Wearable Activity Trackers: A Survey on Utility, Privacy, and Security

Journal Article

Author(s):
Salehzadeh Niksirat, Kavous; Velykoivanenko, Lev; Zufferey, Noé; Cherubini, Mauro; Huguenin, Kévin; Humbert, Mathias

Publication date:
2024-07

Permanent link:
https://doi.org/10.3929/ethz-b-000661382

Originally published in:
ACM Computing Surveys 56(7), https://doi.org/10.1145/3645091

Wearable Activity Trackers: A Survey on Utility, Privacy, and Security

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

Over the past decade, wearable activity trackers (WATs) have become increasingly popular. However, despite many research studies in different fields (e.g. psychology, health, and design), few have sought to jointly examine the critical aspects of utility (i.e., benefits brought by these devices), privacy, and security (i.e., risks and vulnerabilities associated with them). To fill this gap, we reviewed 236 studies that researched the benefits of using WATs, the implications for the privacy of users of WATs, and the security vulnerabilities of these devices. Our survey revealed that these devices expose users to several threats. For example, WAT data can be mined to infer private information, such as the personality traits of the user. Whereas many works propose empirical findings about users' privacy perceptions and their behaviors in relation to privacy, we found relatively few studies researching technologies to better protect users' privacy with these devices. This survey contributes to systematizing knowledge on the utility, privacy, and security of WATs, shedding light on the state-of-the-art approaches with these devices, and discussing open research opportunities.

CCS Concepts: • **Human-centered computing → Ubiquitous and mobile computing**; • **Security and privacy → Human and societal aspects of security and privacy**; *Systems security*; *Network security;*

Additional Key Words and Phrases: Wearable activity tracker, fitness tracker, privacy, security, utility, survey, literature review

ACM Reference Format:
Kavous Salehzadeh Niksirat, Lev Velykoivanenko, Noé Zufferey, Mauro Cherubini, Kévin Huguenin, and Mathias Humbert. 2024. Wearable Activity Trackers: A Survey on Utility, Privacy, and Security. *ACM Comput. Surv.* 56, 7, Article 183 (April 2024), 40 pages. https://doi.org/10.1145/3645091

L. Velykoivanenko and N. Zufferey contributed equally to this work.

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.

Authors' addresses: K. Salehzadeh Niksirat (Corresponding author), University of Lausanne, Department of Information Systems, Internef, Dorigny Campus 1015, Lausanne, VD, Switzerland and École Polytechnique Fédérale de Lausanne (EPFL), School of Computer and Communication Sciences, BC 202, Station 14, Ecublens, 1015, Lausanne, VD, Switzerland; e-mail: kavous.salehzadehniksirat@unil.ch; L. Velykoivanenko, N. Zufferey, M. Cherubini, K. Huguenin, and M. Humbert, University of Lausanne, Department of Information Systems, Internef, Dorigny Campus,1015, Lausanne, VD, Switzerland; e-mails: lev.velykoivanenko@unil.ch, noe.zufferey@unil.ch, mauro.cherubini@unil.ch, kevin.huguenin@unil.ch, mathias.humbert@unil.ch.

ACM 0360-0300/2024/04-ART183
https://doi.org/10.1145/3645091

1 INTRODUCTION

Wearable Activity Trackers (WATs) are smart devices that record human activity data. They often exist in the form of wrist-worn bracelets and watches, such as fitness trackers and smartwatches. WATs are becoming extremely popular. In 2020, the market was estimated to be $36.3 billion and is projected to grow to $114.4 billion by 2028.[1] Due to high sales and market penetration, many WAT devices, brands, and **Service Providers (SPs)**, such as the Apple Watch, Fitbit, and Garmin, have become household names.

There has been extensive research on WATs. Researchers have studied WATs from different perspectives, such as design [187], psychology and behavior change [133], health [194], rehabilitation [97], reliability and accuracy [53], security and privacy [153], usability [159], and sensing technology [217]. Three very important aspects of WATs are utility, privacy, and security. Like any other technology, WATs have benefits but also expose users to risks. On the one hand, they can empower users to become more self-conscious and improve their well-being. On the other hand, due to the sensitive nature of the data they collect, they can also endanger users' privacy. These benefits and risks are also related to how users *perceive* the utility and privacy of their WATs. Utility and privacy are interwoven concepts. According to the privacy calculus theory [17, 137], before using technology, users usually perform risk-benefit analyses and consider the tradeoffs between them. It is also essential to not overlook the critical dimension of security, as it plays a pivotal role in mitigating risks where the data collected by WATs must be protected from unauthorized access. In this survey, we provide knowledge on the benefits WATs provide, the users' perception of them, and the associated security and privacy risks. For additional relevant topics, we cover existing regulations for the protection of users, security vulnerabilities of WATs, and the existing privacy-enhancing solutions. The contributions of this survey are threefold:

- We discover the main privacy issues that stem from using WATs.
- We shed light on the utility aspects of WATs; they have implications for privacy and security.
- We review the WATs' potential security vulnerabilities, attacks on WATs, and the existing countermeasures.

1.1 Novelty Statement

Numerous literature surveys related to WATs—and wearables in general—have been published. Table 1 summarizes these surveys. Several surveys provide valuable insights and in-depth knowledge, from different perspectives, about wearables. For example, they review applications of wearables for healthcare [110, 177, 256], rehabilitation [181], occupational safety [179, 232], and activity recognition [130]. They also review the reliability [81], adoption [117], privacy [52, 206], and security [56, 216, 223] of wearables. However, these surveys cover various types of IoT devices and wearables (e.g., eye-worn glasses, EEG devices) that are not specifically designed to track **Physical Activity (PA)**, thus making it difficult to determine which findings are specific to WATs. The present survey focuses solely on WATs to reveal related findings and research gaps that are specific to WATs.

Whereas previous surveys on WATs focused on utility [220], reliability [68, 127], quality [213], and WATs' effectiveness for behavior change [231], the present survey takes a *holistic* approach by integrating *utility*, *privacy*, and *security* aspects. This is important for three reasons. First, research on WATs is *multi-faceted*, as these devices serve practical purposes by collecting personal data and exposing users to privacy threats. The comprehensive approach provided by this survey ensures that readers gain a well-rounded understanding of the benefits and perils of using these devices.

[1] https://www.fortunebusinessinsights.com/fitness-tracker-market-103358 (last accessed February 2024).

Table 1. Summary of the Published Surveys about the Utility, Privacy, and Security of WATs and Generic Wearables

	Device		Aspect			
Surveys	**Wearables**[†]	**WATs**	**Utility**	**Privacy**	**Security**	**Year ▲**
Pantelopoulos and Bourbakis [177]	✓	–	◔	○	○	2009
Patel et al. [181]	✓	–	◔	○	○	2012
Lara and Labrador [130]	✓	–	◔	◔	○	2012
Evenson et al. [68]	-	✓	◔	○	○	2015
Iqbal et al. [110]	✓	–	◔	○	○	2016
Kolla et al. [127]	–	✓	◔	○	○	2016
Kalantari [117]	✓	–	◔	◑	◔	2017
Seneviratne et al. [216]	✓	–	◔	◔	●	2017
Shrestha and Saxena [223]	✓	–	◔	●	●	2017
Sullivan and Lachman [231]	–	✓	◔	○	○	2017
Georgiou et al. [81]	✓	–	◔	○	○	2018
Datta et al. [52]	✓	–	○	◑	○	2018
Saa et al. [206]	✓	–	○	◑	○	2018
D'Mello et al. [56]	✓	–	◔	◔	◑	2018
Wu and Luo [256]	✓	–	◔	○	◔	2019
Shin et al. [220][‡]	–	✓	●	◑	○	2019
Schiller et al. [213]	–	✓	◑	◔	◔	2020
Svertoka et al. [232]	✓	–	◔	◑	◔	2021
Pasquale et al. [179]	✓	–	◔	○	○	2022
→ **Ours**	–	✓	●	●	●	2024

○, ◔, ◑, and ● show roughly the extent to which each survey covered each domain, indicating the following: ○ *Not Covered*, ◔ *Minimally Covered*, ◑ *Moderately Covered*, and ● *Mostly Covered.* [†] These papers cover a wide range of wearable devices, such as head-mounted displays, biosensor systems, smart glasses, smart watches, fitness trackers, vital signs monitors, industrial wearables, smart fabrics, EEG devices, and other physiological sensors. [‡] Shin et al. [220] present a comprehensive survey about WAT utility for papers published between 2013 and 2017. However, their focus on privacy is limited, with only half a page devoted to 29 privacy-related papers. This work does not cover security, nor does it discuss the tradeoffs between utility and privacy.

Second, utility, privacy, and security are inherently *intertwined*, where challenges in one domain inevitably affect the others. The well-documented tradeoff between utility and privacy further illustrates this connection [17, 137]. In addition, privacy threats identified for WATs are necessarily connected to the security measures implemented by SPs. Our integrated approach offers valuable insights into three cardinal dimensions of WAT research. Third, the holistic approach also allowed us to draw a research agenda for WATs by identifying six research gaps that researchers might explore next.

Finally, many research articles on WATs have been published in the past 5 years but were not considered in past surveys of wearable technology. Given the speed at which new technologies in WATs emerge and advancements in sensor technologies (e.g., oximeter sensors added after COVID-19), updating the survey on WATs research was necessary.

1.2 Survey Method

Figure 1 summarizes our methodology. We conducted a systematic literature review following the assessment criteria of Kitchenham et al. [126] (e.g., inclusion/exclusion criteria, comprehensive

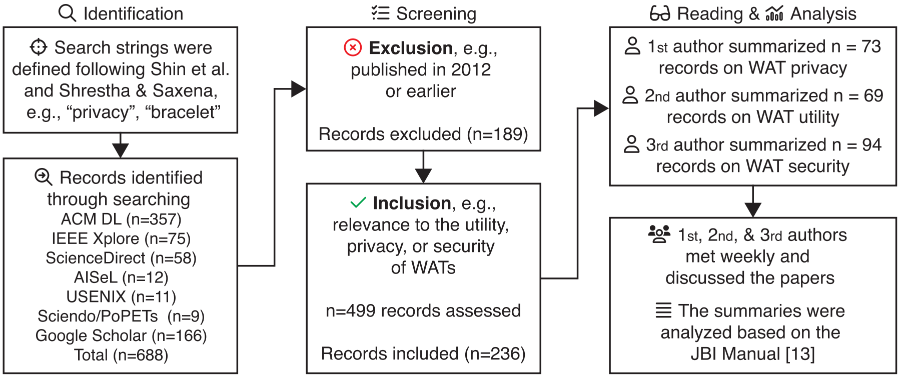
Identification
Search strings were defined following Shin et al. and Shrestha & Saxena, e.g., "privacy", "bracelet"
Records identified through searching
ACM DL (n=357)
IEEE Xplore (n=75)
ScienceDirect (n=58)
AISeL (n=12)
USENIX (n=11)
Sciendo/PoPETs (n=9)
Google Scholar (n=166)
Total (n=688)
Screening
Exclusion, e.g., published in 2012 or earlier
Records excluded (n=189)
Inclusion, e.g., relevance to the utility, privacy, or security of WATs
n=499 records assessed
Records included (n=236)
Reading & Analysis
1st author summarized n = 73 records on WAT privacy
2nd author summarized n = 69 records on WAT utility
3rd author summarized n = 94 records on WAT security
1st, 2nd, & 3rd authors met weekly and discussed the papers
The summaries were analyzed based on the JBI Manual [13]

Fig. 1. Summary of the survey methodology. The full list of search strings are listed in Section 1.2.

literature search). To identify relevant papers, we crafted a set of search strings that encompassed the key terms related to our research focus: ["physical activity data" OR "fitness data" OR "fitness tracking" OR "wearable activity tracking" OR "physical activity tracker" OR "fitness tracker" OR "wearable activity tracker"] AND ["utility" OR "privacy" OR "security" OR "perception" OR "understanding" OR "experience" OR "expectation" OR "sharing"] AND ["system" OR "device" OR "application" OR "app" OR "service" OR "bracelet" OR "wrist-worn"]. We chose these specific keywords, according to previous surveys [220, 223], to ensure a comprehensive search and to enable us to capture a wide range of relevant literature while excluding studies that do not directly contribute to our inquiry. For example, we include "physical activity data" and "fitness data", as they are directly related to the topic of WATs. In addition, we used "fitness tracker" and "wearable activity tracker", as they were interchangeably used in the literature to refer to WATs. We also used terms such as "bracelet" and "app", as they uncover studies related to the physical form factor of WATs or other entities in the WAT ecosystem. We searched in ACM DL, IEEE Xplore, the AIS library, USENIX, PoPETs, ScienceDirect, and Springer Link. We used Google Scholar to include papers from other databases and publishers (e.g., Taylor & Francis). To update our paper database during the review process, we also kept track of the most recent and relevant published proceedings (e.g., IMWUT). We identified 688 papers (after removing duplicates). After retrieving the full articles, we excluded the papers that (i) are not written in English, (ii) were published in 2012 or earlier, or (iii) are not peer reviewed (e.g., position papers, letters, editorials, prefaces, article summaries, theses, patents, or books). We included only the papers that met both of the following criteria: (i) they are about WATs and/or have implications for WATs, and (ii) they have direct relevance to the utility, privacy, and/or security of WATs. The first author applied the inclusion and exclusion criteria and later confirmed them with the second and third authors. Out of 688 papers, 236 were selected to be reviewed (including two papers we added after the first survey submission).[2] Three authors summarized the papers' context, methodology, and findings. The reviews were discussed in weekly meetings. To synthesize the findings, we adhered to the guidelines provided in the *JBI Manual for Evidence Synthesis* [13]. First, we reviewed the summaries of the papers, identifying the common patterns and homogeneity between them. Then we highlighted aspects of heterogeneity and diversity with regard to their findings.

1.3 Survey Structure

The remainder of the survey is organized as follows. In Section 2, we define WATs and explain their ecosystem. In Section 3, we discuss several aspects of WATs' utility, such as their core benefits and

[2] The list of the reviewed papers and their summaries are available on OSF (https://doi.org/10.17605/osf.io/7mkre)

different usage patterns, including social usage and data sharing. In Section 4, we first discuss the risks of WATs for users' privacy and the main findings about users' awareness, attitudes, and behaviors. We review WATs' privacy policies, the existing regulations for protecting users, and the ethical aspects of using WATs for research or health campaigns. In Section 5, we discuss how utility, privacy, and security are intertwined and how users make tradeoffs among these aspects. In Section 6, we review different types of attacks and security vulnerabilities related to WATs. In both Sections 4 and 6, we present the existing work as **Privacy-Enhancing Technologies (PETs)** and security countermeasures. In Section 7, we discuss several open issues concerning WATs and possible opportunities for future research. We conclude the article in Section 8.

2 WAT DEFINITION AND ECOSYSTEM

There is no consensus about the definition of a WAT. However, there are many commonalities between the various definitions. To create a standardized definition, we took a philosophical approach [201] by identifying the *essential* and *accidental* properties of WATs, according to earlier studies on WATs [23, 106, 186]. To be a WAT, an object needs to have all of the following essential properties (E) and can also have accidental ones (A):

- E1. It must be worn on the body
- E2. It must have sensors that record physiological/environmental data
- E3. It must be an electronic/digital device
- E4. It can come in various forms (e.g., wrist-worn, strap, clip-on)
- E5. It must provide data analysis that is available to users, without the need for a health professional
- E6. It must enable users to gain access to actionable information that is derived from the sensor data
- A1. It can upload data to a server or connected device
- A2. It uses a docking station to sync with a PC or uses WiFi to upload data directly
- A3. It enables users to visualize data in graphical format on a companion app or website
- A4. It enables users to visualize data on the WAT itself
- A5. It can provide immediate feedback
- A6. It can provide general/numerical feedback (after an activity)

The most common *sensors* used in WATs are accelerometers, photoplethysmograms (used for measuring heart rate and respiration), pulse oximeters (blood oxygenation), gyroscopes, altimeters, and GPS. The more advanced and recent models tend to include a compass, thermometer, microphone, magnetometer, ambient light sensor, and an electrodermal activity sensor. Therefore, we consider smartwatches as WATs, even if they offer more functionalities than some fitness trackers. We do not consider medical-connected devices (e.g., insulin pumps) and wearable devices with very specific purposes (e.g., connected shoes) as WATs.

The typical WAT *ecosystem* is composed of a WAT paired with a connected device (e.g., smartphone, tablet) on which a companion app provided by the WAT's SP is installed. The companion app communicates through the Internet with the SP's servers (Figure 2(a)). The servers store the users' WAT data and can process raw WAT data and perform various analytics [113]. The WAT collects data by using different sensors and regularly synchronizes with the companion app that uses Bluetooth communication (see Figure 2(b)). During this synchronization, the data is usually uploaded to the SP's servers. The connected device can store recent data, whereas older data needs to be downloaded from the server (see Figure 2(c)). The connected device can also send data to the WAT, such as firmware updates or notifications [242]. A user can also permit **Third-Party Applications (TPAs)**, such as Strava, to access their data (see Figure 2(d)). The TPA requests data

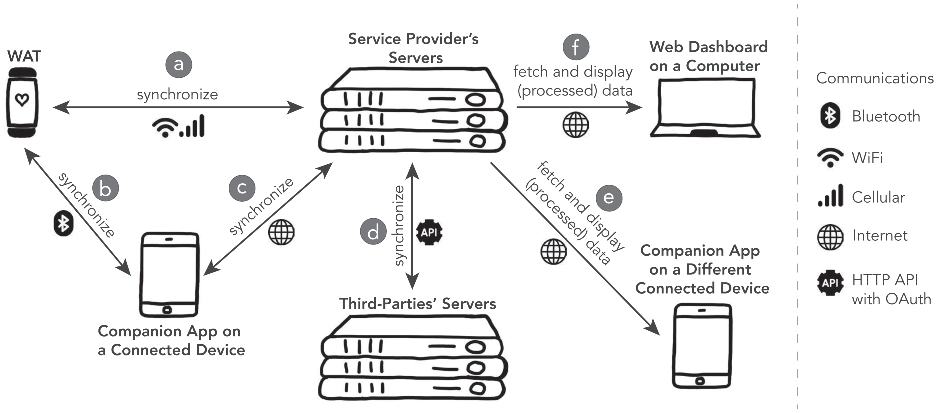
WAT
a
synchronize
Service Provider's Servers
f
fetch and display (processed) data
Web Dashboard on a Computer
b
synchronize
c
synchronize
d
synchronize
API
e
fetch and display (processed) data
Companion App on a Connected Device
Third-Parties' Servers
Companion App on a Different Connected Device
Communications
Bluetooth
WiFi
Cellular
Internet
HTTP API with OAuth

Fig. 2. WAT ecosystem, adapted from Velykoivanenko et al. [242].

from the SP's server by using a dedicated API or, in some cases, it directly accesses data stored on the connected device (e.g., through Apple's Health app). The user will then generally be able to access their data by using the TPA's functionalities. The same data-sharing method also works in reverse, thus permitting the companion app and/or the SP to access the data originally collected by a TPA [269]. Many existing WATs, such as the Apple Watch,[3] Fitbit, and Garmin match this model. Users can also access their data by using secondary connected devices (see Figure 2(e)) or on the web dashboard of their SP (see Figure 2(f)).

3 BENEFITS AND UTILITIES

Research shows that WATs can provide users with a variety of benefits:

- *Physical activity*: WATs can increase users' motivation to engage in PA [43, 76, 97, 98, 113, 133, 151, 159, 173, 180, 186, 190, 194, 199, 228, 253]. They can help users increase PA [43, 76, 97, 98, 143, 171, 174, 194, 199, 221], improve sports performance, and monitor their performance [180, 186, 196, 253].[4] However, the increase in PA might not always be sustained after the users stop using a WAT [131, 171]. Generally, as WAT use increases, users tend to perceive more benefits [76, 149].
- *Health improvements*: WATs can provide the motivation for measurable benefits, such as weight loss for obese patients [76, 194, 253], and can have a positive effect on users' perceived self-efficacy and health behavior [200].
- *Medical benefits*: WATs can improve interactions between patients and medical practitioners [97, 159] and support patient monitoring [27, 115, 159, 186].
- *Social benefits*: WATs can facilitate, support, and strengthen users' social bonding [94, 174, 194, 196, 199, 202, 211], and can support collaborative fitness goals [203].
- *Sleep quality*: Many WATs provide a sleep-tracking functionality. Users see benefits in having access to their sleep data [197], even if some track their sleep without a specific goal [202]. However, users might have difficulties using such a functionality, due to not tracking continuously [145, 242], to not trusting the accuracy of the data [186, 197], and/or to not being able to easily manipulate or interpret the data [145, 197].

[3] Health data collected through Apple devices is end-to-end encrypted and could be accessed. through mobile APIs.
[4] In one study, Gui et al. [94] found that tracking does not increase PA.

Table 2. WAT Users Identified in the Literature with Different Types of Usage Patterns

User Types	**Differences**
Behavior-change trackers vs. *Instrumental* trackers vs. *Curiosity-focused* trackers [67]	Behavior-change trackers do a lot of research and aim to reach their goals. Instrumental trackers seek to maximize the benefits of their tools. Curiosity-focused trackers use WATs out of curiosity.
Technologically savvy vs. *Non–technologically savvy* users [139, 205]	Technologically savvy users are more likely to find WATs easy to use.
Younger vs. *Older* users [122, 139, 188, 205, 211]	Older adults had difficulties with setting up/syncing their trackers with TPAs [139]; older adults require the support of younger family members to help them overcome technological barriers [211].
Elite athlete vs. *Amateur athlete* users [196]	Elite athletes focus on tracking metrics they consider important (e.g., HR) and share data to portray a specific image of themselves to impress their fans and confuse rivals.
Power users† [76, 143, 151, 163, 233]	With regard to use consistency, they exemplify the simplest use pattern by having consistent and intense tracker use.
Long-phase users† [76, 143, 163]	They track without major disruptions for long periods of time.
Consistent users† [76, 163]	They track with moderate consistency.
Intermittent users† [76, 163]	They have consistent but sparse usage; they do not want complete logging; instead, they have other reasons for tracking.
Inconsistent users† [143, 233]	They go through periods of varying length (daily use) and take breaks of varying lengths.
Experimenters† [163]	They use WATs frequently but for short periods of time (e.g., only while exercising).
Hop-on hop-off users† [163, 233]	They frequently take long breaks yet regularly resume use.
Quantified-selfers† [113]	They never lose interest in the information provided by WATs.

† These usage patterns emerge after long-term WAT use.

- *Others*: WATs can help users teach children to be more independent (e.g., via chore reminders) [174]. They can also support scientific research [199, 243, 262]. Some users simply use WATs as watches [131, 186, 202] and/or to satisfy their curiosity and design tastes [202].

Next, we review general WAT usage patterns, data-sharing practices, and the ways WAT use was found to evolve over time. Finally, we summarize the studies that focus on the usability and user experience of WATs.

3.1 WAT Usage Patterns and Motivations

Users have unique reasons for (and ways of) using WATs [89, 112, 113, 125, 163]. Various patterns have been identified based on the profile characteristics of WAT users (Table 2). Users check their WATs more often while exercising [10, 92] and prefer to engage in activities that their WATs can track [76]. Users might use different trackers to track different types of activities (e.g., using one to track walks and another to track runs) [10, 202]. Users might concurrently use multiple devices [6, 42, 145]. Next, we list users' motivations for tracking:

- *Logging*: Some users use WATs to document their activities [176, 186, 202].[5]
- *Goal setting*: WATs usually support users in setting daily or weekly PA goals. Most users use the default 10K steps per day goal [233] , whereas others pursue longitudinal achievements (e.g., walking 10K steps every day for 30 days in a row) [202]. Users might also have broader goals that are not directly measured by WATs (e.g., weight loss) [186, 202]. Generally, users follow defaults set by WATs [76, 133].
- *Self-reflection*: Some users do not follow specific goals with WATs [10, 133]. Instead, they use WATs to reflect and learn about themselves [92]. For this, they mainly refer to their

[5] To read a survey on personal informatics, see the work of Epstein et al. [64].

short-term usage data (e.g., only for the current day) [42, 202, 233]. This analysis helps users to consider contextual information [209] (e.g., their emotional state [6]). Long-term data are rarely analyzed [42, 202, 233], but when it is, it prompts users to reconsider their past behaviors with regard to their PA [42] (e.g., peaks and extreme data).

- *Social benefits*: Some users share data with groups to compete with others (e.g., challenging others or chatting about PA) [190]. Some users like having access to other people's WAT data [94] to give and receive support [94, 139, 141, 190].
- *Monetary incentives*: Some users use their trackers to gain financial rewards, such as benefits provided by health insurance companies [159].

3.2 Social Usage and Data Sharing

The most common way of sharing WAT data is through companion apps on smartphones or, less frequently, through desktop companion software [71]. Findings on users' propensity to share WAT data are varied. Tang and Kay [233] found that about 50% of users use social features, whereas Rooksby et al. [202] found that only a small percentage share their WAT data. To share and compare data easily, those who share tend to use devices and apps that are similar to those their friends and family have [94, 139, 196, 211]. Interestingly, Fritz et al. [76] found that sharing with friends and family is not an effective strategy for increasing motivation, whereas sharing with strangers is. Sharing could support reaching a common goal and increase motivation. In *cooperative tracking*, a group goal must be reached under specific constraints (e.g., only one member of the group can contribute toward the activity goal at a given time) [199, 203]. This was found to increase relatedness and boost individual motivation [203]. In general, users find value in comparing their data with that of others [10, 190, 253]. Sharing enables users to *engage* in constructive discussions [190], and to *compete* with friends, family [159, 209, 221], and strangers [190, 202].

Caregivers can monitor their children's data to check if they are healthy or to keep track of the children's chores [174]. When a child's tracker does not work correctly, they can feel 'left out.' Families in low-income neighborhoods could have limited engagement with WATs, as they often prioritize their children's education over their physical health [209]. But WATs can promote social mindfulness in high-crime areas, where users feel a sense of safety and community support [208].

Users' willingness to share WAT data depends on the *type of data* shared and *with whom* it is shared [78, 190]. Users mainly share WAT data with people they know [78, 94, 190] and with people who are similar to them (e.g., same gender, goals, activities, and/or interests) [190, 211, 228]. Pevnick et al. [183] found that male and young healthcare workers are more willing to share WAT data with healthcare providers. Users share data with friends and strangers to compete and/or to show a positive image of themselves, whereas they share data with family members to encourage and motivate one another to be healthier [7].

Users can also share data to increase their social status [159, 196, 253]. Some might even manipulate their data for entertainment/presentation purposes [94, 196], which can be perceived as *bragging* [202]. Furthermore, some users might feel *intrusive* looking at WAT data belonging to people that they do not know [190]. Finally, other research has identified groups of users who prefer to not share their WAT data [76, 202].

3.3 Evolution over Time

The way users use their WATs changes over time [76, 233]. We identified four categories of usage duration:

- *First evaluation (0–1 month)*: WAT use is generally consistent over time [163], and users explore and experiment with different features [121]. During this initial phase, they begin to experience most of the previously discussed benefits (e.g., increases in PA, strengthening of social bonds). During this phase, users typically decide whether WATs bring value to their lives [188], or if they will stop using them [143].

- *Short-term use (1–6 months)*: Users *accommodate* WATs into their lives [121]. During this phase, the frequency of use was found to vary: from short periods of time to almost every day [143, 163].
- *Medium-term use (6–12 months)*: Users *integrate* WATs into their lives, benefiting from improved well-being, lifestyle changes, noticeable physiological changes (e.g., weight loss), reinforced PA awareness, and greater social reach [194].
- *Long-term use and fading of interest (>12 months)*: Some users integrate WATs *more deeply* into their lives, whereas others lose their initial enthusiasm yet still continue to use them for their routine activities [76].

Over time, users' habits were found to change: they change their motivations [10] and goals [186, 233] to use WATs. Interestingly, WAT data utility becomes less meaningful and relevant over time, as users correlate it with their routines [113]. After long-term use, distinct usage patterns emerge. These usage patterns are summarized in the second half of Table 2.

Several studies have identified patterns of engagement with WATs, more specifically around *adoption*, *adherence*, and *abandonment*. Table 3 summarizes various elements that were found to positively or negatively influence users' decisions to adopt, adhere to, or abandon their WATs.

Adoption. Research has identified several factors that can either motivate users to adopt WATs or can hinder their adoption [173]. For example, *curiosity* and *trust* can act as nudges for adoption, whereas *lack of interest* and *privacy concerns* can be hindersome. Understanding how users typically acquire WATs helped us better understand WAT adoption. Most often, individuals were found to have purchased the WATs *themselves* [47]. Specific WAT models might be selected based on friends' recommendations [151, 202]. However, they can also be acquired *indirectly* as part of a wellness program [47, 102], as a gift, or as a prize [47].

Adherence. Users' adherence to WATs is influenced by a variety of factors. For example, users' perceived benefits of using WATs [25], convenient access to health information [32], and expert advice in companion apps [255] positively affect users' decisions for adherence. In addition, when a user feels invested in a WAT, they are more likely to use it [47]. Once WAT use becomes routine, users continue using it, purely out of habit, even if they no longer perceive any benefits [115, 131, 204]. On a different note, Tang et al. [234] defined different thresholds for assessing users' level of adherence, as follows: (i) strictly, more than 0 steps on a given day, (ii) more than 500 steps on a given day, (iii) more than 10 hours of data recorded on a given day, and (iv) activity logged in the morning, afternoon, and evening (or so-called "3-a-day"). They showed that the step-related thresholds (items (i) and (ii)) are more effective and lead to similar adherence features when they are used to include/categorize participants in research studies. In contrast, the "more than 10 hours" and "3-a-day" thresholds (items (iii) and (iv)) have diverse effects on participant inclusion/categorization.

Abandonment. After a certain time, most users were found to abandon their WATs. During the first 30 days after acquisition, if a user does not use their WAT *weekly*, they are more likely to stop using it [70]. Past research identified the following proportions of users who churn after initial setup:

- A small portion of users abandon their WATs within the first week [47].
- Many users abandon during the first 3 months [47, 131].
- Others abandon within 6 months [47, 57, 163].
- The remainder abandon within the first 3 years [70].

Table 3. Different Factors That Can Positively or Negatively Influence Adoption, Adherence, and Abandonment

Factor	Adop.	Adhe.	Aban.
To get *benefits* (increasing PA [43, 67] and keeping motivation [43, 76, 176])	↗	–	–
Perception of WATs as useful and beneficial [25, 193]	↗	↗	–
To gain *utility* (customization [266], fashion and ergonomic [54, 253], and design trends [44])	–	↗	–
Trusting SPs [2]	↗	–	–
For *curiosity* [131, 202]	↗	–	–
Social influence [79, 124, 198] and *intergenerational* motivations [174, 209, 211]	↗	–	–
To continue *sharing* data with friends and family [94]	–	↗	–
Constructs of *Self-Determination Theory (SDT)*: Relatedness, Competence, and Autonomy [266]	–	↗	–
Convenient *access* to health information [32] and expert health advice [255]	–	↗	–
Being offered *financial incentives* for sharing WAT data, such as through corporate wellness programs [43, 159, 176]	↗	–	–
Feeling *financially invested* in a WAT [47]	–	↗	–
Habituation: When usage becomes routine [115, 131, 204]	–	↗	–
Collecting data *for the future* when more advanced analysis techniques are available [113, 131]	–	↗	–
A lack of interest [43, 47] or *willingness* to become overly focused on WAT data [43, 209]	↘	–	–
Lack of alignment with users' personal fitness goals or using another WAT and not wanting to switch, in the context of employer-sponsored wellness programs [43]	↘	–	–
A *misalignment* between expectations and the experienced reality of using WATs [47, 131, 194]	–	–	↗
After *accomplishing initial goals* [14, 47, 65]	–	–	↗
Internalizing PA goals and habits [89]	–	–	↗
Contextual changes such as changes in life circumstances [14], participating in activities that their WAT cannot track [47, 65] (e.g., a new fitness program), and changing jobs/schools if the new workplace/school does not allow tracking on their premises [47]	–	–	↗
Changes in initial *intrinsic motivations* [14] and after the sense of curiosity is fulfilled [47, 113, 121, 131]	–	–	↗
Health-related reasons such as injuries [14, 47, 65] or physical inability to engage in PA [47, 91, 98, 115]	–	–	↗
Lack of utility [14, 66, 131], *technical barriers* [43], and *issues with data* [14, 131] (e.g., lack of accuracy [14, 65, 102, 131, 171] and/or feeling uncertainty about data [6, 102])	↘	–	↗
Physical *discomfort* (e.g., skin irritation) [14, 47, 102, 115, 131, 159, 186, 242]	–	–	↗†
Unpleasant *aesthetics* [102]	–	–	↗
Too much *investment of time and effort* for tracking (e.g., having to sync the device) [14, 43, 65, 131]	↘	–	↗
Privacy concerns [14, 43, 65, 79, 124, 137, 173, 176, 198, 215, 242]	↘	–	↗†
Lack of social engagement [102], inability to compare data with others [47, 102], or losing interest in comparisons with others [14]	–	–	↗
Charging the WAT [102, 242]	–	–	↗†
Hygiene reasons [242]	–	–	↗†
Being *forced* to (e.g., during security checks) [242]	–	–	↗†
After seeing *negative results* (e.g., not wearing the WAT on days with low PA) [180]	–	–	↗†
Negative emotions (e.g., guilt for not meeting daily PA goals) [6, 14, 65, 66, 89, 91, 97, 98, 115, 171]	–	–	↗
Forgetfulness [14, 67, 242]	–	–	↗

↗ and ↘ indicate positive and negative impacts, respectively. † The abandonment could be temporary.

The reasons for abandoning WATs vary greatly: tracking is no longer feasible or necessary, WATs do not provide sufficient utility, and the cost of using WATs is perceived to be too high (see Table 3). Sometimes users suspend usage of their WATs temporarily [163]. In Table 3, we report factors that can cause temporary vs. permanent abandonment. Epstein et al. [65] found that users who abandon their WATs can feel *guilty* when the abandonment is due to factors beyond their control, *frustrated* when they realize they could not achieve their initial goals, and *relieved* if they realize they no longer need to invest the time and effort to maintain the device active. When users were found to be experiencing negative emotions in relation to the usage of their WAT, removing it could reinstate a feeling of control [89].

3.4 Usability and User Experience

Overall, interfaces of WATs are perceived as easy to use [159, 186, 188]. In general, users perceive the immediate feedback provided by WATs as useful, because it helps them achieve their goals [173], and to become more aware of their body image [29]. However, past research has identified several usability issues with different types of WATs.[6] Matt et al. [159] found that the *onboarding* experience might be overwhelming for some users. Furthermore, users were found to have issues with basic tasks, such as synchronizing their WATs with their online accounts [167, 174]. With many types of WATs, the user interface tends to lack customization, personalization, and language (localization) support [167]. Additional issues were identified with navigation, text entry, and voice recognition [26, 167], and also with insufficient *accessibility* support [167]. New users of WATs were found to have trouble making sense of the numerical and visual representation of their PA data [10, 121], which could lead to frustration with their WATs [6, 188].

Past research also identified issues with WATs' activity detection and notification. Several types of WATs were found to incorrectly identify context (e.g., WATs giving prompts to walk while the user is on an airplane) [167]. WAT notifications were also found to be disruptive, interfering with concentration (e.g., by distracting the user by vibrating/flashing), and can reduce sports performances [10].

Identified issues also concerned the *accuracy* of measurements of WATs. Data collected by WATs was found to not always represent actual PA (e.g., steps were recorded when none were taken [159]). Accuracy issues can elicit negative emotions in users (e.g., mistrust and annoyance) toward their WATs [76, 98]. Users were found to have differing requirements for accuracy [186, 261]. Some categories of users were found to care about the accuracy of WAT data [26, 65, 145, 167, 176, 188, 202, 253], whereas other types of users were not very interested in the accuracy of their WAT data [94]. More specifically, past research identified that users tend to perceive the accuracy of their WAT data in three ways: *accurate and reliable* [196]; *partially accurate, but still useful* [6, 26, 186, 196, 202]; and *inaccurate and unreliable* [26, 65, 98, 159, 167, 186, 202].

Finally, many issues identified in past research are related to the *ergonomics* and form factors of WATs:

- physical discomfort [102, 145, 159, 196];
- insufficient battery life [26, 145, 167];
- fragility [26];
- not being waterproof [159, 167];
- readability of the display under direct sunlight [167]; and
- insufficient feedback (e.g., weak vibration, lack of alerts, and presentation issues) [167].

4 PRIVACY

We begin by discussing the types of information that can be derived from WAT data and whether this information poses any threats to user privacy. **Machine Learning (ML)** models using WAT data can be used to infer the following information about users:

- *Health metrics*: WAT data can be used to monitor ECG waveforms [37], post-surgery complications [264], symptoms of multiple sclerosis [95], SARS-COV-2 infections [105], and mental health states (e.g., stress resilience) [3], and it can be used to predict the readmission

[6] It is important to note that many of these usability issues may have been addressed or resolved over time.

of cancer patients [15]. Combining WAT data with other resources can help build a health persona [111]. In an edge case, WAT data could help specialists better understand the social engagements between autistic children who have difficulties with non-verbal communication [251].

— *Activities*: Studies about **Human Activity Recognition (HAR)** show how activities can be inferred using WAT data. The most frequently inferred activity types are *eating* and *drinking* [28, 236, 252]. In addition, in relation to consumption, a model to detect users' *drunkenness* in real time was developed [99]. Shoaib et al. [222] use WAT data to detect *smoking* events. WAT data can also be used for other purposes, such as tracing the *geometric motion of a user's arm* [217], recognizing objects moved by users and the identity of the users who moved them [195], and preventing *pedestrian distractions* [245]. Several novel algorithms and frameworks were developed for HAR (e.g., [1, 144]). Dietrich and van Laerhoven [55] propose a typology for classifying the different contexts of WAT usage. Activities can be successfully recognized, even for short-duration data (i.e., short and quick movements) [240]. Such inferences are generally more efficient than with other common devices' data (i.e., smartphones) [53]. This is because WATs, unlike phones that are usually in users' purses or pockets, are close to the body (i.e., wrist-worn).[7]

— *Personal characteristics*: Users' WAT movements, when using NFC payment terminals, can help infer their *height* [229]. Information shared by users on social media in a WAT context can be used to infer personal information, such as *weight* [250]. Under certain conditions, users' *handwriting* can also be recognized with WAT data, where inference is made not only to detect the event but also to infer the written letters and words [254, 257]. For example, WAT data can be used to recognize air-writing gestures (and words) [11], finger-writing gestures [259], and gestures of writing on a whiteboard [12]. WAT data can also be used to predict users' *moods* and subsequently to recommend music [138]. More recently, Zufferey et al. [268] showed that WAT data can be used to infer users' *personality traits*, particularly three of the Big Five personality traits (i.e., openness, extraversion, and neuroticism).

— *Location*: A few studies focus on *location inference*. Hassan et al. [103] studied bypassing EPZs (endpoint privacy zones) to infer WAT users' locations; they could infer more than four-fifths of the locations. EPZ is a mitigation technique that consists in defining a private zone within which some data are not revealed. Meteriz et al. [162] also showed that location inference is possible, with certain previous knowledge and by using the elevation profile.

Are WATs Risky for Users' Privacy? A large majority of research on WAT inferences show that WAT data can also be used in *adversarial settings*, with potentially negative consequences for user privacy. For example, all information about consumption (e.g., eating, drinking, smoking), activities (e.g., sports), location (e.g., city name), traits (e.g., personality), and disease (e.g., cancer) can be directly used by adversaries (e.g., health insurers, employers, and advertisers) to target their customers and/or even to discriminate against them.

4.1 WAT User Privacy Awareness, Knowledge, Concern, Attitude, and Behavior

Awareness and Knowledge. Most users tend to have a *limited understanding* of how WATs and their ecosystem work (i.e., how their data is processed and analyzed). Users are not aware of who has access to their data, and of how their data are transmitted, stored, and used [45, 49, 253]. They also cannot judge the difference between storing data on a cloud and on a device [35]. Velykoiva-

[7] "The hand is the visible part of the brain."—a quote attributed to Immanuel Kant by David Katz (see https://web.archive.org/web/20240203213122/https://www.gutefrage.net/frage/aus-welcher-quelle-von-kant-kommt-das-zitat-die-hand-ist-das-aeussere-gehirn-des-menschen; accessed February 2024).

nenko et al. [242] showed that only a small proportion of users understood correctly how data is transferred between their WAT and the SP's servers. These findings are supported by the research of Wieneke et al. [253], which found that users do not understand how SPs use their data, and by Zufferey et al. [269], who show that users lack knowledge about the data-sharing ecosystem—in particular, users' understanding of TPAs. The mental models of most WAT users do not correspond with the WAT ecosystem, and they become confused about which data they really shared with TPAs [269]. Users' lack of awareness might be due to a lack of interest in learning about how WAT data is used [253].

Users also have *limited knowledge about the privacy policies of SPs* [45, 246]. Vitak et al. [246] found that after they were asked to read the relevant part of the terms of service, most users were not aware of what they had given consent to and were surprised about the extent of access they provided to SPs.

Several *misconceptions* have been identified, including overconfidence in privacy knowledge [147]. Some users mistakenly believe that WATs are secure due to their lack of conventional "input" methods, such as a keyboard. Hence, they assume that sensitive information (e.g., a password) is not saved [147]. As people tend to use the same code for diverse applications and devices (e.g., ATM PIN codes), the risk of such attacks increases [148]. Users' beliefs depend on the *type of information* collected by WATs. Most users recognize only sensors that they can see and verify [191]. They believe that sensitive information not directly related to a specific sensor cannot be inferred from their data [242]. Users tend to believe that most privacy risks are *unlikely to materialize* [78]. They first consider the likelihood of being subject to privacy risk, and only then do they contemplate its severity [30]. As a result, not knowing the likelihood of such threats prevents them from thinking about their severity.[8] Many users consider privacy only from a 'social privacy' point of view and do not think about how their data could be used by third parties [152].

Privacy Concerns. Most users express only minor privacy concerns [7, 30, 123, 134, 147, 267]. The majority perceive their WAT data as harmless, innocuous, and not sensitive [134, 147, 267]. They report that they would share their data without requiring that the privacy boundaries be managed [147, 267]. Lidynia et al. [142] found that their study participants did not consider storing data on the SP's server (compared to their device) as a critical issue. Many users had mainly utility-related concerns (e.g., to have a better self-image from data sharing) rather than privacy-related ones [7].

Aktypi et al. [4] highlight that multiple factors reassure users about their privacy, especially the fact that they tend to trust WAT companies. However, there is no consensus about this trust. Although some studies show that users trust companies to handle their data [267] and believe in companies' technical capabilities to prevent privacy breaches [134], others [22, 147, 242] do not. Given the huge amount of data collected from millions of individuals, some users cannot see how their data can be used against them: " the information that would come from my device would be just a drop in the ocean" [4, p. 8]. For some users, privacy concerns can evolve over time. Some start being concerned if their data is misused or after their privacy is violated [123]. In the workplace context (for more details, see Section 4.3), at first, some users perceive their data as harmless. But over time, they report different concerns, as their data creates many inter-colleague discussions that reveal their private-life activities and create social pressure [87]. Interestingly, with the participants of research experiments, those who usually are unconcerned about privacy expressed their concerns about WATs, after being confronted with questions about their private life [147, 253]. This could be due to the well-known privacy paradox [82], where users report

[8] Gerber et al. [83] show that users perceive privacy risk scenarios as *likely* if they are written in an abstract form.

having privacy concerns, but then they behave as if they do not have these concerns. Finally, Vitak et al. [246] show that the more value users place on their WAT data, the more privacy concerns they have.

The minority of users who are aware of privacy risks tend to be more concerned about their privacy. *Concerned users* use coping mechanisms [19], implement stronger privacy safeguards to protect their information [35, 147, 267], and contemplate abandoning their devices [198]. Three types of concerns are recognized:

— *Data collection and storage*: Concerns about the anonymization of data [22] and the location of the data storage [22, 142].

— *Control over data*: Concerns about the data being used for purposes other than the pre-defined purpose or being shared with third parties [22, 147]. Some users believe they have limited control over the disclosure of their own data [147, 159, 172]. They also mention the *forced-choice dilemma,* where they have to decide between using the device (and facing the consequences) and not using it. Last, they mention the *post-purchase lock-in effect* where privacy policies might change after agreeing to them.

— *Storage security*: Some users are concerned about their devices or the SPs' platforms being hacked. They believe that security breaches could lead to negative consequences [172, 175].

Attitudes. Overall, users who are unaware of privacy risks tend to share more [184]. However, users' willingness to share WAT data is strongly related to the *type of data* and to the targeted *audience* [78, 214]. They perceive location data to be the most sensitive data type [77, 132, 142, 185, 267] and are concerned about the associated negative consequences, such as home burglary and bike theft [185]. In addition, users are more reluctant to share movement data, other than step data [123]. Weight and sleep data [142], as well as any data related to **Personally Identifiable Information (PII)** and financial information [7], are perceived as particularly sensitive. If users sell their data, they would ask for significantly more money for their location data than for health-related data [77].

However, even for the most sensitive data, users change their sharing decisions, based on the intended recipients. They generally seem willing to share their location with their friends, whereas they do not want to share it with online advertisers [78]. Schneegass et al. [214] found that users' willingness to share is inversely proportional to the size of the recipient group they share the data with. This finding is in line with other studies [7, 78, 134, 142, 269], wherein users would be willing to share their data with small groups of people, such as their family, friends and colleagues, and/or with health practitioners if they ask for it, but they would not share with the general public, employers, insurance companies, banks, and advertisers.

In the context of *sharing WAT data with family*, parents are interested in monitoring their children's health and activity levels, but not to the extent that it would compromise their relationships or prevent children from developing self-sufficiency [129]. However, usage of WATs by parents for monitoring their children can deteriorate trust in both directions [116]. Li et al. [139] find that younger users worry about their family members' opinions about them, based on their WAT data. Potapov and Marshall [187] reveal children's concerns about their data being misused by their teachers in a school context. In a different context, Leitão [136] shows that WATs can be used by abusive partners for stalking, threatening, and harassing (a.k.a. intimate partner abuse).

Behaviors. Overall, users take two types of privacy-related actions:

— *Preventive actions before privacy violation*: A few users report adjusting the privacy settings of their WATs immediately after setting up their device (i.e., after unboxing),[9] whereas others

[9] Some users find privacy settings complex and that they have difficulties adjusting them [185, 267].

could not remember when they changed them, and yet others thought they were using the default settings [267]. In the context of the workplace, users might consider partial sharing if they could exclude specific parts of their data related to private situations [123]. Almost one-third of users usually do not revoke the WAT data access they granted to TPAs, as they forget that they installed them on their devices [269]. A minority of users consider removing WATs for privacy-related reasons (e.g., before engaging in sexual activity) [242].

— *Mitigating actions after privacy violation*: Users use two main coping mechanisms [18–20]. The first is emotion-focused coping when the perceived level of threat is high and the level of efficacy is low, and the second is problem-focused coping when the perceived level of threat is low and the level of efficacy is high. Therefore, in the event of a privacy breach, users will likely not be able to show rational behavior and will instead seek emotional support. Although users' privacy perceptions do not have an effect on their preventive actions [30], their perceptions can affect their mitigating actions [18]: higher privacy concerns increase users' threat perception that it has an effect on an individual's coping behavior. Surprisingly, when users were asked what they would do if their SP had a security breach, none mentioned that they would stop using their WAT; however, they said this might affect their future WAT purchases [134].

Individual differences play an important role in users' privacy awareness, concerns, attitudes, and behavior. For example, older users tend to be more relaxed with data sharing [214] and give more value to their WAT data [246]. Women tend to share more data than men do [214]. The findings of studies about the differences between users from different regions are rather inconsistent. Ilhan and Fietkiewicz [109] find significant differences, regarding their level of concern and awareness, between users from the United States and those from Germany. However, the same group of researchers did not observe any differences between users from the United States and Europe [74]. Earlier studies categorized users into different classes:

— Non-sensitive and Sensitive users [142];
— Unconcerned, Somewhat Concerned, and Highly Concerned users [147];
— Data Protectors (i.e., those concerned with privacy), Benefit Maximizers (i.e., those concerned with utility), and Fact Enthusiasts (i.e., those most concerned with motivational design) [35]; and
— Users, Former Users, and Non-users [74].

The last item helps us understand individuals' reasons for using technology or abandoning it and if they would contemplate using such technology in the future. Previous studies [60, 74] show that *non*-users of WATs are more concerned than users about the collection of WAT data. Surprisingly, former users are less concerned about privacy than actual users [74]. In contrast, Bélanger et al. [25] do not find any significant difference between the privacy concerns of users and non-users.

4.2 Privacy Policies, Regulations, and Ethics

4.2.1 Privacy Policy. As a means of communication between SPs and users, privacy policies are used to inform users about the data collection and usage practices and to obtain their permission. However, their usability and compliance with users' privacy needs and data-protection regulations is still under debate. Many studies have reviewed WAT-related privacy policies and identified two main issues:

— *A lack of (legal) accountability*: Braghin et al. [31] argue that privacy policies are of "dubious validity." Users report a lack of accountability in cases of privacy breaches [4]. Paul and Irvine [182] found many statements that have the potential to violate user privacy in the privacy policy content of four market leaders in 2012.[10] Several studies present heuristic frameworks for evaluating privacy policies. Katurura and Cilliers [118] showed that both Fitbit and Apple did not provide minimal protection for choice or consent: before they collect data, these companies ask for consent; however, after the collection, the users were not permitted to enforce how their data is used. Hutton et al. [108] compared the privacy policies of self-tracking apps in different domains and show that apps related to WATs generally met fewer heuristics, compared with apps related to other types of tracking (e.g., time management, cost management). Becker et al. [24] showed that the type of statements used in privacy policies can influence users' decisions about disclosing their health information (e.g., policies framed positively).

— *Usability problem*: Privacy policies are lengthy, complex, and annoyingly profuse, thus users often do not read them to avoid cognitive load. Furthermore, users perceive their acceptance as a binary choice (i.e., forced-choice dilemma): a necessary condition to use the device [185].

Researchers propose several *solutions*. Gluck et al. [85] show that shortening the privacy policies to some extent can be an effective way to increase user awareness. Guo et al. [96] propose a visualization tool, called *Poli-see*, for helping users understand WAT privacy policies. Drozd and Kirrane [58] present CURE, a consent-collection system that obtains users' partial consent in a more usable fashion and that provides the users with a better explanation of the consent they have given. Murmann et al. [168] study the adoption of privacy notifications (e.g., notifying users when their data is stored on a cloud or when it is transferred to another country) and show that most of their respondents perceived notifications as useful. Masuch et al. [158] show that confidence-building mechanisms (i.e., statements by SPs about how data will be treated securely) resulted in an increase of the users' expectations about the security of the service. However, users observed a large discrepancy between expectation and reality. This negatively influenced their satisfaction and intentions to continue using their WATs. Thuraisingham et al. [237] propose a (hypothetical) privacy-aware data management framework to enable users to manage the collection, storage, sharing, and analysis of their own data.

4.2.2 Protective Laws for Users. Most of the works about existing regulations, laws, and policies studied regulations in the United States and Europe. In the United States, there are several relevant regulations. However, none are effective [33, 34, 128, 135]. More specifically, users are not affected by federal legislation, such as HIPAA (the Health Insurance Portability and Accountability Act) or HITECH (the Health Information Technology for Economic and Clinical Health) Act, as they are not expansive enough to address WAT data. WAT data is not counted as protected health information because SPs are not covered entities, unlike hospitals or clinics [157]. In the case of WAT data being stored by a covered entity, HIPAA is applicable only for data processing and disclosure and not for data collection [75]. Similarly, the FDA (the U.S. Food and Drug Administration) classifies WATs as low-risk wellness products [128, 239]. As a result, WAT data is not protected by the FD&C (the U.S. Federal Food, Drug, and Cosmetic) Act [33, 34]. The Privacy Act of 1974 is another relevant law that regulates the collection, usage, and disclosure of PII. But the definition of PII in this act is rather limited [33], as it includes only information such as names, e-mail addresses, and social security numbers. Similarly, WAT data is not protected by the ECPA (the Electronic Communication Privacy Act) [33, 34], as the ECPA does not include devices that use radio frequency identification.

Researchers advocate for new WAT regulations, recommend including WAT data in existing frameworks (e.g., the Privacy Act of 1974 [33]) and the expansion of terminologies such as "covered

[10] Note that these findings are from almost a decade ago. Some of these products are no longer sold, and some policies might have been amended.

entities" and "third parties" to include SPs [128]. Brinson and Rutherford [33] also developed a portal to help users and data brokers interact and determine the use of their data.

Several studies on legislation in other countries have been conducted. Daly [50] discusses that the most important source of WAT regulation in Australia is the TGA (the Therapeutic Goods Administration). However, the TGA's regulations can be easily avoided if WAT manufacturers do not intend for their WATs to be classified as medical devices (as defined by the TGA). Similarly, Katurura and Cilliers [118] showed that the POPIA (the Protection of Personal Information Act) in South Africa cannot force foreign manufacturers to comply. Compared to other countries, in the **European Union (EU)**, the GDPR (General Data Protection Regulation) provides better protection for users [75, 135, 156]. The GDPR has several advantages. First, it forbids processing personal data, except in far-reaching conditions (i.e., if they are anonymized) [135]. Second, it forbids the processing of data concerning health, unless the patient has explicitly consented.[11] This affects the collection of health-related data, such as heart rate data. Third, it is an enforceable law and is applicable to foreign manufacturers who export their products to the EU [75, 156].[12] This is further supported by the Privacy Shield 2.0.[13] Fourth, it permits the use of *anonymized* data for science and research purposes and for the sake of technological development and demonstration [135].

4.2.3 Use of WAT Data in Investigations. WAT data can be used as evidence in *forensic* investigations regarding, for example, suspicious deaths, airplane crashes, malpractice [241], and even detecting police brutality [241], especially in cases of racial injustice [166]. WAT data integrity can also be assessed—for example, insurance companies can check whether a reported activity was created artificially [225]. Several studies present software tools for forensic science [101, 225] and guidelines for investigators [5, 101]. Other studies [5, 101, 263] show the forensic soundness of their tools or guidelines by using existing WATs. Only one study fails to recover information, after a forensic analysis [160]. It used a real-life scenario instructing a participant (with a Fitbit) to walk to a specific location and hit the ground several times, then to return to their point of departure. Future studies should use similar real-life scenarios to validate the reliability of forensic methods. Courts and forensic investigators can face several *challenges* that reduce the objectivity of judicial decisions [128, 241]:

- *WAT accuracy*: To ensure the accuracy of measured metrics, in particular, if a non-standard WAT was used.
- *Data integrity*: To ensure data integrity by confirming that the data were not changed after an incident and that the WAT was not worn by other individuals.
- *Data handling*: To handle massive amounts of data and still create precise statistical/inference models, even if part of the data is missing.
- *User privacy*: To maintain users' privacy during forensic investigations, particularly in interdependent privacy situations [107]. Hassenfeldt et al. [104] show that using web scraping and leaderboard information from Strava, they can access other users' information, regardless if their data is private or public. Kumari and Hook [128] argue that courts should try to obtain data from the users themselves or from their acquaintances. Accordingly, asking SPs to share data should not be the first option.

[11] Other exceptions include when the processing is necessary to protect the vital interests of the patient or of another person, to perform another contract for the patient, or to carry out a task of public interest or of other legitimate interests, except when such interests are overridden by the interests and personal data protection rights of the patient. For details, see Article 6 GDPR (https://gdpr-info.eu/art-6-gdpr/; accessed February 2024).

[12] Here, the product includes all equipment and covers mobile devices, applications, services, and wearable devices.

[13] EU-U.S. Privacy Shield framework (see https://www.privacyshield.gov; accessed February 2024).

4.2.4 Ethics. Several studies analyze the ethical implications of using WATs for users [150, 227, 239]. Lupton [150] uses the term *dataveillance* (i.e., digital surveillance of individuals) to explain how WAT use can lead to "function creep" (i.e., using data for purposes other than living a healthy and active lifestyle). Tuovinen and Smeaton [239] define the term *wearable intelligence* as the convenience and simplicity of using WATs. They discuss that, unlike in the context of a black box, users need to know that the information presented to them is an approximation generated by computational models and not absolutely accurate. In addition, they warn about a potential *power imbalance* between non-expert users and expert data analyst entities, as this imbalance can cause further privacy and trust issues. Steinberg [227] discusses the fairness of insurance companies that use WATs as incentive programs, where users can receive a discount on their premiums if they choose to share their data with insurers.

In addition to taking ethics into consideration for users, researchers should be mindful of *research ethics*. The collection of WAT data can serve in the development of ML models to infer users' states and propose proper interventions for them. It has become common practice to collect such datasets and to share them with the public to support open science. Publicly sharing such a large dataset has privacy risks for the data owners and ethical risks for designers (i.e., designing interventions based on biased datasets). Lee et al. [132] conduct a risk-benefit assessment with WAT data owners and show that financial compensation was the main incentive for data owners. Some data owners accept to provide even more data to receive even more money. Among those who refused the offer, some mentioned they would accept only if the compensation amount was higher. Less than half of the data owners thought they were subject to surveillance. Some also mentioned a lack of trust about how data would be handled by researchers. Given these vulnerabilities, it is important to protect WAT data owners after data collection. We recommend that, beyond routine practices, such as using informed consent and anonymization, researchers should consider data sharing with *restricted access*. Among the FAIR[14] open science repositories, Zenodo provides an option for restricted access,[15] where data can be stored privately on the platform, and researchers can share access to it only after certain agreements.[16]

4.3 'Health@Work' or Workplace Surveillance?

In the context of workplaces, existing studies show that employers have a vested interest in promoting the use of WATs for their employees [75, 123]. This creates a profitable business for WAT manufacturers, as they can sell more of their products (and additional services) to companies.[17] Companies intending to adopt WAT-based wellness programs follow either a *wellness model* or a *performance management model* [156]. Whereas the former is used to promote healthy lifestyle habits and to enhance the well-being of the employees, the latter aims to increase efficiency, productivity, and safety.[18] The concern with the first model is for employees' privacy, whereas the second is more serious, as data can be used to monitor and detect misconduct, and it can negatively affect employees' careers.

Most studies focus on the first model [43, 87, 88]. Many employees report perceiving wellness programs positively. They usually participate in such programs to improve their awareness of their activity levels, to become more physically active [43], or to socialize [87]. During the campaigns,

[14] https://www.go-fair.org/fair-principles/ (accessed February 2024).

[15] https://about.zenodo.org/policies/ (accessed February 2024).

[16] For example, a data recipient must agree to not make data public and not infer data owners' identities.

[17] https://healthsolutions.fitbit.com/corporatewellness/ (accessed February 2024).

[18] To read comprehensive surveys on the use of wearables for safety at work, see the work of Pasquale et al. [179] and Svertoka et al. [232].

employees can become concerned about the erosion of the boundary between their work and personal lives. However, they also tend to discuss their WAT data with colleagues (as an ice breaker for conversations during breaks). In the workplace, discussions about step counts or activities can increase social pressure, breach privacy boundaries, and hence raise tensions. Studies show that not all employees are happy to join such campaigns, and some decide to not join [43, 87].

Given the lack of evidence of the long-term benefits of wellness campaigns and the social distance created between participants and non-participants, Gorm and Shklovski [88] suggest reconsidering the notion of "success" in such campaigns. Marassi and Collins [156] discuss the privacy and autonomy concerns of wearing WATs in the workplace and express many reservations, especially about the employees' "right to bodily integrity," "life-work boundaries," and the "power imbalance" between employers and employees. In the United States, there is no legislation that protects employees' privacy [34].[19] In the EU, the GDPR does not permit employers to monitor their employees. To address these issues, previous studies recommend (i) clarifying the terms and implications of information disclosure to employees [34]; (ii) proposing new laws that limit data collection by employers [34]; and (iii) using a coaching-based approach, where employers use third-party services that provide health advice to their employees [156].

4.4 Privacy-Enhancing Technologies

Users, in general, are open to using PETs [269]. Therefore, designing useful solutions could be a promising approach to preserving users' privacy. As an addition to the work of Alqhatani and Lipford [8] that reviews existing PETs provided by known WAT brands, our work reviews the PETs proposed by the literature:[20]

- *Anonymization techniques*: Given the high dimension and sequential time-series nature of WAT data, anonymizing such datasets is challenging. Na et al. [169] showed that accelerometer data can be deanonymized with high accuracy. Multiple studies focus on methods for effectively anonymizing WAT data. Parameshwarappa et al. [178] used a multi-level clustering anonymization technique to prevent the re-identification of users. Gong et al. [86] proposed a theoretical framework for federated learning that preserves individuals' privacy and trains an ML model by using multiple WATs' data. Garbett et al. [80] designed 'ThinkActive': an activity-sharing platform for classrooms with the aim of enabling students to use pseudonymized avatars.
- *Limited sharing and data minimization*: Wang et al. [249] studied user preferences and sharing behavior related to partial-data release. Epstein et al. [63] investigated if fine-grained step-count sharing can help users preserve privacy while they share activities. Velykoivanenko et al. [242] assessed users' utility perceptions to inform future PET design. They also show that there is a high potential for implementing *data minimization* that can avoid certain privacy risks.
- *Pedagogical solutions*: Torre et al. [238] modeled the complexity of WATs and TPAs to compute the probabilities of inferring different information from WAT data. They show that users can protect their privacy by not sharing certain data. Aktypi et al. [4] designed a pedagogical tool that informs users of the risks they are exposed to when sharing certain WAT data (e.g., running route), together with other information (e.g., the information available their social media). Alvarez et al. [9] showed that watching a video about privacy and security

[19] For example, there was a case in California where an employee's claim that their employer violated their privacy by linking their Apple account to a work-related device was rejected by a court [39].
[20] PETs for usable and effective privacy policies [58, 96, 237] were already discussed in Section 4.2.1.

risks of collecting and sharing WAT data can significantly improve attitudes toward cybersecurity, whereas a text version of the information has no significant effect. Sanchez et al. [212] modeled the privacy preferences of users and developed a system for recommending personalized privacy settings to users.

- *Others*: Data integrity is critical for healthcare providers and insurance companies that are interested in users' WAT data. Du Toit [59] designed *PAUDIT*, a decentralized data architecture that enables users to store their WAT data in a personal online data store and permits healthcare providers to read data and audit the logs (i.e., changes made to the access control list). Ghazinour et al. [84] proposed an access-management tool that enhances users' decision making by enabling them to share their WAT data after considering four aspects: purpose (why), visibility (who), granularity (how), and retention (when).

5 JOINT ANALYSIS OF UTILITY AND PRIVACY

According to privacy calculus theory [17, 137], technology users always weigh the perceived benefits and (privacy) risks. Perceived utility and privacy concerns affect users' intentions to use their devices [137, 215]. Several studies [25, 27, 175, 267] found that users prefer to take a *utilitarian* approach and that the perceived benefits can outweigh their privacy concerns. They usually perceive a fairly positive effect from data sharing [7, 24]. However, some users (e.g., older adults [62]) do not make rational tradeoffs by ignoring or underestimating the risks [253]. Furthermore, some users often willingly share data, despite compromising their privacy, as they find the health and social benefits worth the risk [147]. They sacrifice privacy to receive immediate financial benefits, such as a reduction in insurance fees [185] or a higher wage [132]. Although users tend to express concerns when they carefully read previously agreed-to data collection policies, they would not change their usage behavior [49].

Although the utility–privacy tradeoff is often imbalanced toward the side of utility, users can still gain privacy if they can turn off a particular feature that they do not use. This is a privacy-by-design approach known as data minimization; it limits data collection and transfers to only that which is essential for a specific purpose. Similarly, using PETs can increase privacy, possibly at the expense of utility. Some PETs (e.g., privacy checkup reminders) have no effect on utility. To understand if users are willing to pay in terms of utility to protect their privacy, a few papers studied user attitudes or behaviors toward such strategies. For example, Velykoivanenko et al. [242] reveal a potential for storing heart rate and sleep data, only locally on users' primary connected devices and not on Fitbit's website. They also showed that data aggregation (i.e., having less granular data) was well received by the users. Similarly, Zufferey et al. [269] show that users are generally inclined to use PETs when exposed to the privacy risks related to the use of WAT TPAs. For example, the majority of their respondents reported that they would be (slightly to extremely) likely to use PETs such as reminders or data minimization techniques that reduce time or spatial granularity.

Finally, following the definition of privacy (a.k.a. contextual integrity) by Nissenbaum [170], earlier studies [25, 36, 159] show that users' utility–privacy tradeoff depends on *context*. Ebert et al. [60] show that WAT users are concerned about privacy marginally more than loyalty card users are. Lehto and Miikael [134] discuss that individuals consider their health data (collected by their doctors) as private/sensitive, unlike data collected from WATs. Furini et al. [77] show that when given a strong altruistic motivation (e.g., sharing data for contact tracing for COVID-19), users tend to agree to share their data. Similarly, research participants might be willing to share their data, as they consider it a donation and contribution to science [132]. Finally, Velykoivanenko et al. [242] argue that users' concerns about the inference of certain types of information (e.g., religion and sexual orientation) are heavily dependent on the social norms and conditions in their country of residence.

Table 4. All Articles about Bluetooth Security and WATs

Type of Attack	Das et al. [51] (2016)	Lotfy and Hale [146] (2016)	Goyal et al. [93] (2016)	Rahman et al. [192] (2016)	Zhang and Liang [265] (2017)	Fafoutis et al. [69] (2017)	Shim et al. [219] (2017)	Classen et al. [46] (2018)	Mendoza et al. [161] (2018)	Braghin et al. [31] (2018)	Celosia and Cunche [40] (2019)	Zuo et al. [270] (2019)	Becker et al. [21] (2019)	Hale et al. [100] (2019)	Wang et al. [248] (2020)	Gouda et al. [90] (2020)	Barman et al. [16] (2021)	Casagrande et al. [38] (2022)
Tracking	✓		✓	✓					✓	✓	✓	✓	✓					
Eavesdropping		✓			✓			✓	✓	✓		✓		✓	✓	✓		✓
Data Injection		✓		✓	✓			✓	✓	✓		✓		✓	✓	✓		✓
DoS			✓	✓	✓			✓						✓				
Traffic Analysis	✓					✓											✓	
Firmware Modif.							✓	✓										
Passive	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Active		✓	✓	✓	✓		✓	✓	✓	✓		✓		✓	✓	✓		✓

For each paper, we indicate the considered types of attacks.
"Active," as opposed to "Passive," relates to an attack where the adversary must interfere with the communication protocol.

6 WAT SECURITY

We first review the security vulnerabilities of WATs, including attacks on WATs' Bluetooth communications,[21] and various vulnerabilities related to companion apps, and discuss ways WAT data can be used to bypass security systems. Next, we review security countermeasures, including security protocols and threat assessments. Last, we review different WAT authentication methods for enhancing user security.

6.1 WAT–Phone Communication

A large amount of research has been conducted on WATs and Bluetooth security. Multiple attacks, privacy issues, and mitigation techniques were identified. Table 4 shows all of the studies related to Bluetooth and **Bluetooth Low Energy (BLE)** security and WATs. By analyzing these studies, we identified six main types of attacks:

- *Tracking*:[22] Several studies [31, 51, 93, 161] analyzed how WATs, from multiple vendors, communicate with their companion apps (generally installed on a smartphone). They show that all of the tested WATs use permanent BLE addresses, which makes them vulnerable to tracking attacks. Although these previous studies state that using address randomization should mitigate the tracking attack, recent studies [40, 270] have shown how generic attribute (GATT) profiles[23] can be used to build unique fingerprints. Becker et al. [21] developed a method to track BLE devices by using features extracted from the payload of advertising messages.

[21] Note that the multiple attacks we review are not necessarily specific to WAT devices (e.g., attacks on Bluetooth or HTTP communications).
[22] Tracking is about being able to locate or identify the presence of a specific device.
[23] GATT profiles are available without any authentication and contain basic information about features and services.

- *Eavesdropping and injection attacks*:[24] Except for one of them, all analyzed studies describing eavesdropping attacks are also about data-injection attacks. Both types of attacks can be performed using similar techniques, such as a **Man-in-the-Middle (MitM)** attack. Several studies [31, 146, 265, 270] show that multiple WATs use unencrypted communication, either while already paired or during the pairing process with a smartphone. They even permit pairing without authentication. Therefore, an attacker can retrieve information about the devices. Rahman et al. [192] reverse-engineered two WATs (Fitbit and Garmin) and built a framework that can perform various attacks, such as injecting data into the devices. Other studies [46, 90, 248] performed attacks that force a device to be paired with a fake companion app that grants access to all transmitted data before redirecting it; the fake companion app was also able to inject data and commands. Mendoza et al. [161] analyzed a Fitbit WAT and show that its communication with a paired smartphone does not follow the BLE security specifications and that the device accepts connections from unknown smartphones. Casagrande et al. [38] reverse-engineered Xiaomi devices and firmware; they show that a large amount of information (including the pairing keys) was not properly encrypted during the communication, thus enabling an attacker to not only eavesdrop on communication but to also alter data.
- *Denial of service*:[25] Goyal et al. [93] performed a **Denial of Service (DoS)** attack on a Fitbit Charge by spamming it with requests that prevent it from communicating with the companion app on a paired smartphone. Rahman et al. [192] developed two different DoS attacks against Fitbit and Garmin devices. They show that it is possible to quickly drain the WATs' batteries by spamming them with BLE requests. Zhang and Liang [265] also show that attackers can conduct DoS by continuously sending fake commands. Classen et al. [46] demonstrate that DoS attacks can be performed on Fitbit WATs by injecting commands to enable the alarm clock or disable the WAT's functionalities, such as pairing and data synchronization.
- *Traffic analysis*:[26] Das et al. [51] analyzed BLE traffic patterns and found that it is possible to identify individual users, with high accuracy. Fafoutis et al. [69] used BLE to analyze the correlation between activity levels and the received signal strength, in the context of a WAT communicating with a smart home system. The results show that the received signal strength and the unencrypted data are strongly correlated. Finally, Barman et al. [16] reported that a large amount of information can be inferred from encrypted Bluetooth traffic between a WAT and its paired smartphone, such as the type of device, actions, and the type of data.
- *Firmware modification*:[27] Shim et al. [219] analyzed a WAT and its companion app's APK. Using reverse engineering, they analyzed the BLE communication when the companion app attempts a firmware update of the WAT. This enabled them to create a fake gateway for injecting malicious firmware updates. Similarly, Classen et al. [46] reverse-engineered Fitbit's firmware to study how to modify it to build custom firmware. They show that attackers can use unencrypted BLE communication to flash modified firmware onto Fitbit devices. As explained earlier, most WATs use unencrypted communication.

[24] An eavesdropping attack consists of intercepting data communication between two devices, whereas an injection attack consists of sending additional (i.e., fake) data to a specific device.

[25] DoS attacks occur when access to a service is temporarily blocked by overloading the host machine or network with requests.

[26] Traffic analysis consists of trying to bypass encryption by using metadata and signal treatment to infer some characteristics of the unencrypted message.

[27] Firmware modification is about inserting malicious code into a device's firmware update.

Hale et al. [100] developed an open source platform that aims to be used by researchers to facilitate wearable security investigations. The platform could be used to collect data, conduct attacks, and identify security vulnerabilities. They used their platform to analyze BLE communications of multiple WATs and observed that all of them use encryption protocols to communicate with their companion apps.

In conclusion, WATs tend to not use any protection mechanisms, such as basic cryptographic schemes [100]; in addition, they send unencrypted traffic, mainly for optimization reasons (e.g., to save battery life). As a result, the public attributes of the transmitted packets can be used to track WATs. Not using encrypted communication can lead to eavesdropping, data injection, and/or firmware modification. MitM attacks can be performed to bypass (basic) encryption mechanisms. An attacker can inject fake commands to conduct DoS attacks. Traffic analysis can disclose sensitive information, even if the communication between a WAT and its paired smartphone is encrypted. Finally, whereas some studies proposed mitigation techniques, only a few of them actually evaluated these techniques.

6.2 Phone–Server Communication and Data Storage

Several studies analyzed the security of WAT companion apps. Goyal et al. [93] analyzed the code of the companion apps, how the data is stored on the paired smartphone, the apps' privacy policies, and the communication between the app and the SPs' servers for two types for two WAT models. They showed that for both WATs, the data stored on the smartphone is not encrypted and some of it is even shared with third parties. Rahman et al. [192] analyzed the HTTP communication between Fitbit and Garmin devices and their servers. They showed that the data was not encrypted, including the user's credentials for Fitbit. Fereidooni et al. [73] considered users as potential adversaries. Users might want to send fake data to their SP's cloud for financial gain.[28] They analyzed multiple WATs and used MitM attacks to inject fake data into their servers. By reverse engineering the companion apps, they showed that multiple companion apps do not encrypt the data stored on the smartphone, which makes it easily readable and writable.

To inject fake data, Fereidooni et al. [73] also conducted MitM attacks between the companion app and the SP. They performed a new attack directly on the WAT by reverse engineering the hardware system and directly accessing the device's memory to inject fake data [72]. After synchronization, the fake data was correctly encrypted and registered by the companion app.

Mendoza et al. [161] analyzed how the Fitbit companion app communicates with Fitbit's servers by sniffing HTTP/HTTPS communication and how TPAs can access data using Fitbit's API. They showed that authentication credentials are sent unencrypted and that the OAuth 2.0 protocol[29] is not correctly implemented. This creates vulnerabilities that an attacker can use to gain access to or modify the data. Classen et al. [46] reverse-engineered the Fitbit companion app to study how to modify it. Modifying the app could enable attackers to associate it with another account in order to download a user's data. Finally, Kazlouski et al. [119] analyzed the communication between two well-known (yet anonymized) WAT companion apps and servers. They collected ground truth by using a MitM setup and sniffed the encrypted packets by using Wireshark. Then they computed correlations of the size and frequency of the packets with the activities, heart rate, and step count. They show that activities and metadata of encrypted packets are strongly correlated and that it is possible to use metadata to identify the occurrence and duration of several activities and even to estimate other information (e.g., estimating the heart rate). In conclusion, multiple devices do not

[28] This applies to cases where users participate in financially incentivized data-sharing schemes, such as corporate wellness programs.
[29] OAuth 2.0 is used to enable TPAs to access some of the data.

implement adequately secure phone storage and communication with the SP's servers, which can lead to serious threats, such as eavesdropping and/or data injection.

6.3 Side-Channel Attacks

Side-channel attacks are a type of security attack that are conducted based on extra available information, instead of using vulnerabilities of security protocols. As the main purpose of WATs is to track users' movements, it is possible to use the sensor data to infer sensitive information, such as the words a user writes, their typing on a keyboard, or even their biometrics.

Maiti et al. [153] studied how WAT sensor data can be used to recognize typing patterns on a computer keyboard. Such attacks can be used by adversaries to collect passwords for bypassing authentication systems. Similarly, Maiti et al. [155] used smartwatch sensor data to infer which keys are typed on a 10-digit keypad and a QWERTY keypad on a smartphone. They reached an accuracy of 74% for the 10-digit keys and had a mean accuracy of 30% for the QWERTY keypad. Sabra et al. [207] and Wang et al. [247] showed how similar attacks can be conducted to infer ATM PIN codes. The former obtains an accuracy of 80% for 6-digit PIN codes; this increases to 93% with five attempts. Lu et al. [148] aimed to infer PIN codes and Android pattern lock patterns. They found that it is possible to infer the Android pattern lock pattern two-thirds of the time, within the first 20 guesses. Maiti et al. [154] studied the inference of rotary combination lock passcodes and showed that WAT sensor data (especially gyroscope data) can be used to greatly increase the likelihood of inferring the lock combination. Eberz et al. [61] studied impersonation attacks. They showed that WAT sensor data can be used to mimic an individual's biometrics (e.g., gait), which would enable bypassing biometrics-based authentication systems.

In general, we can affirm that using WAT sensor data to bypass a security system is a potential threat that should be considered by vendors. Several mitigation techniques are proposed. For example, WATs could deactivate sensors when they detect real-time activities such as typing [153]. Alternatively, WATs could add fine-grained noise to sensor data, in such a way that activities, such as walking or swimming, are still recognized but fine hand movements, such as typing, are not recognized [247]. Or, users can simply remove their devices when they type.

6.4 Security Protocols, Countermeasures, and Threat Assessment

Although a large number of studies related to security are about weaknesses, attacks, and privacy leaks, some of them are about *new protocols* and *tools* that can help preserve the security of systems. To protect against different attacks, Rahman et al. [192] propose an encryption protocol based on symmetric keys. They show that their solution has little effect on the device's performance. Using a system of tagged packets, Skalka et al. [226] develop a framework to manage and filter private data at the edge-router level. Yan et al. [260] propose an ML-based method that uses received signal strength indicators to detect spoofing attacks from peripheral devices (e.g., additional sensors worn on the foot) with high accuracy. Finally, Xin et al. [258] show that their new framework is effective at detecting when data is injected in WAT sensor data streams through specific data variations.

A few studies aimed to *identify* and *assess* the different types of *existing attacks*. To classify attacks, Mnjama et al. [164] developed a conceptual WAT threat assessment framework based on the CIA triad (i.e., confidentiality, integrity, availability) and on Microsoft STRIDE (i.e., spoofing, tempering, repudiation, information disclosure, denial of service, the elevation of privilege). They analyzed different phases of WAT data transmission and storage and the current health-wearable literature. Moganedi and Pottas [165] identified all known vulnerabilities affecting WATs and discussed these vulnerabilities with regard to their corresponding parts of the WAT ecosystem and the ways they are classified according to various existing standards. To classify the different currently known vulnerabilities, they identified five main components in the WAT ecosystem

Table 5. Summary of Authentication Methods Using WAT for Security Applications

Authors	Authentication Method	Results/Key Findings
Cola et al. [48] and Johnston and Weiss [114]	Gait as an authentication factor	Low error rates (2%–3%)
Vhaduri and Poellabauer [244]	Physiological and activity data from WATs	High accuracy in user recognition
Tehranipoor et al. [235]	Electrocardiogram (ECG) data	ECG-based keys can effectively identify users
Chen et al. [41]	Keypad simulation with biometrics	Effective and resilient authentication method
Li et al. [140]	Movement data from WATs and IoT device usage input	Robust authentication for IoT devices
Shen et al. [218]	Protocol based on handshaking patterns	Secure communication channel without transmitting encryption keys between two WATs
Shrestha and Saxena [224]	Wrist movements and web service usage-data comparison	Authentication for web service accounts
Sturgess et al. [229, 230]	NFC payments with smartwatches	Prevents unauthorized payments with smartwatches

(the WAT, Bluetooth, smartphone companion app, WiFi, and cloud storage) and six control families (access control, audit and accountability, identification and authentication, system and communication protection, system and information integrity, and PII processing and transparency).

6.5 WAT-Based Authentication for Security

WAT data can be used to enhance security systems by using the collected data to authenticate users, and by either substituting or complementing other credentials. Table 5 provides a concise summary of various authentication methods utilizing WATs for security-related applications.

Notably, gait-based authentication was found to exhibit low error rates [48, 114]. Vhaduri and Poellabauer [244] demonstrated high accuracy in user recognition by using physiological and activity data collected by WATs. Tehranipoor et al. [235] showed the effectiveness of ECG-based keys for user identification. Chen et al. [41] introduced a resilient authentication system that combines credentials and biometrics by using a virtual 12-key keypad on a user's fingers. Sturgess et al. [230] developed an authentication system for NFC payments with smartwatches. This system detects the intent to pay and then authenticates the user when they want to proceed with payment by using their smartwatch and an NFC terminal. This system prevents attackers from paying with stolen devices or from executing unwanted payments with unlocked devices worn by the user. However, in another study, the same authors showed that an attacker of approximately the same height as the user has a 20.6% higher likelihood of impersonating the user [229]. In summary, WATs are equipped with multiple sensors that enable them to be used for biometric authentication: the WAT's firmware could use the biometric data to ensure that the device is activated only when used by its rightful owner; third-party services could also use the collected biometric information for user authentication.

7 OPEN ISSUES AND RESEARCH AGENDA

In our survey, we provide comprehensive information about the utility, privacy, and security of WATs. We reveal several open issues. In this section, we review and categorize these open issues and then make recommendations regarding future research for researchers and opportunities for designers and policymakers.

Defining "WATs". One of the first findings from our survey is that there is no clear definition of WATs and that research on WATs is scattered across different overlapping categories (e.g., wearables, IoT). The lack of a clear definition leads to difficulty in identifying related literature, inconsistent research findings, and ineffective privacy regulations. A first step would be to properly define a "WAT" and to delimit research on the topic for more focused, consistent, and comparable research. This survey makes the first step in this direction.

Designing Privacy-Enhanced WATs. The literature shows that privacy risks are huge, diverse, and widespread in terms of the information that can be inferred and of the consequences. Part of these risks stem from the behaviors of the users; this is due to their lack of knowledge and/or awareness of the WAT ecosystem and the privacy risks. When users are not concerned about privacy, they tend to behave carelessly. In addition, as users often choose utility when considering the utility–privacy tradeoffs of WATs, PETs must be particularly effective and desirable for users. To achieve this goal, we believe that future research should focus on the following: designing PETs that use the specificities of WAT data (e.g., numerical time series, TPAs), as is done for location data [189], and on pedagogical solutions to increase users' understanding of WAT ecosystems. To do so, a user-centered approach should be taken (e.g., participatory design or co-design [120]). However, the following topics are sufficiently covered in the current research landscape: usage patterns; habits; the underlying reasons for adoption, adherence, and abandonment; and users' privacy concerns.

Improving Privacy for WAT Data. Another issue identified in this survey is related to the policies governing the collection of user data via WATs. SPs enact policies that provide them many opportunities to develop business intelligence and to offer additional services to users. However, this often comes at the expense of diminished privacy for the users whose data was collected. More importantly, informed consents are often presented through long, complex, and tedious-to-read legal text, which induces users to accept the terms without understanding their implications. A few studies propose alternative solutions (e.g., abstractions or visualizations) to improve privacy policy legibility, but unfortunately, none are yet used in practice. Future studies should further investigate this aspect. In addition, competent authorities should create regulations that would require SPs to use easy-to-understand privacy policies. A related issue is the lack of protective regulations for users. The main limitation of the current legislation is that WAT data are not classified as health information. Consequently, WAT SPs are not obliged to adhere to specific legislation, which could offer better protection for users' data (e.g., ECPA and HIPAA). We believe that legal scholars and policymakers should rework existing regulations to better protect WAT users.

Increasing WAT Security. Our survey shows that WATs are vulnerable. Many communications and storage protocols are vulnerable to attacks such as eavesdropping or side-channel attacks. There could be several factors contributing to these vulnerabilities: the low computational power of some WATs; the costs required to implement higher security standards; and/or the characteristics, which are typically not associated with identifiable information, of WAT data. Another interesting perspective to consider is that SPs are typically not considered adversaries in security research, as we noted in our survey. When they are considered adversaries, they are generally considered as honest but curious. This survey reveals that many types of inference are possible with WAT data and that SPs should be modeled as adversaries. Future research should therefore focus on raising WAT security standards and on studying business models and data management plans typically associated with WATs.

Studying Privacy Risks of WATs More Extensively. We also reviewed many studies on HAR and inference. Most of the HAR papers are functionality oriented, wherein they mainly highlight HAR benefits and focus on achieving high performance. Most privacy-oriented inference papers do not consider activities or specific personal information (e.g., health), as most of them study the inference of data, such as passwords or other types of information that could be used for authentication.

We believe that future research should investigate privacy risks more systematically by finding inspiration from inference studies published on location and smartphone data (e.g., religion, political views, or consumption habits), as done recently by Zufferey et al. [268].

Conducting Meta-Analyses and Replication Studies. We identified studies of WATs' utility, privacy, and security that reported heterogeneous and sometimes opposite findings. Meta-analyses could be useful for comparing these diverse and sometimes conflicting findings. Similarly, studies comparing users vs. non-users, as well as some cross-cultural studies, have reported inconsistent findings. This underlines the need for replication studies in WAT research. To enable replication (and reproducibility), researchers should follow transparency and openness practices (e.g., see the work of Niksirat et al. [210] for guidelines on research transparency and openness).

8 CONCLUSION

In this survey paper, we meticulously reviewed 236 peer-reviewed published papers, with a primary focus on WATs' utility, privacy, and security. In our survey, we delved into diverse aspects of WATs, highlighting their associated benefits while addressing the associated risks. This work showed that WATs are particularly vulnerable to multiple types of attacks. For instance, the data they collect can be used to infer sensitive personal information. After presenting the current state of research, we provided a discussion highlighting multiple opportunities for research. This constitutes an essential step in future research into the utility, privacy, and security of WATs.

ACKNOWLEDGMENTS

We thank Holly Cogliati for proofreading this article.

REFERENCES

[1] A. Abedin, M. Ehsanpour, Q. Shi, H. Rezatofighi, and D. C. Ranasinghe. 2021. Attend and discriminate: Beyond the state-of-the-art for human activity recognition using wearable sensors. *IMWUT* 5, 1 (2021), 1–22. https://doi.org/10.1145/3448083

[2] F. Adebesin and R. Mwalugha. 2020. The mediating role of organizational reputation and trust in the intention to use wearable health devices: Cross-country study. *JMIR mHealth and uHealth* 8, 6 (2020), e16721. https://doi.org/10.2196/16721

[3] D. A. Adler, V. W.-S. Tseng, G. Qi, J. Scarpa, S. Sen, and T. Choudhury. 2021. Identifying mobile sensing indicators of stress-resilience. *IMWUT* 5, 2 (2021), 1–32. https://doi.org/10.1145/3463528

[4] A. Aktypi, J. R. Nurse, and M. Goldsmith. 2017. Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the Conference on Multimedia Privacy and Security (MPS '17)*. ACM, 1–11. https://doi.org/10.1145/3137616.3137617

[5] A. Almogbil, A. Alghofaili, C. Deane, T. Leschke, A. Almogbil, and A. Alghofaili. 2020. Digital forensic analysis of Fitbit wearable technology: An investigator's guide. In *Proceedings of the IEEE International Conference on Cyber Security and Cloud Computing (CSCloud '20)International Conference on Edge Computing and Scalable Cloud (EdgeCom '20)*. IEEE, 44–49. https://doi.org/10.1109/CSCloud-EdgeCom49738.2020.00017

[6] D. Alqahtani, C. Jay, and M. Vigo. 2020. The role of uncertainty as a facilitator to reflection in self-tracking. In *Proceedings of the ACM Designing Interactive Systems Conference (DIS '20)*. ACM, 1807–1818. https://doi.org/10.1145/3357236.3395448

[7] A. Alqhatani and H. R. Lipford. 2019. "There is nothing that I need to keep secret": Sharing practices and concerns of wearable fitness data. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '19)*. 421–434. https://www.usenix.org/conference/soups2019/presentation/alqhatani

[8] A. Alqhatani and H. R. Lipford. 2021. Exploring the design space of sharing and privacy mechanisms in wearable fitness platforms. In *Workshop on Usable Security and Privacy (USEC '21)*, Vol. 7. Internet Society, 9. https://www.ndss-symposium.org/ndss-paper/auto-draft-178/

[9] S. L. Alvarez, S. L. Baller, and A. Walton. 2021. Who owns your health data? Two interventions addressing data of wearable health devices among young adults and future health clinicians. *Journal of Consumer Health on the Internet* 25, 1 (2021), 35–49. https://doi.org/10.1080/15398285.2020.1852386

[10] F. Amini, K. Hasan, A. Bunt, and P. Irani. 2017. Data representations for in-situ exploration of health and fitness data. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '17)*. ACM, 163–172. https://doi.org/10.1145/3154862.3154879

[11] C. Amma, M. Georgi, and T. Schultz. 2012. Airwriting: Hands-free mobile text input by spotting and continuous recognition of 3D-space handwriting with inertial sensors. In *Proceedings of the 2012 16th International Symposium on Wearable Computers*. IEEE, 52–59. https://doi.org/10.1109/ISWC.2012.21

[12] L. Ardüser, P. Bissig, P. Brandes, and R. Wattenhofer. 2016. Recognizing text using motion data from a smartwatch. In *Proceedings of Pervasive Computing and Communication Workshops (PerCom Workshops '16)*. IEEE, 1–6. https://doi.org/10.1109/PERCOMW.2016.7457172

[13] E. M. Aromataris and Z. Munn. 2020. JBI Manual for Evidence Synthesis. Retrieved February 18, 2024 from https://jbi-global-wiki.refined.site/space/MANUAL

[14] C. Attig and T. Franke. 2020. Abandonment of personal quantification: A review and empirical study investigating reasons for wearable activity tracking attrition. *Computers in Human Behavior* 102 (2020), 223–237. https://doi.org/10.1016/j.chb.2019.08.025

[15] S. Bae, A. K. Dey, and C. A. Low. 2016. Using passively collected sedentary behavior to predict hospital readmission. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '16)*. ACM, 616–621. https://doi.org/10.1145/2971648.2971750

[16] L. Barman, A. Dumur, A. Pyrgelis, and J.-P. Hubaux. 2021. Every byte matters: Traffic analysis of Bluetooth wearable devices. *IMWUT* 5, 2 (2021), 1–45. https://doi.org/10.1145/3463512

[17] S. B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11 (2006). https://doi.org/10.5210/fm.v11i9.1394

[18] K. Baskaran and S. K. Mathew. 2020. Danger vs fear: An empirical study on wearable users' privacy coping. In *Proceedings of the Computers and People Research Conference (SIGMIS-CPR '20)*. ACM, 123–132. https://doi.org/10.1145/3378539.3393856

[19] K. Baskaran, V. Sugumaran, and S. K. Mathew. 2020. Are you coping or copping out? Wearable users' information privacy perspective. *AMCIS 2020 Proceedings* 8 (2020), 11.

[20] K. Baskaran, V. Sugumaran, and S. K. Mathew. 2021. What do I do? Uncovering fitness tracker users' privacy coping strategy. *AMCIS 2021 Proceedings* 5 (2021), 6. https://aisel.aisnet.org/amcis2021/info_security/info_security/5

[21] J. K. Becker, D. Li, and D. Starobinski. 2019. Tracking anonymized Bluetooth devices. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 50–65. https://doi.org/10.2478/popets-2019-0036

[22] M. Becker. 2018. Understanding users' health information privacy concerns for health wearables. In *Proceedings of the Hawaii International Conference on System Sciences*. 3261–3270. https://doi.org/10.24251/HICSS.2018.413

[23] M. Becker, A. Kolbeck, C. Matt, and T. Hess. 2017. Understanding the continuous use of fitness trackers: A thematic analysis. *PACIS 2017 Proceedings* 40 (2017), 12. https://aisel.aisnet.org/pacis2017/40

[24] M. Becker, C. Matt, and T. Hess. 2020. It's not just about the product: How persuasive communication affects the disclosure of personal health information. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 51, 1 (2020), 37–50. https://doi.org/10.1145/3380799.3380804

[25] F. Bélanger, R. E. Crossler, and J. Correia. 2021. Privacy maintenance in self-digitization: The effect of information disclosure on continuance intentions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 52, 2 (2021), 7–24. https://doi.org/10.1145/3462766.3462769

[26] R. Benbunan-Fich. 2020. User satisfaction with wearables. *AIS Transactions on Human-Computer Interaction* 12, 1 (2020), 1–27. https://doi.org/10.17705/1thci.00126

[27] K. S. Bhat and N. Kumar. 2020. Sociocultural dimensions of tracking health and taking care. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), Article 129, 24 pages. https://doi.org/10.1145/3415200

[28] J.-I. Biel, N. Martin, D. Labbe, and D. Gatica-Perez. 2018. Bites'n'Bits: Inferring eating behavior from contextual mobile data. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (2018), Article 125, 33 pages. https://doi.org/10.1145/3161161

[29] A. Boldi, A. Silacci, M.-O. Boldi, M. Cherubini, M. Caon, N. Zufferey, K. Huguenin, and A. Rapp. 2024. Exploring the impact of commercial wearable activity trackers on body awareness and body representations: A mixed-methods study on self-tracking. *Computers in Human Behavior* 151 (2024), 108036. https://doi.org/10.1016/j.chb.2023.108036

[30] S. Boysen, B. Hewitt, D. Gibbs, and A. McLeod. 2019. Refining the threat calculus of technology threat avoidance theory. *Communications of the Association for Information Systems* 45, 1 (2019), 95–115. https://doi.org/10.17705/1CAIS.04505

[31] C. Braghin, S. Cimato, and A. D. Libera. 2018. Are mHealth apps secure? A case study. In *Proceedings of the IEEE Annual Computer Software and Applications Conference (COMPSAC '18)*, Vol. 02. IEEE, 335–340. https://doi.org/10.1109/COMPSAC.2018.10253

[32] N. H. Brinson, M. S. Eastin, and L. F. Bright. 2019. Advertising in a quantified world: A proposed model of consumer trust, attitude toward personalized advertising and outcome expectancies. *Journal of Current Issues & Research in Advertising* 40, 1 (2019), 54–72. https://doi.org/10.1080/10641734.2018.1503108

[33] N. H. Brinson and D. N. Rutherford. 2020. Privacy and the quantified self: A review of U.S. health information policy limitations related to wearable technologies. *Journal of Consumer Affairs* 54, 4 (2020), 1355–1374. https://doi.org/10.1111/joca.12320

[34] E. A. Brown. 2016. The Fitbit fault line: Two proposals to protect health and fitness data at work. *Yale Journal of Health Policy, Law and Ethics* 16, 1 (2016), 1–50. https://heinonline.org/HOL/P?h=hein.journals/yjhple16&i=7

[35] L. Burbach, C. Lidynia, P. Brauner, and M. Ziefle. 2019. Data protectors, benefit maximizers, or facts enthusiasts: Identifying user profiles for life-logging technologies. *Computers in Human Behavior* 99 (2019), 9–21. https://doi.org/10.1016/j.chb.2019.05.004

[36] L. Calloway, H. Hadan, S. Gopavaram, S. Mare, and L. J. Camp. 2020. Privacy in crisis: Participants' privacy preferences for health and marketing data during a pandemic. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES '20)*. ACM, 181–189. https://doi.org/10.1145/3411497.3420223

[37] Y. Cao, F. Li, H. Chen, X. liu, L. Zhang, and Y. Wang. 2022. Guard your heart silently: Continuous electrocardiogram waveform monitoring with wrist-worn motion sensor. *IMWUT* 6, 3 (2022), 1–29. https://doi.org/10.1145/3550307

[38] M. Casagrande, E. Losiouk, M. Conti, M. Payer, and D. Antonioli. 2022. BreakMi: Reversing, exploiting and fixing Xiaomi fitness tracking ecosystem. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022, 3 (2022), 330–366. https://doi.org/10.46586/tches.v2022.i3.330-366

[39] Casetext. 2014. Sunbelt Rentals, Inc., Plaintiff, v. Santiago Victor, Defendant. Retrieved February 18, 2024 from https://casetext.com/case/sunbelt-rentals-inc-v-victor

[40] G. Celosia and M. Cunche. 2019. Fingerprinting Bluetooth-Low-Energy devices based on the generic attribute profile. In *Proceedings of the International ACM Workshop on Security and Privacy for the Internet (IoT S&P '19)*. ACM, 24–31. https://doi.org/10.1145/3338507.3358617

[41] W. Chen, L. Chen, Y. Huang, X. Zhang, L. Wang, R. Ruby, and K. Wu. 2019. Taprint: Secure text input for commodity smart wristbands. In *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom '19)*. ACM, 1–16. https://doi.org/10.1145/3300061.3300124

[42] E. K. Choe, B. Lee, H. Zhu, N. H. Riche, and D. Baur. 2017. Understanding self-reflection: How people reflect on personal data through visual data exploration. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '17)*. ACM, 173–182. https://doi.org/10.1145/3154862.3154881

[43] C.-F. Chung, N. Gorm, I. A. Shklovski, and S. Munson. 2017. Finding the right fit: Understanding health tracking in workplace wellness programs. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 4875–4886. https://doi.org/10.1145/3025453.3025510

[44] M. Cifor and P. Garcia. 2020. Gendered by design: A duoethnographic study of personal fitness tracking systems. *ACM Transactions on Social Computing* 2, 4 (2020), Article 15, 22 pages. https://doi.org/10.1145/3364685

[45] L. Cilliers. 2020. Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal* 49, 2-3 (2020), 150–156. https://doi.org/10.1177/1833358319851684

[46] J. Classen, D. Wegemer, P. Patras, T. Spink, and M. Hollick. 2018. Anatomy of a vulnerable fitness tracking system: Dissecting the Fitbit cloud, app, and firmware. *IMWUT* 2, 1 (2018), Article 5, 24 pages. https://doi.org/10.1145/3191737

[47] J. Clawson, J. A. Pater, A. D. Miller, E. D. Mynatt, and L. Mamykina. 2015. No longer wearing: Investigating the abandonment of personal health-tracking technologies on Craigslist. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 647–658. https://doi.org/10.1145/2750858.2807554

[48] G. Cola, M. Avvenuti, F. Musso, and A. Vecchio. 2016. Gait-based authentication using a wrist-worn device. In *Proceedings of the International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services (MOBIQUITOUS '16)*. ACM, 208–217. https://doi.org/10.1145/2994374.2994393

[49] P. Dahlstrøm, E. Fauchald, B. Fimreite, and M. Lillebo. 2020. Users knowledge and attitudes towards data collection in activity trackers. *EReMCIS 2020 Proceedings* 2020 (2020), 4.

[50] A. Daly. 2015. *The Law and Ethics of 'Self-Quantified' Health Information: An Australian Perspective*. SSRN Scholarly Paper ID 2559068. Social Science Research Network. https://papers.ssrn.com/abstract=2559068

[51] A. K. Das, P. H. Pathak, C.-N. Chuah, and P. Mohapatra. 2016. Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. In *Proceedings of the International Workshop on Mobile Computing Systems and Applications (HotMobile '16)*. ACM, 99–104. https://doi.org/10.1145/2873587.2873594

[52] P. Datta, A. S. Namin, and M. Chatterjee. 2018. A survey of privacy concerns in wearable devices. In *Proceedings of the 2018 IEEE International Conference on Big Data (Big Data '18)*. IEEE, 4549–4553. https://doi.org/10.1109/BigData.2018.8622110

[53] I. L. de Faria and V. Vieira. 2018. A comparative study on fitness activity recognition. In *Proceedings of the Brazilian Symposium on Multimedia and the Web (WebMedia '18)*. ACM, 327–330. https://doi.org/10.1145/3243082.3267452

[54] P. P. Dhawale and R. J. Wellington. 2015. Identifying the characteristics of usability that encourage prolonged use of an activity monitor. In *Proceedings of the New Zealand Conference on Human Computer Interaction (HCI '15)*. ACM, 39–42. https://doi.org/10.1145/2808047.2808056

[55] M. Dietrich and K. van Laerhoven. 2015. A typology of wearable activity recognition and interaction. In *Proceedings of the International Workshop on Sensor Based Activity Recognition and Interaction*. ACM, 1–8. https://doi.org/10.1145/2790044.2790048

[56] O. D'Mello, M. Gelin, F. B. Khelil, R. E. Surek, and H. Chi. 2018. Wearable IoT security and privacy: A review from technology and policy perspective. In *Future Network Systems and Security*, Robin Doss, Selwyn Piramuthu, and Wei Zhou (Eds.). Communications in Computer and Information Science. Springer International Publishing, 162–177. https://doi.org/10.1007/978-3-319-94421-0_13

[57] N. Dreher, E. K. Hadeler, S. J. Hartman, E. C. Wong, I. Acerbi, H. S. Rugo, M. C. Majure, A. J. Chien, L. J. Esserman, and M. E. Melisko. 2019. Fitbit usage in patients with breast cancer undergoing chemotherapy. *Clinical Breast Cancer* 19, 6 (2019), 443–449.e1. https://doi.org/10.1016/j.clbc.2019.05.005

[58] O. Drozd and S. Kirrane. 2020. Privacy CURE: Consent comprehension made easy. In *ICT Systems Security and Privacy Protection*, Marko Hölbl, Kai Rannenberg, and Tatjana Welzer (Eds.). IFIP Advances in Information and Communication Technology. Springer International Publishing, 124–139. https://doi.org/10.1007/978-3-030-58201-2_9

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

[60] N. Ebert, K. A. Ackermann, and P. Heinrich. 2020. Does context in privacy communication really matter? A survey on consumer concerns and preferences. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, 1–11. https://doi.org/10.1145/3313831.3376575

[61] S. Eberz, G. Lovisotto, A. Patane, M. Kwiatkowska, V. Lenders, and I. Martinovic. 2018. When your fitness tracker betrays you: Quantifying the predictability of biometric features across contexts. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (S&P '18)*. IEEE, 889–905. https://doi.org/10.1109/SP.2018.00053

[62] H. Ehrari, F. Ulrich, and H. Andersen. 2020. Concerns and trade-offs in information technology acceptance: The balance between the requirement for privacy and the desire for safety. *Communications of the Association for Information Systems* 47, 1 (2020), 227–247. https://doi.org/10.17705/1CAIS.04711

[63] D. A. Epstein, A. Borning, and J. Fogarty. 2013. Fine-grained sharing of sensed physical activity: A value sensitive approach. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '13)*. ACM, 489–498. https://doi.org/10.1145/2493432.2493433

[64] D. A. Epstein, C. Caldeira, M. C. Figueiredo, X. Lu, L. M. Silva, L. Williams, J. H. Lee, Q. Li, S. Ahuja, Q. Chen, P. Dowlatyari, C. Hilby, S. Sultana, E. V. Eikey, and Y. Chen. 2020. Mapping and taking stock of the personal informatics literature. *IMWUT* 4, 4 (2020), Article 126, 38 pages. https://doi.org/10.1145/3432231

[65] D. A. Epstein, M. Caraway, C. Johnston, A. Ping, J. Fogarty, and S. A. Munson. 2016. Beyond abandonment to next steps: Understanding and designing for life after personal informatics tool use. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 1109–1113. https://doi.org/10.1145/2858036.2858045

[66] D. A. Epstein, J. H. Kang, L. R. Pina, J. Fogarty, and S. A. Munson. 2016. Reconsidering the device in the drawer: Lapses as a design opportunity in personal informatics. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '16)*. ACM, 829–840. https://doi.org/10.1145/2971648.2971656

[67] D. A. Epstein, A. Ping, J. Fogarty, and S. A. Munson. 2015. A lived informatics model of personal informatics. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 731–742. https://doi.org/10.1145/2750858.2804250

[68] K. R. Evenson, M. M. Goto, and R. 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 (2015), 159. https://doi.org/10.1186/s12966-015-0314-1

[69] X. Fafoutis, L. Marchegiani, G. Z. Papadopoulos, R. Piechocki, T. Tryfonas, and G. Oikonomou. 2017. Privacy leakage of physical activity levels in wireless embedded wearable systems. *IEEE Signal Processing Letters* 24, 2 (2017), 136–140. https://doi.org/10.1109/LSP.2016.2642300

[70] L. Faust, P. Jiménez-Pazmino, J. K. Holland, O. Lizardo, D. Hachen, and N. V. Chawla. 2019. What 30 days tells us about 3 years: Identifying early signs of user abandonment and non-adherence. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '19)*. ACM, 216–224. https://doi.org/10.1145/3329189.3329196

[71] A. Fedosov, J. Ojala, E. Niforatos, T. Olsson, and M. Langheinrich. 2016. Mobile first? Understanding device usage practices in novel content sharing services. In *Proceedings of the International Academic Mindtrek Conference (AcademicMindtrek '16)*. ACM, 198–207. https://doi.org/10.1145/2994310.2994317

[72] H. Fereidooni, J. Classen, T. Spink, P. Patras, M. Miettinen, A.-R. Sadeghi, M. Hollick, and M. Conti. 2017. Breaking fitness records without moving: Reverse engineering and spoofing Fitbit. In *Research in Attacks, Intrusions, and Defenses*. Lecture Notes in Computer Science, Vol. 10453. Springer, 48–69. https://doi.org/10.1007/978-3-319-66332-6_3

[73] H. Fereidooni, T. Frassetto, M. Miettinen, A.-R. Sadeghi, and M. Conti. 2017. Fitness trackers: Fit for health but unfit for security and privacy. In *Proceedings of the IEEE/International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE '17)*. IEEE, 19–24. https://doi.org/10.1109/CHASE.2017.54

[74] K. Fietkiewicz and A. Ilhan. 2020. Fitness tracking technologies: Data privacy doesn't matter? The (un)concerns of users, former users, and non-users. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 3439–3448. https://doi.org/10.24251/HICSS.2020.421

[75] K. J. Fietkiewicz and M. Henkel. 2018. Privacy protecting fitness trackers: An oxymoron or soon to be reality? In *Social Computing and Social Media*. Lecture Notes in Computer Science, Vol. 10913. Springer, 431–444. https://doi.org/10.1007/978-3-319-91521-0_31

[76] T. Fritz, E. M. Huang, G. C. Murphy, and T. Zimmermann. 2014. Persuasive technology in the real world: A study of long-term use of activity sensing devices for fitness. In *Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 487–496. https://doi.org/10.1145/2556288.2557383

[77] M. Furini, S. Mirri, M. Montangero, and C. Prandi. 2020. Can IoT wearable devices feed frugal innovation? In *Proceedings of the Workshop on Experiences with the Design and Implementation of Frugal Smart Objects (FRUGALTHINGS '20)*. ACM, 1–6. https://doi.org/10.1145/3410670.3410861

[78] S. Gabriele and S. Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, 1–12. https://doi.org/10.1145/3313831.3376651

[79] Y. Gao, H. Li, and Y. Luo. 2015. An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems* 115, 9 (2015), 1704–1723. https://doi.org/10.1108/IMDS-03-2015-0087

[80] A. Garbett, D. Chatting, G. Wilkinson, C. Lee, and A. Kharrufa. 2018. ThinkActive: Designing for pseudonymous activity tracking in the classroom. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, 1–13. https://doi.org/10.1145/3173574.3173581

[81] K. Georgiou, A. V. Larentzakis, N. N. Khamis, G. I. Alsuhaibani, Y. A. Alaska, and E. J. Giallafos. 2018. Can wearable devices accurately measure heart rate variability? A systematic review. *Folia Medica* 60, 1 (2018), 7–20. https://doi.org/10.2478/folmed-2018-0012

[82] N. Gerber, P. Gerber, and M. Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002

[83] N. Gerber, B. Reinheimer, and M. Volkamer. 2019. Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 267–288. https://doi.org/10.2478/popets-2019-0047

[84] K. Ghazinour, E. Shirima, V. R. Parne, and A. BhoomReddy. 2017. A model to protect sharing sensitive information in smart watches. *Procedia Computer Science* 113 (2017), 105–112. https://doi.org/10.1016/j.procs.2017.08.322

[85] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal. 2016. How short Is too short? Implications of length and framing on the effectiveness of privacy notices. In *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS '16)*. 321–340. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck

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

[87] N. Gorm and I. Shklovski. 2016. Sharing steps in the workplace: Changing privacy concerns over time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 4315–4319. https://doi.org/10.1145/2858036.2858352

[88] N. Gorm and I. Shklovski. 2016. Steps, choices and moral accounting: Observations from a step-counting campaign in the workplace. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work and Social Computing*. ACM, 148–159. https://doi.org/10.1145/2818048.2819944

[89] N. Gorm and I. Shklovski. 2017. Participant driven photo elicitation for understanding activity tracking: Benefits and limitations. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, 1350–1361. https://doi.org/10.1145/2998181.2998214

[90] O. M. Gouda, D. J. Hejji, and M. S. Obaidat. 2020. Privacy assessment of fitness tracker devices. In *Proceedings of the International Conference on Computer, Information, and Telecommunication Systems (CITS '20)*. IEEE, 1–8. https://doi.org/10.1109/CITS49457.2020.9232503

[91] R. Gouveia, S. Barros, and E. Karapanos. 2014. Understanding users' disengagement with wearable activity trackers. In *Proceedings of the 2014 Advances in Computer Entertainment Conference Workshops (ACE Workshops '14)*. ACM, 1–3. https://doi.org/10.1145/2693787.2693802

[92] R. Gouveia, E. Karapanos, and M. Hassenzahl. 2018. Activity tracking in Vivo. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, 1–13. https://doi.org/10.1145/3173574.3173936

[93] R. Goyal, N. Dragoni, and A. Spognardi. 2016. Mind the tracker you wear: A security analysis of wearable health trackers. In *Proceedings of the Annual ACM Symposium on Applied Computing (SAC '16)*. ACM, 131–136. https://doi.org/10.1145/2851613.2851685

[94] X. Gui, Y. Chen, C. Caldeira, D. Xiao, and Y. Chen. 2017. When fitness meets social networks: Investigating fitness tracking and social practices on WeRun. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 1647–1659. https://doi.org/10.1145/3025453.3025654

[95] G. Guo, H. Zhang, L. Yao, H. Li, C. Xu, Z. Li, and W. Xu. 2021. MSLife: Digital behavioral phenotyping of multiple sclerosis symptoms in the wild using wearables and graph-based statistical analysis. *IMWUT* 5, 4 (2021), 1–35. https://doi.org/10.1145/3494970

[96] W. Guo, J. Rodolitz, and E. Birrell. 2020. Poli-See: An interactive tool for visualizing privacy policies. In *Proceedings of the Workshop on Privacy in the Electronic Society (WPES '20)*. ACM, 57–71. https://doi.org/10.1145/3411497.3420221

[97] A. Gupta, T. Heng, C. Shaw, D. Gromala, J. Leese, and L. Li. 2020. Oh, I didn't do a good job: How objective data affects physiotherapist-patient conversations for arthritis patients. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '20)*. ACM, 156–165. https://doi.org/10.1145/3421937.3421991

[98] A. Gupta, T. Heng, C. Shaw, L. Li, and L. Feehan. 2018. Designing pervasive technology for physical activity self-management in arthritis patients. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '18)*. ACM, 1–10. https://doi.org/10.1145/3240925.3240956

[99] M. A. Gutierrez, M. L. Fast, A. H. Ngu, and B. J. Gao. 2016. Real-time prediction of blood alcohol content using smartwatch sensor data. In Smart Health. Lecture Notes in Computer Science, Vol. 9545. Springer, 175–186.

[100] M. L. Hale, K. Lotfy, R. F. Gamble, C. Walter, and J. Lin. 2019. Developing a platform to evaluate and assess the security of wearable devices. *Digital Communications and Networks* 5, 3 (2019), 147–159. https://doi.org/10.1016/j.dcan.2018.10.009

[101] F. Hantke and A. Dewald. 2020. How can data from fitness trackers be obtained and analyzed with a forensic approach? In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW '20)*. IEEE, 500–508. https://doi.org/10.1109/EuroSPW51379.2020.00073

[102] D. Harrison, P. Marshall, N. Bianchi-Berthouze, and J. Bird. 2015. Activity tracking: Barriers, workarounds and customisation. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 617–621. https://doi.org/10.1145/2750858.2805832

[103] W. U. Hassan, S. Hussain, and A. Bates. 2018. Analysis of privacy protections in networks—Or—You can run, but can you hide? In *Proceedings of the USENIX Symposium on Security*. 497–512. https://www.usenix.org/conference/usenixsecurity18/presentation/hassan

[104] C. Hassenfeldt, S. Baig, I. Baggili, and X. Zhang. 2019. Map my murder: A digital forensic study of mobile health and fitness applications. In *Proceedings of the International Conference on Availability, Reliability, and Security (ARES '19)*. ACM, 1–12. https://doi.org/10.1145/3339252.3340515

[105] R. P. Hirten, M. Danieletto, L. Tomalin, K. H. Choi, M. Zweig, E. Golden, S. Kaur, D. Helmus, A. Biello, R. Pyzik, A. Charney, R. Miotto, B. S. Glicksberg, M. Levin, I. Nabeel, J. Aberg, D. Reich, D. Charney, E. P. Bottinger, L. Keefer, M. Suarez-Farinas, G. N. Nadkarni, and Z. 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 (2021), e26107. https://doi.org/10.2196/26107

[106] M. B. Hoy. 2016. Personal activity trackers and the quantified self. *Medical Reference Services Quarterly* 35, 1 (2016), 94–100. https://doi.org/10.1080/02763869.2016.1117300

[107] M. Humbert, B. Trubert, and K. Huguenin. 2019. A survey on interdependent privacy. *ACM Computing Surveys* 52, 6 (2019), Article 122, 40 pages. https://doi.org/10.1145/3360498

[108] L. Hutton, B. A. Price, R. Kelly, C. McCormick, A. K. Bandara, T. Hatzakis, M. Meadows, and B. Nuseibeh. 2018. Assessing the privacy of mHealth apps for self-tracking: Heuristic evaluation approach. *JMIR mHealth and uHealth* 6, 10 (2018), e185. https://doi.org/10.2196/mhealth.9217

[109] A. Ilhan and K. J. Fietkiewicz. 2020. Data privacy-related behavior and concerns of activity tracking technology users from Germany and the USA. *Aslib Journal of Information Management* 73, 2 (2020), 180–200. https://doi.org/10.1108/AJIM-03-2020-0067

[110] M. H. Iqbal, A. Aydin, O. Brunckhorst, P. Dasgupta, and K. Ahmed. 2016. A review of wearable technology in medicine. *Journal of the Royal Society of Medicine* 109, 10 (2016), 372–380. https://doi.org/10.1177/0141076816663560

[111] L. Jalali and R. Jain. 2013. Building health persona from personal data streams. In *Proceedings of the International Workshop on Personal Data Meets Distributed Multimedia (PDM '13)*. ACM, 19–26. https://doi.org/10.1145/2509352.2509400

[112] T. James, L. Wallace, and J. Dean. 2019. Using organismic integration theory to explore the associations between users' exercise motivations and fitness technology feature set use. *Management Information Systems Quarterly* 43, 1 (2019), 287–312. https://aisel.aisnet.org/misq/vol43/iss1/15

[113] M. H. Jarrahi, N. Gafinowitz, and G. Shin. 2018. Activity trackers, prior motivation, and perceived informational and motivational affordances. *Personal and Ubiquitous Computing* 22, 2 (2018), 433–448. https://doi.org/10.1007/s00779-017-1099-9

[114] A. H. Johnston and G. M. Weiss. 2015. Smartwatch-based biometric gait recognition. In *Proceedings of the International Conference on Biometrics Theory, Applications, and Systems (BTAS '15)*. IEEE, 1–6. https://doi.org/10.1109/BTAS.2015.7358794

[115] S. L. Jones, W. Hue, R. M. Kelly, R. Barnett, V. Henderson, and R. Sengupta. 2021. Determinants of longitudinal adherence in smartphone-based self-tracking for chronic health conditions: Evidence from axial spondyloarthritis. *IMWUT* 5, 1 (2021), Article 16, 24 pages. https://doi.org/10.1145/3448093

[116] M. S. Jørgensen, F. K. Nissen, J. Paay, J. Kjeldskov, and M. B. Skov. 2016. Monitoring children's physical activity and sleep: A study of surveillance and information disclosure. In *Proceedings of the Australian Conference on Computer (Human Interaction '16)*. ACM, 50–58. https://doi.org/10.1145/3010915.3010936

[117] M. Kalantari. 2017. Consumers' adoption of wearable technologies: Literature review, synthesis, and future research agenda. *International Journal of Technology Marketing* 12, 3 (2017), 274. https://doi.org/10.1504/IJTMKT.2017.089665

[118] M. Katurura and L. Cilliers. 2019. Privacy in wearable health devices: How does POPIA measure up? In *Kalpa Publications in Computing*, Vol. 12. EasyChair, 112–122. https://doi.org/10.29007/qsp7

[119] A. Kazlouski, T. Marchioro, H. Manifavas, and E. Markatos. 2021. I still see you! Inferring fitness data from encrypted traffic of wearables. In *Proceedings of the International Joint Conference on Biomedical Engineering Systems and Technologies*. 369–376. https://doi.org/10.5220/0010233103690376

[120] F. Kensing and J. Blomberg. 1998. Participatory design: Issues and concerns. *Computer Supported Cooperative Work* 7, 3 (1998), 167–185. https://doi.org/10.1023/A:1008689307411

[121] D.-J. Kim, Y. Lee, S. Rho, and Y.-K. Lim. 2016. Design opportunities in three stages of relationship development between users and self-tracking devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, 699–703. https://doi.org/10.1145/2858036.2858148

[122] S. Kim and A. Choudhury. 2020. Comparison of older and younger adults' attitudes toward the adoption and use of activity trackers. *JMIR mHealth and uHealth* 8, 10 (2020), e18312. https://doi.org/10.2196/18312

[123] S. Kim, A. Thakur, and J. Kim. 2020. Understanding users' perception towards automated personality detection with group-specific behavioral data. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, 1–12. https://doi.org/10.1145/3313831.3376250

[124] T. B. Kim and C.-T. B. Ho. 2021. Validating the moderating role of age in multi-perspective acceptance model of wearable healthcare technology. *Telematics and Informatics* 61 (2021), 101603. https://doi.org/10.1016/j.tele.2021.101603

[125] Y.-H. Kim, J. H. Jeon, B. Lee, E. K. Choe, and J. Seo. 2017. OmniTrack: A flexible self-tracking approach leveraging semi-automated tracking. *IMWUT* 1, 3 (2017), Article 67, 28 pages. https://doi.org/10.1145/3130930

[126] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. 2009. Systematic literature reviews in software engineering—A systematic literature review. *Information and Software Technology* 51, 1 (2009), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

[127] B. P. Kolla, S. Mansukhani, and M. P. Mansukhani. 2016. Consumer sleep tracking devices: A review of mechanisms, validity and utility. *Expert Review of Medical Devices* 13, 5 (2016), 497–506. https://doi.org/10.1586/17434440.2016.1171708

[128] V. Kumari and S. A. Hook. 2017. The privacy, security and discoverability of data on wearable health devices: Fitness or folly? In *Universal Access in Human–Computer Interaction. Human and Technological Environments*. Lecture Notes in Computer Science, Vol. 10279. Springer, 50–64. https://doi.org/10.1007/978-3-319-58700-4_5

[129] A. Kuzminykh and E. Lank. 2019. How much is too much? Understanding the information needs of parents of young children. *IMWUT* 3, 2 (2019), Article 52, 21 pages. https://doi.org/10.1145/3328923

[130] O. D. Lara and M. A. Labrador. 2012. A survey on human activity recognition using wearable sensors. *IEEE Communications Surveys & Tutorials* 15, 3 (2012), 1192–1209. https://doi.org/10.1109/SURV.2012.110112.00192

[131] A. Lazar, C. Koehler, J. Tanenbaum, and D. H. Nguyen. 2015. Why we use and abandon smart devices. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 635–646. https://doi.org/10.1145/2750858.2804288

[132] H. Lee, S. Kang, and U. Lee. 2022. Understanding privacy risks and perceived benefits in open dataset collection for mobile affective computing. *IMWUT* 6, 2 (2022), 1–26. https://doi.org/10.1145/3534623

[133] C. Lehrer, U. Y. Eseryel, A. Rieder, and R. Jung. 2021. Behavior change through wearables: The interplay between self-leadership and IT-based leadership. *Electronic Markets* 31, 4 (2021), 747–764. https://doi.org/10.1007/s12525-021-00474-3

[134] M. Lehto and M. Miikael. 2017. Health information privacy of activity trackers. In *Proceedings of the 2017 16th European Conference on Cyber Warfare and Security (ECCWS '17)*. 243–251.

[135] D. Leibenger, F. Möllers, A. Petrlic, R. Petrlic, and C. Sorge. 2016. Privacy challenges in the quantified self movement—An EU perspective. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 315–334. https://doi.org/10.1515/popets-2016-0042

[136] R. Leitão. 2019. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the Designing Interactive Systems Conference (DIS '19)*. ACM, 527–539. https://doi.org/10.1145/3322276.3322366

[137] H. Li, J. Wu, Y. Gao, and Y. Shi. 2016. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics* 88 (2016), 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

[138] J. Li, Z. He, Y. Cui, C. Wang, C. Chen, C. Yu, M. Zhang, Y. Liu, and S. Ma. 2022. Towards ubiquitous personalized music recommendation with smart bracelets. *IMWUT* 6, 3 (2022), 1–34. https://doi.org/10.1145/3550333

[139] Q. Li, C. Caldeira, D. A. Epstein, and Y. Chen. 2020. Supporting caring among intergenerational family members through family fitness tracking. In *Proceedings of the Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth '20)*. ACM, 1–10. https://doi.org/10.1145/3421937.3422018

[140] X. Li, F. Yan, F. Zuo, Q. Zeng, and L. Luo. 2019. Touch well before use: Intuitive and secure authentication for IoT devices. In *Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom '19)*. ACM, 1–17. https://doi.org/10.1145/3300061.3345434

[141] Y. Liao. 2019. Sharing personal health information on social media: Balancing self-presentation and privacy. In *Proceedings of the International Conference on Social Media and Society (SMSociety '19)*. ACM, 194–204. https://doi.org/10.1145/3328529.3328560

[142] C. Lidynia, P. Brauner, and M. Ziefle. 2018. A step in the right direction—Understanding privacy concerns and perceived sensitivity of fitness trackers. In *Advances in Human Factors in Wearable Technologies and Game Design*, Tareq Ahram and Christianne Falcão (Eds.). Advances in Intelligent Systems and Computing. Springer International Publishing, 42–53. https://doi.org/10.1007/978-3-319-60639-2_5

[143] B. Y. Lim, J. Kay, and W. Liu. 2019. How does a nation walk? Interpreting large-scale step count activity with weekly streak patterns. *IMWUT* 3, 2 (2019), Article 57, 46 pages. https://doi.org/10.1145/3328928

[144] C. Liu, L. Zhang, Z. Liu, K. Liu, X. Li, and Y. Liu. 2016. Lasagna: Towards deep hierarchical understanding and searching over mobile sensing data. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. ACM, 334–347. https://doi.org/10.1145/2973750.2973752

[145] W. Liu, B. Ploderer, and T. Hoang. 2015. In bed with technology: Challenges and opportunities for sleep tracking. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*. ACM, 142–151. https://doi.org/10.1145/2838739.2838742

[146] K. Lotfy and M. L. Hale. 2016. Assessing pairing and data exchange mechanism security in the wearable Internet of Things. In *Proceedings of the International Conference on Mobile Services (MS '16)*. IEEE, 25–32. https://doi.org/10.1109/MobServ.2016.15

[147] B. Lowens, V. G. Motti, and K. Caine. 2017. Wearable privacy: Skeletons in the data closet. In *Proceedings of the International Conference on Healthcare Informatics (ICHI '17)*. IEEE, 295–304. https://doi.org/10.1109/ICHI.2017.29

[148] C. X. Lu, B. Du, H. Wen, S. Wang, A. Markham, I. Martinovic, Y. Shen, and N. Trigoni. 2018. Snoopy: Sniffing your smartwatch passwords via deep sequence learning. *IMWUT* 1, 4 (2018), Article 152, 29 pages. https://doi.org/10.1145/3161196

[149] A. Lunney, N. R. Cunningham, and M. S. Eastin. 2016. Wearable fitness technology: A structural investigation into acceptance and perceived fitness outcomes. *Computers in Human Behavior* 65 (2016), 114–120. https://doi.org/10.1016/j.chb.2016.08.007

[150] D. Lupton. 2016. The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society* 45, 1 (2016), 101–122. https://doi.org/10.1080/03085147.2016.1143726

[151] D. Lupton. 2020. 'Better understanding about what's going on': Young Australians' use of digital technologies for health and fitness. *Sport, Education and Society* 25, 1 (2020), 1–13. https://doi.org/10.1080/13573322.2018.1555661

[152] D. Lupton. 2021. "Sharing Is Caring": Australian self-trackers' concepts and practices of personal data sharing and privacy. *Frontiers in Digital Health* 3 (2021), 11. https://doi.org/10.3389/fdgth.2021.649275

[153] A. Maiti, O. Armbruster, M. Jadliwala, and J. He. 2016. Smartwatch-based keystroke inference attacks and context-aware protection mechanisms. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIA CCS '16)*. ACM, 795–806. https://doi.org/10.1145/2897845.2897905

[154] A. Maiti, R. Heard, M. Sabra, and M. Jadliwala. 2018. Towards inferring mechanical lock combinations using wrist-wearables as a side-channel. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '18)*. ACM, 111–122. https://doi.org/10.1145/3212480.3212498 arXiv:1710.00217

[155] A. Maiti, M. Jadliwala, J. He, and I. Bilogrevic. 2018. Side-channel inference attacks on mobile keypads using smartwatches. *IEEE Transactions on Mobile Computing* 17, 9 (2018), 2180–2194. https://doi.org/10.1109/TMC.2018.2794984

[156] S. Marassi and P. Collins. 2021. Is that lawful? Data privacy and fitness trackers in the workplace. *International Journal of Comparative Labour Law and Industrial Relations* 37, 1 (2021), 30. https://kluwerlawonline.com/journalarticle/International+Journal+of+Comparative+Labour+Law+and+Industrial+Relations/37.1/IJCL2021003

[157] C. M. Mares. 2016. To cover or not to cover: The relationship between the Apple Watch and the Health Insurance Portability and Accountability Act. *DePaul Journal of Health Care Law* 18, 2 (2016), 159–180. https://heinonline.org/HOL/P?h=hein.journals/dephcl18&i=173

[158] K. Masuch, M. Greve, and S. Trang. 2021. Fitness first or safety first? Examining adverse consequences of privacy seals in the event of a data breach. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. 3871. https://doi.org/10.24251/HICSS.2021.469

[159] C. Matt, M. Becker, A. Kolbeck, and T. Hess. 2019. Continuously healthy, continuously used?—A thematic analysis of user perceptions on consumer health wearables. *Pacific Asia Journal of the Association for Information Systems* 11, 1 (2019), 108–132. https://doi.org/10.17705/1pais.11105

[160] S. Mcnary and A. Hunter. 2018. Wearable device data for criminal investigation. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. Lecture Notes in Computer Science, Vol. 11342. Springer, 60–71. https://doi.org/10.1007/978-3-030-05345-1_5

[161] F. A. Mendoza, L. Alonso, A. M. López, , and D. D. S. Patricia Arias Cabarcos. 2018. Assessment of fitness tracker security: A case of study. *Proceedings* 2, 19 (2018), 1235. https://doi.org/10.3390/proceedings2191235

[162] Ü. Meteriz, N. F. Yıldıran, J. Kim, and D. Mohaisen. 2020. Understanding the potential risks of sharing elevation information on fitness applications. In *Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS '20)*. IEEE, 464–473. https://doi.org/10.1109/ICDCS47774.2020.00063

[163] J. Meyer, M. Wasmann, W. Heuten, A. El Ali, and S. C. Boll. 2017. Identification and classification of usage patterns in long-term activity tracking. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 667–678. https://doi.org/10.1145/3025453.3025690

[164] J. Mnjama, G. Foster, and B. Irwin. 2017. A privacy and security threat assessment framework for consumer health wearables. In *Proceedings of the 2017 Conference on Information Security for South Africa (ISSA '17)*. IEEE, 66–73. https://doi.org/10.1109/ISSA.2017.8251776

[165] S. Moganedi and D. Pottas. 2020. Identification of information security controls for fitness wearable manufacturers. In *Information and Cyber Security*, Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, Jan Eloff, and Reinhardt Botha (Eds.). Communications in Computer and Information Science. Springer International Publishing, 112–128. https://doi.org/10.1007/978-3-030-66039-0_8

[166] K. R. Moore, N. Jones, B. S. Cundiff, and L. Heilig. 2018. Contested sites of health risks: Using wearable technologies to intervene in racial oppression. *Communication Design Quarterly* 5, 4 (2018), 52–60. https://doi.org/10.1145/3188387.3188392

[167] V. G. Motti and K. Caine. 2016. Smart wearables or dumb wearables? Understanding how context impacts the UX in wrist worn interaction. In *Proceedings of the International Conference on the Design of Communication (SIGDOC '16)*. ACM, 1–10. https://doi.org/10.1145/2987592.2987606

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

[169] L. Na, C. Yang, C.-C. Lo, F. Zhao, Y. Fukuoka, and A. Aswani. 2018. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. *JAMA Network Open* 1, 8 (2018), e186040–e186040. https://doi.org/10.1001/jamanetworkopen.2018.6040

[170] H. Nissenbaum. 2004. Privacy as contextual integrity. *HeinOnline* 79 (2004), 119.

[171] K. Nuss and K. Li. 2021. Motivation for physical activity and physical activity engagement in current and former wearable fitness tracker users: A mixed-methods examination. *Computers in Human Behavior* 121 (2021), 106798. https://doi.org/10.1016/j.chb.2021.106798

[172] J. Orlosky, O. Ezenwoye, H. Yates, and G. Besenyi. 2019. A look at the security and privacy of Fitbit as a health activity tracker. In *Proceedings of the ACM Southeast Conference (ACM SE '19)*. ACM, 241–244. https://doi.org/10.1145/3299815.3314468

[173] J. Owen, D. Archibald, and D. Wickramanayake. 2019. The willingness to adopt fitness wearables in Jamaica: A study on wearable fitness trackers in Kingston and St. Andrew. *International Journal of Internet of Things* 8, 2 (2019), 36–45. https://doi.org/10.5923/j.ijit.20190802.02

[174] I. Oygür, D. A. Epstein, and Y. Chen. 2020. Raising the responsible child: Collaborative work in the use of activity trackers for children. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), Article 157, 23 pages. https://doi.org/10.1145/3415228

[175] X. Page, P. Bahirat, M. I. Safi, B. P. Knijnenburg, and P. Wisniewski. 2018. The Internet of what? Understanding differences in perceptions and adoption for the Internet of Things. *IMWUT* 2, 4 (2018), Article 183, 22 pages. https://doi.org/10.1145/3287061

[176] S. Paluch and S. Tuzovic. 2019. Persuaded self-tracking with wearable technology: Carrot or stick? *Journal of Services Marketing* 33, 4 (2019), 436–448. https://doi.org/10.1108/JSM-03-2018-0091

[177] A. Pantelopoulos and N. Bourbakis. 2009. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics* 40, 1 (2009), 1–12. https://doi.org/10.1109/TSMCC.2009.2032660

[178] P. Parameshwarappa, Z. Chen, and G. Koru. 2020. An effective and computationally efficient approach for anonymizing large-scale physical activity data: Multi-level clustering-based anonymization. *International Journal of Information Security and Privacy* 14, 3 (2020), 72–94. https://doi.org/10.4018/IJISP.2020070105

[179] V. D. Pasquale, V. De Simone, M. Radano, and S. Miranda. 2022. Wearable devices for health and safety in production systems: A literature review. *IFAC-PapersOnLine* 55, 10 (2022), 341–346. https://doi.org/10.1016/j.ifacol.2022.09.410

[180] M. Patel and A. A. O'Kane. 2015. Contextual influences on the use and non-use of digital technology while exercising at the Gym. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2923–2932. https://doi.org/10.1145/2702123.2702384

[181] S. Patel, H. Park, P. Bonato, L. Chan, and M. Rodgers. 2012. A review of wearable sensors and systems with application in rehabilitation. *Journal of NeuroEngineering and Rehabilitation* 9, 1 (2012), 21. https://doi.org/10.1186/1743-0003-9-21

[182] G. Paul and J. Irvine. 2014. Privacy implications of wearable health devices. In *Proceedings of the International Conference on Security of Information and Networks (SIN '14)*. ACM, 117–121. https://doi.org/10.1145/2659651.2659683

[183] J. M. Pevnick, G. Fuller, R. Duncan, and B. M. R. Spiegel. 2016. A large-scale initiative inviting patients to share personal fitness tracker data with their providers: Initial results. *PLOS ONE* 11, 11 (2016), e0165908. https://doi.org/10.1371/journal.pone.0165908

[184] J. Pinchot and D. Cellante. 2021. Privacy concerns and data sharing habits of personal fitness information collected via activity trackers. *Journal of Information Systems Applied Research* 14, 2 (2021), 4–13. http://jisar.org/2021-14/n2/JISARv14n2p4.html

[185] Z. Pingo and B. Narayan. 2018. Users' responses to privacy issues with the connected information ecologies created by fitness trackers. In *Maturity and Innovation in Digital Libraries*. Lecture Notes in Computer Science, Vol. 11279. Springer, 240–255. https://doi.org/10.1007/978-3-030-04257-8_25

[186] Z. Pingo and B. Narayan. 2019. "My smartwatch told me to see a sleep doctor": A study of activity tracker use. *Online Information Review* 44, 2 (2019), 503–519. https://doi.org/10.1108/OIR-04-2018-0115

[187] K. Potapov and P. Marshall. 2020. LifeMosaic: Co-design of a personal informatics tool for youth. In *Proceedings of the Interaction Design and Children Conference (IDC '20)*. ACM, 519–531. https://doi.org/10.1145/3392063.3394429

[188] K. C. Preusse, T. L. Mitzner, C. B. Fausset, and W. A. Rogers. 2017. Older adults' acceptance of activity trackers. *Journal of Applied Gerontology* 36, 2 (2017), 127–155. https://doi.org/10.1177/0733464815624151

[189] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie. 2019. The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials* 21, 3 (2019), 2772–2793. https://doi.org/10.1109/COMST.2018.2873950

[190] A. Puussaar, A. K. Clear, and P. Wright. 2017. Enhancing personal informatics through social sensemaking. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 6936–6942. https://doi.org/10.1145/3025453.3025804

[191] E. Rader and J. Slaker. 2017. The importance of visibility for folk theories of sensor data. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS '17)*. 257–270. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/rader

[192] M. Rahman, B. Carbunar, and U. Topkara. 2016. Secure management of low power fitness trackers. *IEEE Transactions on Mobile Computing* 15, 2 (2016), 447–459. https://doi.org/10.1109/TMC.2015.2418774

[193] D. Rajanen and M. Weng. 2017. Digitization for fun or reward? A study of acceptance of wearable devices for personal healthcare. In *Proceedings of the International Academic Mindtrek Conference (AcademicMindtrek '17)*. ACM, 154–163. https://doi.org/10.1145/3131085.3131118

[194] M. Randriambelonoro, Y. Chen, and P. Pu. 2017. Can fitness trackers help diabetic and obese users make and sustain lifestyle changes? *Computer* 50, 3 (2017), 20–29. https://doi.org/10.1109/MC.2017.92

[195] J. Ranjan and K. Whitehouse. 2015. Object hallmarks: Identifying object users using wearable wrist sensors. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 51–61. https://doi.org/10.1145/2750858.2804263

[196] A. Rapp and L. Tirabeni. 2018. Personal informatics for sport: Meaning, body, and social relations in amateur and elite athletes. *ACM Transactions on Computer-Human Interaction* 25, 3 (2018), Article 16, 30 pages. https://doi.org/10.1145/3196829

[197] R. Ravichandran, S.-W. Sien, S. N. Patel, J. A. Kientz, and L. R. Pina. 2017. Making sense of sleep sensors: How sleep sensing technologies support and undermine sleep health. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 6864–6875. https://doi.org/10.1145/3025453.3025557

[198] R. Reith, C. Buck, T. Eymann, and B. Lis. 2020. Integrating privacy concerns into the unified theory of acceptance and use of technology to explain the adoption of fitness trackers. *International Journal of Innovation and Technology Management* 17, 7 (2020), 37. https://doi.org/10.1142/S0219877020500492

[199] X. Ren, B. Yu, Y. Lu, and A. Brombacher. 2018. Exploring cooperative fitness tracking to encourage physical activity among office workers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), Article 146, 20 pages. https://doi.org/10.1145/3274415

[200] A. Rieder, U. Y. Eseryel, C. Lehrer, and R. Jung. 2021. Why users comply with wearables: The role of contextual self-efficacy in behavioral change. *International Journal of Human–Computer Interaction* 37, 3 (2021), 281–294. https://doi.org/10.1080/10447318.2020.1819669

[201] T. Robertson Ishii and P. Atkins. 2020. Essential vs. accidental properties. In *The Stanford Encyclopedia of Philosophy* (Winter 2020 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=essential-accidental#

[202] J. Rooksby, M. Rost, A. Morrison, and M. Chalmers. 2014. Personal tracking as lived informatics. In *Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 1163–1172. https://doi.org/10.1145/2556288.2557039

[203] J. Rooksby, M. Rost, A. Morrison, and M. Chalmers. 2015. Pass the ball: Enforced turn-taking in activity tracking. In *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2417–2426. https://doi.org/10.1145/2702123.2702577

[204] A. Rubin and J. Ophoff. 2018. Investigating adoption factors of wearable technology in health and fitness. In *Proceedings of the Open Innovations Conference (OI '18)*. IEEE, 176–186. https://doi.org/10.1109/OI.2018.8535831

[205] M. A. Rupp, J. R. Michaelis, D. S. McConnell, and J. 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. https://doi.org/10.1016/j.apergo.2018.02.005

[206] P. Saa, O. Moscoso-Zea, and S. Lujan-Mora. 2018. Wearable technology, privacy issues. In *Proceedings of the International Conference on Information Technology and Systems (ICITS '18)*. 518–527. https://doi.org/10.1007/978-3-319-73450-7_49

[207] M. Sabra, A. Maiti, and M. Jadliwala. 2018. Keystroke inference using ambient light sensor on wrist-wearables: A feasibility study. In *Proceedings of the ACM Workshop on Wearable Systems and Applications*. ACM, 21–26. https://doi.org/10.1145/3211960.3211973

[208] H. Saksono, C. Castaneda-Sceppa, J. Hoffman, M. Seif El-Nasr, V. Morris, and A. G. Parker. 2018. Family health promotion in low-SES neighborhoods: A two-month study of wearable activity tracking. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, 1–13. https://doi.org/10.1145/3173574.3173883

[209] H. Saksono, C. Castaneda-Sceppa, J. Hoffman, M. Seif El-Nasr, V. Morris, and A. G. Parker. 2019. Social reflections on fitness tracking data: A study with families in low-SES neighborhoods. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, 1–14. https://doi.org/10.1145/3290605.3300543

[210] K. Salehzadeh Niksirat, L. Goswami, P. S. B. Rao, J. Tyler, A. Silacci, S. Aliyu, A. Aebli, C. Wacharamanotham, and M. Cherubini. 2023. Changes in research ethics, openness, and transparency in empirical studies between CHI 2017 and CHI 2022. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. ACM, 1–23. https://doi.org/10.1145/3544548.3580848

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

[212] O. R. Sanchez, I. Torre, Y. He, and B. P. Knijnenburg. 2020. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User-Adapted Interaction* 30, 3 (2020), 513–565. https://doi.org/10.1007/s11257-019-09246-3

[213] B. Schiller, T. Brogt, J. P. M. Schuler, G. Strobel, and S. Eicker. 2020. Identifying quality factors for self-tracking solutions: A systematic literature review. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 3690–3699. http://hdl.handle.net/10125/64194

[214] S. Schneegass, R. Poguntke, and T. Machulla. 2019. Understanding the impact of information representation on willingness to share information. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, 1–6. https://doi.org/10.1145/3290605.3300753

[215] E. Schomakers, C. Lidynia, and M. Ziefle. 2019. Listen to my heart? How privacy concerns shape users' acceptance of e-Health technologies. In *Proceedings of the International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob '19)*. IEEE, 306–311. https://doi.org/10.1109/WiMOB.2019.8923448

[216] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne. 2017. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2573–2620. https://ieeexplore.ieee.org/document/7993011

[217] S. Shen, H. Wang, and R. Roy Choudhury. 2016. I am a smartwatch and I can track my user's arm. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services*. ACM, 85–96. https://doi.org/10.1145/2906388.2906407

[218] Y. Shen, B. Du, W. Xu, C. Luo, B. Wei, L. Cui, and H. Wen. 2020. Securing cyber-physical social interactions on wrist-worn devices. *ACM Transactions on Sensor Networks* 16, 2 (2020), Article 19, 22 pages. https://doi.org/10.1145/3378669

[219] J. Shim, K. Lim, J. Jeong, S.-j. Cho, M. Park, and S. Han. 2017. A case study on vulnerability analysis and firmware modification attack for a wearable fitness tracker. *IT Convergence Practice* 5, 4 (2017), 25–33.

[220] G. Shin, M. H. Jarrahi, Y. Fei, A. Karami, N. Gafinowitz, A. Byun, and X. Lu. 2019. Wearable activity trackers, accuracy, adoption, acceptance and health impact: A systematic literature review. *Journal of Biomedical Informatics* 93 (2019), 103153. https://doi.org/10.1016/j.jbi.2019.103153

[221] G. D. Shin. 2020. Investigating the impact of daily life context on physical activity in terms of steps information generated by wearable activity tracker. *International Journal of Medical Informatics* 141 (2020), 104222. https://doi.org/10.1016/j.ijmedinf.2020.104222

[222] M. Shoaib, H. Scholten, P. J. M. Havinga, and O. D. Incel. 2016. A hierarchical lazy smoking detection algorithm using smartwatch sensors. In *Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications, and Services (Healthcom '16)*. IEEE, 1–6. https://doi.org/10.1109/HealthCom.2016.7749439

[223] P. Shrestha and N. Saxena. 2017. An offensive and defensive exposition of wearable computing. *ACM Computing Surveys* 50, 6 (2017), Article 92, 39 pages. https://doi.org/10.1145/3133837

[224] P. Shrestha and N. Saxena. 2020. Hacksaw: Biometric-free non-stop web authentication in an emerging world of wearables. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20)*. ACM, 13–24. https://doi.org/10.1145/3395351.3399366

[225] M. Siddiqi, S. T. Ali, and V. Sivaraman. 2020. Forensic verification of health data from wearable devices using anonymous witnesses. *IEEE Internet of Things Journal* 7, 11 (2020), 10745–10762. https://doi.org/10.1109/JIOT.2020.2982958

[226] C. Skalka, J. Ring, D. Darias, M. Kwon, S. Gupta, K. Diller, S. Smolka, and N. Foster. 2019. Proof-carrying network code. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. ACM, 1115–1129. https://doi.org/10.1145/3319535.3363214

[227] E. Steinberg. 2021. Run for your life: The ethics of behavioral tracking in insurance. *Journal of Business Ethics* 179, 3 (2021), 665–682. https://doi.org/10.1007/s10551-021-04863-8

[228] D. Stück, H. T. Hallgrímsson, G. Ver Steeg, A. Epasto, and L. Foschini. 2017. The spread of physical activity through social networks. In *Proceedings of the International Conference on World Wide Web (WWW '17)*. 519–528. https://doi.org/10.1145/3038912.3052688

[229] J. Sturgess, S. Eberz, I. Sluganovic, and I. Martinovic. 2022. Inferring user height and improving impersonation attacks in mobile payments using a smartwatch. In *Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops '22)*. IEEE, 775–780. https://doi.org/10.1109/PerComWorkshops53856.2022.9767287

[230] J. Sturgess, S. Eberz, I. Sluganovic, and I. Martinovic. 2022. WatchAuth: User authentication and intent recognition in mobile payments using a smartwatch. *arXiv:2202.01736 [cs]* 2022). http://arxiv.org/abs/2202.01736

[231] A. N. Sullivan and M. E. Lachman. 2017. Behavior change with fitness technology in sedentary adults: A review of the evidence for increasing physical activity. *Frontiers in Public Health* 4 (2017), 16. https://www.frontiersin.org/articles/10.3389/fpubh.2016.00289

[232] E. Svertoka, S. Saafi, A. Rusu-Casandra, R. Burget, I. Marghescu, J. Hosek, and A. Ometov. 2021. Wearables for industrial work safety: A survey. *Sensors* 21, 11 (2021), 3844. https://doi.org/10.3390/s21113844

[233] L. M. Tang and J. Kay. 2017. Harnessing long term physical activity data—How long-term trackers use data and how an adherence-based interface supports new insights. *IMWUT* 1, 2 (2017), Article 26, 28 pages. https://doi.org/10.1145/3090091

[234] L. M. Tang, J. Meyer, D. A. Epstein, K. Bragg, L. Engelen, A. Bauman, and J. Kay. 2018. Defining adherence: Making sense of physical activity tracker data. *IMWUT* 2, 1 (2018), Article 37, 22 pages. https://doi.org/10.1145/3191769

[235] F. Tehranipoor, N. Karimian, P. A. Wortman, and J. A. Chandy. 2018. Low-cost authentication paradigm for consumer electronics within the Internet of wearable fitness tracking applications. In *Proceedings of the International Conference on Consumer Electronics (ICCE '18)*. IEEE, 1–6. https://doi.org/10.1109/ICCE.2018.8326233

[236] E. Thomaz, I. Essa, and G. D. Abowd. 2015. A practical approach for recognizing eating moments with wrist-mounted inertial sensing. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 1029–1040. https://doi.org/10.1145/2750858.2807545

[237] B. Thuraisingham, M. Kantarcioglu, E. Bertino, J. Z. Bakdash, and M. Fernandez. 2018. Towards a privacy-aware quantified self data management framework. In *Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT '18)*. ACM, 173–184. https://doi.org/10.1145/3205977.3205997

[238] I. Torre, O. R. Sanchez, F. Koceva, and G. Adorni. 2018. Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing* 22, 2 (2018), 345–364. https://doi.org/10.1007/s00779-017-1068-3

[239] L. Tuovinen and A. F. Smeaton. 2019. Unlocking the black box of wearable intelligence: Ethical considerations and social impact. In *Proceedings of the IEEE Congress on Evolutionary Computation (CEC '19)*. IEEE, 3235–3243. https://doi.org/10.1109/CEC.2019.8790173

[240] Y. F. van Kasteren, L. Perimal-Lewis, and A. Maeder. 2018. Detecting short-duration ambulatory episodes in Fitbit®data. In *Proceedings of the Australasian Computer Science Week Multiconference (ACSW '18)*. ACM, 1–5. https://doi.org/10.1145/3167918.3167954

[241] D. Vandervort. 2016. Medical device data goes to court. In *Proceedings of the International Conference on Digital Health (DH '16)*. ACM, 23–27. https://doi.org/10.1145/2896338.2896341

[242] L. Velykoivanenko, K. Salehzadeh Niksirat, N. Zufferey, M. Humbert, K. Huguenin, and M. Cherubini. 2021. Are those steps worth your privacy? Fitness-tracker users' perceptions of privacy and utility. *IMWUT* 5, 4 (2021), Article 181, 41 pages. https://doi.org/10.1145/3494960

[243] J. Vermeulen, L. MacDonald, J. Schöning, R. Beale, and S. Carpendale. 2016. Heartefacts: Augmenting mobile video sharing using wrist-worn heart rate sensors. In *Proceedings of the ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, 712–723. https://doi.org/10.1145/2901790.2901887

[244] S. Vhaduri and C. Poellabauer. 2017. Wearable device user authentication using physiological and behavioral metrics. In *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC '17)*. IEEE, 1–6. https://doi.org/10.1109/PIMRC.2017.8292272

[245] N. Vinayaga-Sureshkanth, A. Maiti, M. Jadliwala, K. Crager, J. He, and H. Rathore. 2018. A practical framework for preventing distracted pedestrian-related incidents using wrist wearables. *IEEE Access* 6 (2018), 78016–78030. https://doi.org/10.1109/ACCESS.2018.2884669

[246] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, and K. Kritikos. 2018. Privacy attitudes and data valuation among fitness tracker users. In Transforming Digital Worlds. Lecture Notes in Computer Science, Vol. 10766. Springer, 229–239. https://doi.org/10.1007/978-3-319-78105-1_27

[247] C. Wang, X. Guo, Y. Chen, Y. Wang, and B. Liu. 2018. Personal PIN leakage from wearable devices. *IEEE Transactions on Mobile Computing* 17, 3 (2018), 646–660. https://doi.org/10.1109/TMC.2017.2737533

[248] J. Wang, F. Hu, Y. Zhou, Y. Liu, H. Zhang, and Z. Liu. 2020. BlueDoor: Breaking the secure information flow via BLE vulnerability. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys '20)*. ACM, 286–298. https://doi.org/10.1145/3386901.3389025

[249] J. Wang, N. Wang, and H. Jin. 2016. Context matters? How adding the obfuscation option affects end users' data disclosure decisions. In *Proceedings of the International Conference on Intelligent User Interfaces (IUI '16)*. ACM, 299–304. https://doi.org/10.1145/2856767.2856817

[250] Y. Wang, I. Weber, and P. Mitra. 2016. Quantified self meets social media: Sharing of weight updates on Twitter. In *Proceedings of the International Conference on Digital Health (DH '16)*. ACM, 93–97. https://doi.org/10.1145/2896338.2896363

[251] J. A. Ward, D. Richardson, G. Orgs, K. Hunter, and A. Hamilton. 2018. Sensing interpersonal synchrony between actors and autistic children in theatre using wrist-worn accelerometers. In *Proceedings of the 2018 ACM International Symposium on Wearable Computers*. ACM, 148–155. https://doi.org/10.1145/3267242.3267263

[252] G. M. Weiss, J. L. Timko, C. M. Gallagher, K. Yoneda, and A. J. Schreiber. 2016. Smartwatch-based activity recognition: A machine learning approach. In *Proceedings of the IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI '16)*. IEEE, 426–429. https://doi.org/10.1109/BHI.2016.7455925

[253] A. Wieneke, C. Lehrer, R. Zeder, and R. Jung. 2016. Privacy-related decision-making in the context of wearable use. *PACIS 2016 Proceedings* 67 (2016), 16. https://aisel.aisnet.org/pacis2016/67

[254] R. Wijewickrama, A. Maiti, and M. Jadliwala. 2019. deWristified: Handwriting inference using wrist-based motion sensors revisited. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19)*. ACM, 49–59. https://doi.org/10.1145/3317549.3319722

[255] N. A. Windasari, F.-R. Lin, and Y.-C. Kato-Lin. 2021. Continued use of wearable fitness technology: A value co-creation perspective. *International Journal of Information Management* 57 (2021), 102292. https://doi.org/10.1016/j.ijinfomgt.2020.102292

[256] M. Wu and J. Luo. 2019. Wearable technology applications in healthcare: A literature review. *Online Journal of Nursing Informatics* 23, 3 (2019). https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review

[257] Q. Xia, F. Hong, Y. Feng, and Z. Guo. 2018. MotionHacker: Motion sensor based eavesdropping on handwriting via smartwatch. In *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '18)*. IEEE, 468–473. https://doi.org/10.1109/INFCOMW.2018.8406879

[258] J. Xin, V. V. Phoha, and A. Salekin. 2022. Combating false data injection attacks on human-centric sensing applications. *IMWUT* 6, 2 (2022), 1–22. https://doi.org/10.1145/3534577

[259] C. Xu, P. H. Pathak, and P. Mohapatra. 2015. Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications (HotMobile '15)*. ACM, 9–14. https://doi.org/10.1145/2699343.2699350

[260] W. Yan, S. Hylamia, T. Voigt, and C. Rohner. 2020. PHY-IDS: A physical-layer spoofing attack detection system for wearable devices. In *Proceedings of the ACM Workshop on Wearable Systems and Applications (WearSys '20)*. ACM, 1–6. https://doi.org/10.1145/3396870.3400010

[261] R. Yang, E. Shin, M. W. Newman, and M. S. Ackerman. 2015. When fitness trackers don't 'fit': End-user difficulties in the assessment of personal tracking device accuracy. In *Proceedings of the Conference on Ubiquitous Computing (UbiComp '15)*. ACM, 623–634. https://doi.org/10.1145/2750858.2804269

[262] S. Yazawa, H. Yoshimoto, and K. Hiraki. 2018. Learning with wearable devices reveals learners' best time to learn. In *Proceedings of the International Conference on Education and E (Learning '18)*. ACM, 87–92. https://doi.org/10.1145/3291078.3291097

[263] Y. H. Yoon and U. Karabiyik. 2020. Forensic analysis of Fitbit Versa 2 data on Android. *Electronics* 9, 9 (2020), 1431. https://doi.org/10.3390/electronics9091431

[264] J. Zhang, D. Li, R. Dai, H. Cos, G. A. Williams, L. Raper, C. W. Hammill, and C. Lu. 2022. Predicting post-operative complications with wearables: A case study with patients undergoing pancreatic surgery. *IMWUT* 6, 2 (2022), 1–27. https://doi.org/10.1145/3534578

[265] Q. Zhang and Z. Liang. 2017. Security analysis of Bluetooth Low Energy based smart wristbands. In *Proceedings of the International Conference on Frontiers of Sensors Technologies (ICFST '17)*. IEEE, 421–425. https://doi.org/10.1109/ICFST.2017.8210548

[266] X. Zhou, A. Krishnan, and E. Dincelli. 2021. Examining user engagement and use of fitness tracking technology through the lens of technology affordances. *Behaviour & Information Technology*. Published Online, April 17, 2021. https://doi.org/10.1080/0144929X.2021.1915383

[267] M. Zimmer, P. Kumar, J. Vitak, Y. Liao, and K. C. 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 (2020), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442

[268] N. Zufferey, M. Humbert, R. Tavenard, and K. Huguenin. 2023. Watch your watch: Inferring personality traits from wearable activity trackers. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*. 193–210. https://www.usenix.org/conference/usenixsecurity23/presentation/zufferey

[269] N. Zufferey, K. Salehzadeh Niksirat, M. Humbert, and K. Huguenin. 2023. "Revoked Just Now!" Users' behaviors toward fitness-data sharing with third-party applications. *Proceedings on Privacy Enhancing Technologies* 2023, 1 (2023), 47–67. https://doi.org/10.56553/popets-2023-0004

[270] C. Zuo, H. Wen, Z. Lin, and Y. Zhang. 2019. Automatic fingerprinting of vulnerable BLE IoT devices with static UUIDs from mobile apps. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*. ACM, 1469–1483. https://doi.org/10.1145/3319535.3354240

Received 22 December 2022; revised 5 November 2023; accepted 31 January 2024