☐ Other [please specify] [ ] (text)
- ☐ Due to privacy reasons
- ☐ Someone close to me asked me to (e.g., a friend)

Q16. [Only shown if 'Due to privacy reasons' was selected in Q15]
In the case where you have **removed** your Fitbit tracker during the **day** for **privacy reasons**, please indicate the reasons/situations.
(check all the options that apply)

Because:
- ☐ I was in the bathroom
- ☐ I was engaged in sexual activity
- ☐ I was having a private conversation with someone
- ☐ I was taking a shower
- ☐ I was in a private place
- ☐ I was consuming illegal drugs (for example, cannabis, cocaine)
- ☐ Other [please specify] [ ] (text)
- ☐ I was consuming alcohol or tobacco
- ☐ Someone asked me to

Sec. 7. RQ4

Q17. During the study, with which frequency did you **wear** your Fitbit tracker at **night** (i.e., **when you were sleeping**)?
- ◯ Never
- ◯ Several nights per month
- ◯ Several nights per week
- ◯ Almost every night (I only missed several nights during the study)
- ◯ Every night

Q18. [Only shown if 'Every night' was not selected in Q17]
For which reasons did you **not wear** your Fitbit tracker at **night** (i.e., **while you were sleeping**)?
(check all the options that apply)

I didn't wear it:
- ☐ To charge it
- ☐ Due to physical comfort reasons (it was bothering me)
- ☐ To avoid electromagnetic radiation (e.g., Bluetooth)
- ☐ For aesthetic reasons
- ☐ For hygiene reasons
- ☐ Because I forgot to wear it
- ☐ Other [please specify] [ ] (text)
- ☐ I did not see the point to track my sleep that night
- ☐ Due to privacy reasons
- ☐ Someone close to me asked me to (e.g., a friend)

Q19. [Only shown if 'Due to privacy reasons' was selected in Q18]
In the case where you decided **not to wear** your Fitbit tracker at **night** (i.e., **while you were sleeping**) for which privacy reasons, please indicate these reasons/situations.
(check all the options that apply)

Because:
- ☐ Because I had consumed illegal drugs
- ☐ Other [please specify] [ ] (text)
- ☐ To avoid recording my sleep data

☐ It was bothering my partner

Sec. 8. RQ1

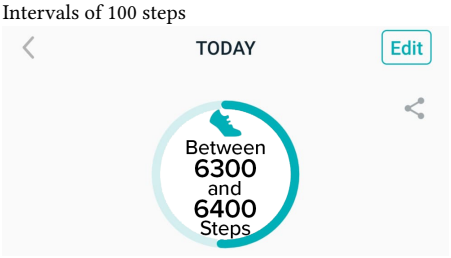
Q20. Imagine that you have walked 6362 steps today!

When using the **website or Fitbit mobile application** to check your step count, to what extent would you find the following displayed **intervals** useful, rather than the precise step count?

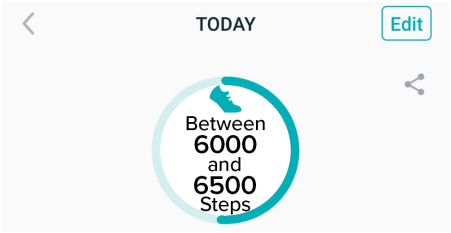
Note: you could still see the precise number on your Fitbit tracker.

Row options:

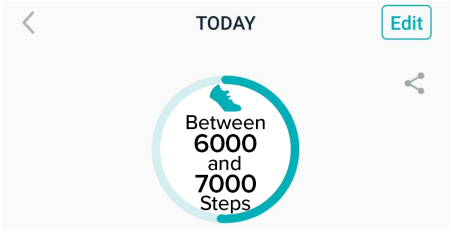
– Intervals of 100 steps



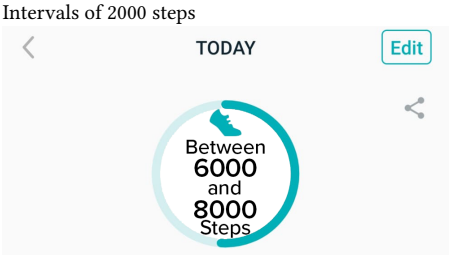
– Intervals of 500 steps



– Intervals of 1000 steps



– Intervals of 2000 steps



Column options:
- ◯ Useless compared to the precise number
- ◯ A lot less useful than seeing the precise number
- ◯ Less useful than seeing the precise number
- ◯ Slightly less useful than seeing the precise number
- ◯ As useful as seeing the precise number

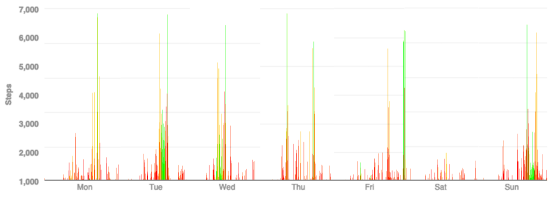
Q21. With which frequency do you look at the following types of data on the **website or Fitbit application**?

Row options:
- The current day (today)
- The current week
- The current month
- The current year
- The entire history

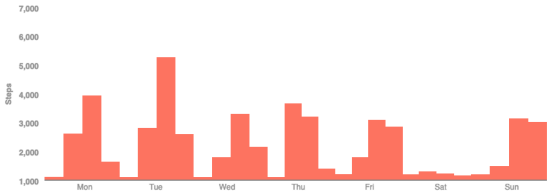
Column options:
- ◯ Never
- ◯ Several times per month
- ◯ Several times per week
- ◯ Almost every day
- ◯ Every day

Q22. Currently (on the website or mobile application), Fitbit supplies your data in intervals of 1min. To what extent would you find the following intervals sufficient for your personal tracking?

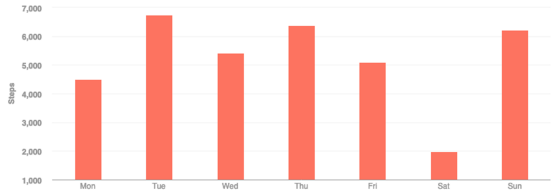
Row options:
- Total for every 15min



- Total for every 6h



– Total per day



Column options:

- ◯ Not at all sufficient
- ◯ Slightly sufficient
- ◯ Moderately sufficient
- ◯ Very sufficient
- ◯ Largely sufficient

Sec. 9. RQ3

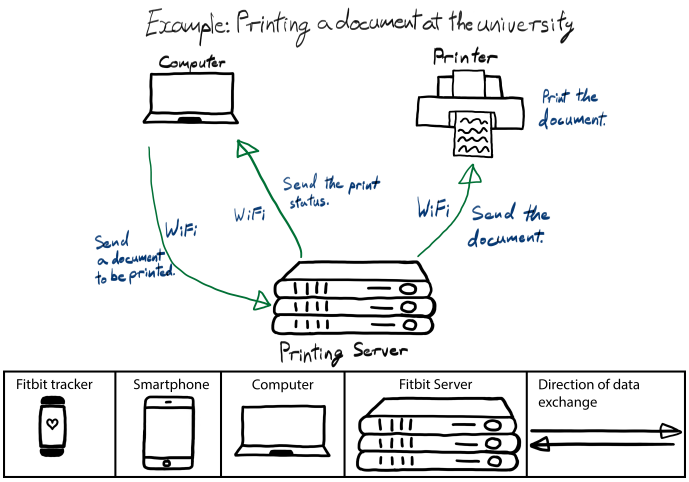
Q23. Please **draw** an image showing how you think your [Randomly assigned based on gender: **step data** or **sleep data**] is processed and transferred over the internet.

Do not forget to **include and label** all the pertinent elements of your drawing, including: the Fitbit tracker, Fitbit's servers, and Fitbit's application on the smartphone.

Instructions:

(a) Look at the following sample drawing.
(b) Please note that the example image is just an example and is not related to Fitbit.
(c) You can find suggested elements below the example.
(d) You do not have to use all the icons. You can also add icons.
(e) Please draw your diagram on a blank A4 sheet of paper.
(f) Take a photo of your drawing.
(g) Send your photo by e-mail to noe.zufferey@unil.ch with the following subject: "(Random Unique User ID)".

Note: We will not judge your drawing abilities, nor your technical understanding.
Do not spend more than 5min on the drawing.
When sending the drawing choose between medium and high quality.



☐ I confirm having drawn and sent the drawing

Sec. 10. RQ2

Q24. Indicate to which extent you agree with the following statements:

Row options:

- All things considered, the Internet would cause serious privacy problems.*
- Compared to others, I am more sensitive about the way online companies handle my personal information.
- To me, it is the most important thing to keep my privacy intact from online companies.
- I believe other people are too much concerned with online privacy issues.*
- Compared with other subjects on my mind, personal privacy is very important.*
- I am concerned about threats to my personal privacy today.

Column options:

◯ Strongly disagree
◯ Disagree
◯ Somewhat disagree
◯ Neither agree nor disagree
◯ Somewhat agree
◯ Agree
◯ Strongly agree

Sec. 11. Interview Participation

Q25. Would you be interested in participating in additional interviews?

If you are chosen, you will have the possibility to decline the invitation. You will be paid 25 CHF per hour.

◯ Yes.
◯ No.
◯ Not sure. I would need additional information.

C PARTICIPANTS STATISTICS

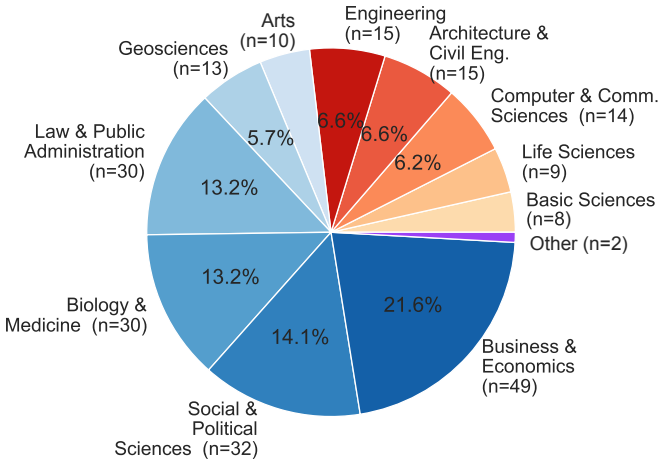


Fig. 14. Participants' field of study. Shades of blue represent participants from UNIL, and shades of red represent participants from EPFL.

Age Range	Female	Male	Other Gender	Total
18–21	90	47	1	138
22–25	42	30	0	72
26–29	7	4	0	11
30–33	4	2	0	6
Total	143	83	1	227

Table 2. Age and gender distribution of survey participant.

Group	Female		Male		Other Gender		Total	
	Potential	Recruited	Potential	Recruited	Potential	Recruited	Potential	Recruited
G1	3	1	1	0	1	0	5	1
G2	3	2	2	1	0	0	5	3
G3	13	6	11	4	0	0	24	10
G4	113	3	64	2	0	0	177	5

Table 3. Distribution of the interviewees per gender and the interview group.