Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours

Sandra Gabriele
York University
Toronto, Canada
sandrag@yorku.ca

Sonia Chiasson
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

ABSTRACT

Personal data collected by fitness trackers can leave users open to security and privacy threats, often without their knowledge. Using an online survey with 212 fitness tracker users, we asked questions to understand participants' knowledge, attitudes and behaviours related to security and privacy, associated with the use of their fitness trackers. We found that users do little to protect their data. While they seem confident about the type of data being collected, they are unsure about how it is being used. Understandably, users are more comfortable sharing their data with friends and work colleagues. We also found that users differentiate between the types of data they are willing to share, suggesting a need for improved sharing preferences. When considering scenarios describing data uses with security and privacy implications, participants recognized that many scenarios were *plausible* but frequently felt that the scenarios were *unlikely* to occur. Overall, our findings lead us to believe that fitness tracker users require a greater awareness of the collection, ownership, storage, and sharing practices related to the tracking of their data.

Author Keywords

Fitness trackers, privacy, online survey, data sharing

CCS Concepts

•Security and privacy → Human and societal aspects of security and privacy;

INTRODUCTION

According to an American College of Sports Medicine survey [40], the top fitness trend for 2019 is wearables, including: fitness trackers, smart watches, heart rate monitors, and GPS tracking. A recent study with 4,109 Canadian adults found 25% of participants reported owning a wearable or smart medical device and use it regularly, mainly to track physical activity, nutrition and sleep patterns [29]. Gary Wolf, the first person to use the term "the quantified self" sees self-tracking as a tool for discovery. Wolf explains that those who track their fitness activities are interested in customizing training to suit their own body types and goals, understanding their own strengths and weaknesses, and revealing their unrealized potential [43]. While fitness trackers have proven useful to increase self-awareness and encourage behaviour change, they are also useful in medicine, to monitor patient health [8]. However, there is a trade-off. The personal data collected by these devices can leave users open to security and privacy threats, often without their knowledge.

The data collected by fitness trackers is especially personal, consisting of information provided by the user (e.g., birth date, weight, pictures or social information), biometric or movement data (e.g., heart rate, steps, GPS coordinates) and contextual data used by the system (e.g., timestamps, unique user ID). Aside from the highly personal nature of the data, of concern is the sheer amount of data collected, continually. When collected over time, aggregated, and combined with other data, the resulting profile can paint an accurate representation of a person's identity and their habits, leaving them open to privacy violations that may cause them harm [1]. However, fitness tracker users are likely unaware of the privacy implications of how the data could be misused, when collected over time or when associated with other information [26].

Recent events highlight potential risks. In 2018, Strava uploaded a heat map of users' anonymous and aggregate fitness tracking data on their website [30]. The emerging usage patterns revealed the locations and habits of troops using their fitness app at secret military bases in Iraq, Afghanistan and Syria [30]. The same year, hackers gained unauthorized access to data, breaching fitness tracker accounts of 150 million MyFitnessPal users [25]. They accessed names, usernames, and passwords that could be used to obtain more sensitive personal information or to break into other accounts [25]. A recent news item [35] reported on the sharing of fitness data via an employer-sponsored wellness program. An employee who had experienced a heart attack was being monitored by his employer, who commented on the employee's increased physical activity. Reportedly, the employee did not find this intrusive; however, it raises privacy questions about how much personal information employers should have about their employees.

Do users willingly or unknowingly share their fitness tracker data? Are they comfortable with this data collection and sharing? Do they understand the potential implications of this type of data collection and sharing? We conducted an online survey with 212 fitness tracker users to understand their knowledge, attitudes, and behaviours related to security and

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376346

privacy. The results demonstrate users': 1) lack of knowledge of the potential implications associated with the collection of their data; 2) complex attitudes towards risks in terms of their own fears, likelihood that threats will occur, the consequences of breaches, and confidence that developers have protected users' privacy and security; and 3) preferences for sharing specific types of data with different groups of people.

BACKGROUND

Researchers have explored users' knowledge of data collection and their perceptions towards privacy and security within a variety of digital contexts. Most studies are concerned with either web/online contexts [4,5,7,10,18] or mobile technologies [23,38]. Some researchers have examined security and privacy more broadly, by looking at a range of existing and emerging technologies [34,39], while others have focused on digital apps [38,41] and social media contexts [12]. Less studied are IoT devices [6], wearables [11,16,26,33], and fitness trackers [1,3,22,31,32,36,42,44].

In the literature review, we distinguish between wearables and fitness trackers. Studies focusing on fitness trackers refer to wrist-worn devices and the fitness-specific data they collect. Wearables include all other tracking devices using sensors to collect a variety of personal data. Except where specified, the rest of this section refers to fitness trackers.

Wearables

Users express a variety of concerns with the security and privacy of their personal data associated with wearable devices. Studies have examined user concerns within the context of: the type of device, type of sensor, and the collected data [26]; the sharing of physiological, psychological and behavioral data collected by sensors [33]; the perception of risk with various data and user preferences for managing their privacy while wearing a lifelogging camera [16]. Within the context of healthcare, cardiac patients and caregivers expressed interest in the benefits of using wearables for health monitoring, but they were not yet willing to adopt these devices [11].

Fitness trackers

Existing research in the area of security and privacy related to fitness trackers includes investigating users' concerns, use and sharing of data and protection strategies [3,22,42,44]; an assessment of the sensitivity of their data [44]; the valuation of their personal fitness information [42] and knowledge of company data collection policies [3,42]; their perceptions of the benefits and drawbacks of using fitness trackers [3,22,44]; misconceptions associated with the collection of data [22]; willingness to share sensor data versus derived information (for example, accelerometer data versus step information) [36]; sharing preferences and behaviours of fitness and health information [31]; and examining folk theories – user beliefs and understandings – of what exactly is collected by sensor data and how these guide users to manage their privacy choices [32]. Others demonstrated to users how their identity can be revealed when fitness tracker and online social network data is merged [1].

Knowledge

Data collection practices

Users are generally ill-informed about digital data collection practices associated with fitness and health related wearables [1,22,26,44] and how data can be misused when collected long-term or combined with other data [26]. They are unaware or unsure of what data is collected, how it is used, who owns the data, with whom it is shared [22,42], what is shared and when it is accessed [22], how it is stored [22,42], for how long [22]and how it is anonymized [1].

Trust in providers

Research indicates participants trust the companies collecting their data [3,44] and would not be concerned about their privacy unless they found reason to doubt them [44]. Aktypi et al. [1], noted that at the beginning of their study, users claimed they trust in the companies who collect their data and believe there is a low risk of negative impacts related to its collection. However, during the study, users revealed they were uncertain whether the companies take steps to maintain their anonymity.

Attitudes

Benefits of tracking

The capacity of digital devices to sense and collect various kinds of personal data has resulted in a culture of self-tracking, a phenomenon adopted by health and fitness conscious individuals, worldwide. Fitness tracker users report several benefits from using their trackers [3,22,44].

While users report that they care about their privacy [42], in practice, they do little to protect their fitness data [1,22]. The *privacy paradox*, which explains the contradiction between users' concern for privacy and security and their protection behaviour, is commonly used to describe this contradictory behaviour [27]. However, Gerber et al. [13,19] make a case for the *privacy calculus* (a calculation of the risks and benefit of use) along with other theories related to decision-making to explain contradictions in privacy attitudes and behaviours.

In Lowens and Motti's [22] study, users' deemed wearing a device that tracked health information beneficial to their health and well-being. Zimmer et al. [44] and Alqhatani and Lipford [3] found fitness tracker users report few drawbacks related to wearing a fitness tracker and found, overall, that participants thought the fitness features were useful to them. They found trackers helpful in motivating them, making them more accountable, encouraging them to be more physically active and giving them the ability to monitor their sleep habits. Zimmer et al. [44] found the social features to be the least important aspect. Similarly, Alqhatani and Lipford [3] reported sharing on social networks sites was not helpful for users.

Privacy concerns

The literature shows variety in the level and type of privacy concerns. Zimmer, et al. [44], found users of fitness trackers have minimal privacy concerns but users would be concerned if data beyond their steps was shared [44]. In line with the *privacy paradox* [27], Vitak, et al. show that users express concern about privacy in relation to their fitness trackers but they demonstrate a lack of concern about what they actually share [42]. Motti and Caine [26] revealed that user concerns are not necessarily related to the kind of wearable, but instead are focused on the type of data the sensors collect. More specifically, users showed the most concern with audio and video recording followed by location data and data that could be exposed by displays. They were less concerned about collecting steps and heart rate because this type of data was deemed as less of a privacy risk. Schneegass et al. [36] found users are not aware of the differences between raw sensor data and derived information. The authors argue that if users understood the implications and were concerned about protecting their data, they would recognize the great amount of information that can be gleaned from the raw data.

Lowens et al. [22] observed that users have an incomplete understanding of privacy risks associated with wrist-worn wearables and, at the same time, their privacy concerns vary. Those concerned about their privacy were also aware of risks associated with their data but are still willing to give up confidentiality. Users were also concerned about lack of control they have over how their data is used.

Behaviour

Sharing data

Sharing preferences are dynamic and change over time [24, 31]. In a 2012 study by Prasad et al. [31], participants were given a Fitbit to use for one week. These new users shared less demographic information than sensed information, and, with some of the information, less with family and friends than with strangers. None of the participants had ever used a fitness tracker before the study, although 11 had previously used a pedometer. We would argue that while the results are applicable to new users, this does not necessarily reflect behaviours of long-time users.

In another study, Raij et al. [33] report that participants expressed concerns with sharing sensor data that discloses conversations, commuting habits, and psychological states. Contrary to the findings of Prasad et al., they found that sharing data with the general public was of significant concern to participants; participants were less concerned with sharing data with other study participants and researchers, regardless of whether their identity was shared with the data.

Taking action

Social factors and concerns relating to self-image can affect user behaviour. Alqhatani and Lipford [3] found social norms and self presentation influence how users make privacy decisions about their fitness tracker data.

Other factors, beyond the control of users (specifically, the design of devices and the systems supporting them) also contribute to users' privacy behaviours. Rader and Slaker [32] concluded that users have difficulty reasoning about privacy because interfaces tend to obscure the complexities involved in data collection [32]. Usability concerns associated with corporate privacy policies are common across digital platforms and devices. Alqhatani and Lipford [3] reported that many of their participants were unaware of their privacy settings and those who were aware had not changed them since setting up their device.

Privacy policies

Research in usable privacy indicates users rarely read privacy policies because they are lengthy, complicated, use legal language [9], and do not facilitate decision-making based on user privacy concerns [17]. Others suggest that overexposure to online privacy notices and reports of data breaches may cause people to “almost ignore them” [4]. Aktypi et al. [1] found that fitness tracker users would feel more secure if the privacy terms and conditions were an industry-government collaboration, and if there was some accountability for privacy violations. However, users were also apprehensive in abandoning the use of their device, even after having read a privacy policy, because of the substantial financial investment already made in purchasing the device.

Despite privacy laws, compliance is inconsistent. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) requires that manufacturers provide privacy policies describing the existence, use, and disclosure of any data collected, and provide both the policy and data upon request [28]. Hilts et al. [15] asked Canadian participants to wear a fitness tracker for 2 months, then make a formal request to the manufacturer. They asked (i) questions about the company's data sharing policies and (ii) for access to all data associated with their accounts. Participants sent an initial request and a reminder, but only 5 of the 9 companies replied formally, and only one company (Apple) fulfilled all requests.

Gaps and opportunities

The literature studying users' concerns about sharing *types of data* collected by fitness trackers is limited. Users generally do not believe fitness tracker data is sensitive [3, 44]. One of the few studies specifically studying fitness tracker users' concerns (as opposed to wearables in general) [44] confirms research on wearables; users would be concerned if the tracker collected or shared information other than steps, such as personal identifiers or location data. We did not find any studies that show substantial detail for fitness trackers. With these studies in mind, we ask users what fitness-related data types they would be most comfortable sharing by providing a detailed list of data types in the three categories listed in Fitbit's sharing preferences (personal, graph and statistical data).

Furthermore, studies examining sharing behaviour with fitness trackers [21, 31] and sensor data [33] have studied only a limited number of *recipients* with whom participants might knowingly or unknowingly disclose data. An exception was a study conducted by Alqhatani and Lipford [3]. Using interviews, they uncovered audiences with whom users share their fitness data (friends, family, strangers, physicians, financial incentive programs and co-workers). Our study, extends this research by using a survey tool to systematically ask participants how comfortable they would be sharing each type of data with six groups of recipients. This allowed us to quantify the responses, and gain insight into with which group they are most and least comfortable sharing their fitness data.

Previous research [44] suggests that a plausible reason why users have a limited understanding of risks and threats associated with sensor data is because no one they know has experienced a breach. However, recent media reports of incidences and data breaches [25, 30, 35] are changing this landscape. Aktypi, et al. [1] used scenarios to present plausible risks, based on users' sharing activities. They developed a tool to educate users about how their fitness data can be used against them when combined with data from online social networks. Users found the threat scenarios credible and intriguing. Our study builds on this work by looking at both whether users believe threats to be *plausible* and whether they think these are *likely to occur*. If users think that threats are unlikely, then they have little incentive to protect themselves and this may partially explain why they take few protective actions.

METHODOLOGY

Our study was reviewed and cleared by our Research Ethics Board. In January 2019, we conducted an online survey with fitness tracker users to determine their: (1) knowledge of data collection and usage practices, and knowledge of the plausibility and likelihood of privacy threats; (2) attitudes towards security and privacy breaches; (3) security and privacy behaviours, and sharing preferences.

Recruitment

We recruited participants and managed the study through Prolific[1], an online crowdsourcing platform specifically for research studies, and hosted the surveys on Qualtrics[2]. International[3] participants were pre-screened using a 5-question survey that took approximately 2 minutes to complete. Of the 508 participants who completed the pre-screen survey, 285 met the criteria (18+ years of age, felt comfortable completing a survey in English, and regularly used a fitness tracker). A total of 252 responded to the full survey, which took approximately 20 minutes to complete. We excluded data from 40 participants whose responses to overlapping demographics questions differed between the pre-screen survey and the full survey, or whose responses were incorrect for one or more of the four attention check questions. In the end, we had a total of 212 valid surveys. We paid participants £ .17 GBP for the pre-screen survey and £ 1.67 GBP for the full survey.

Survey Structure

Through several iterations of the survey structure, we conducted pilot tests with 6 participants to identify technical concerns, verify the appropriateness of wording, and test completion time. The final survey has 100 questions, including 4 attention-check questions. It consisted of "yes/no/don't know", multiple choice, and 5-point Likert scales questions, and 6 open-ended text questions. The questionnaire is available in the accompanying supplementary material. We asked about:

Demographics: Participants' age, education, work experience, expertise, and brand of fitness tracker.

Confidence in knowledge of Data Collection and Use: Participants' confidence in their knowledge of what is collected by their fitness trackers and how it is used.

Knowledge of Potential Threats: The *plausibility* and *likelihood* of 20 scenarios. Based on potential threats suggested in the literature and news reports of actual breaches, we developed scenarios describing potential risks and threats relating to fitness trackers. The scenarios were briefly described and, similar to Rice and Bogdanov's [34] survey examining corporate data collection and usage practices, participants answered 'yes', 'no', 'don't know' to whether the scenario "could possibly occur" and whether it "would likely occur". We wanted to force participants to take a position and a Likert scale would have been more difficult to interpret. For example, the first scenario described: *An employer fired an employee because they could tell from the employee's fitness tracker data that she was coming to work late, leaving early, and taking multiple unwarranted breaks throughout the day*. Furthermore, we believed it important to ask participants' opinion of both plausibility and likelihood to capture the subtlety between the two. For "possible", we wanted to know if they thought scenarios were credible and with "likely", whether scenarios could conceivably occur.

Attitudes: Security and privacy concerns associated with fitness tracker use. Skirpan, et al. [39] used a set of 6 psychological factors to characterize risk perception. We used some of these factors to frame questions eliciting user opinions surrounding the threats associated with fitness trackers: fear of specific threats, the likelihood of the threats occurring, the severity and potential consequences of breaches, and participants' confidence that developers have adequately protected against breaches.

Behaviours: Current security and privacy practices relating to their fitness tracker, their comfort level sharing fitness tracker data with various recipients, and the type of data they would share with whom. We asked about 6 different sharing recipient groups and 14 different types of data based on data collected and represented by Fitbit devices. We considered a broader set of features but found that Fitbit settings were included in most other devices and apps. Fitbits are the most popular fitness tracking devices, so these provided us a baseline that would be familiar to a wide range of users.

ANALYSIS

Given our methodology, all of our data is self-reported and as such represents participants' subjective perspective. Our survey was designed to capture the knowledge, attitudes and behaviours of fitness tracker users. Because of the exploratory nature of the survey, we primarily used descriptive statistics and graphic representations to summarize responses and draw insights. We use non-parametric statistical methods (Friedman Rank Sum Test, the Nemenyi post-hoc test, and the Wilcoxon Signed-rank Test) for within-group comparisons.

RESULTS

Demographics

113 international participants identified as female, 98 as male and 1 identified as other. They ranged in age from 18 – 73 years old. In terms of education, 55% had completed a university degree, 10% had some university education and 35%

[1] https://prolific.ac/

[2] https://www.qualtrics.com/research-core/survey-software/

[3] Prolific recruits participants from the United Kingdom, the United States, Poland, Canada, Portugal, Italy, Germany, Australia, Spain, Mexico and other countries

Table 1. Number of participants using each fitness tracker brand

	Tracker Brand	Total	Percentage
1	Fitbit	75	36%
2	Apple	36	17%
3	Samsung	26	12%
4	Xiaomi	21	10%
5	Garmin	18	8%
6	Other brands	31	14%
7	Smartphone apps	5	2%

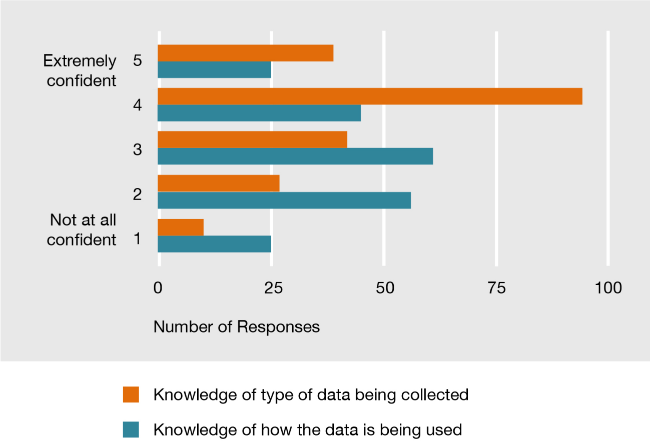

Figure 1. Perceived knowledge of fitness tracker data collection and use, reported using a 5-point Likert scale.

had not attended university. Participants used a variety of fitness trackers brands or digital apps meant for tracking fitness directly from their smart phone (Table 1).

Knowledge

Data collection and use – On a 5-point Likert scale (from 1, not at all confident to 5, extremely confident) participants rated their knowledge of 1) the types of data being collected by their fitness tracker; and 2) how the data is being used. Figure 1 demonstrates that participants feel fairly confident in their knowledge of what data is collected but are less confident in how the data is being used. The responses in both questions follows a relatively normal distribution, also highlighting that a fair number of participants use these devices with no clear understanding of what they collect or why.

Potential threats – For each of the 20 scenarios, we asked participants to select "yes", "no", "don't know" to indicate: (i) the *possibility* that a scenario *could* occur, and (ii) the *likelihood* that a scenario *would* occur.

A heat map of "yes" responses (Figure 2) shows that while participants thought several scenarios were plausible, they also believed many of them unlikely to occur. This skepticism suggests that participants may implicitly trust those responsible for data collection and sharing, underestimate the ease with which some of these scenarios could occur, or are displaying evidence of the optimistic bias effect by overestimating positive outcomes [37].

Possible	Likely	Scenarios
94	83	Tracked and mapped running routes, provided an accurate picture of a user's movements.
91	83	Based on running data, an advertiser targeted ads for a specific brand of running shoes.
87	71	Insurance companies offer discounts based on an individual's health and fitness information.
86	60	Heart rate data combined with video footage at a crime scene helps identify a murder suspect.
85	52	A hacker could tell the location and discern the user activity based on fitness tracker data.
79	58	Life insurance companies cancel coverage of unhealthy people, based on fitness tracker data.
74	50	Police officers used fitness tracker data as evidence to arrest someone for a crime.
71	27	An employee was fired based on tracker data showing fitness activities during work hours.
70	28	A hacker denied the user access to his own account until he paid a ransom.
68	44	Data was intercepted by hackers when transmitting from the fitness tracker to the server.
63	37	Collection of fitness tracker caused identity theft, profiling, stalking and extortion.
61	21	Sleep data suggesting poor cognitive/mental health are used against a job applicant.
58	29	Fitness tracker data provided a burglar with the location, number of floors and when a user would be home.
58	28	Border control officers denied a man entry based on location data showing countries he visited previously.
48	19	A user's sexual activity was revealed based on the data showing changes in heart rate and intensity of movement.
46	17	Based on fitness data, city council denied citizens with a high level of fitness, a new fitness facility.
42	15	Data about an employee's menstrual and ovulation cycles were used by an employer for human resource planning.
41	10	An adoption agency denied a couple a child a based upon fitness tracker data suggesting an unhealthy lifestyle.
32	16	A fitness tracker user was identified simply by their gait (walking pattern).
21	10	Fitness tracker data was used to discriminate against users based on race, religion and gender.

Figure 2. Percentage of participants who responded "yes" to whether each scenario describing threats associated with fitness data collection was *possible* and *likely*.

Attitudes

Security and privacy concerns – As summarized in Figure 3), participants used a 5-point Likert scale to react to five concerns: (T1) data shared without permission, (T2) data tampering, (T3) account hijacking, (T4) data used against you, (T5) identity theft due to data breach. For each they indicated:

- their fear of each threat;
- the likelihood that the threat would occur;
- the severity of the consequences, should the threat occur;
- their level of confidence that developers had protected against the threat.

Fearfulness – The median responses to Concerns T1 – T5, respectively, were 3, 2, 2, 3, 3 (where 1 is "not at all fearful" and 5 is "extremely fearful"). Participants rated their fearfulness at the lower-to-mid points of the Likert scale for most concerns. A visual scan of an area plot confirms this result, showing few

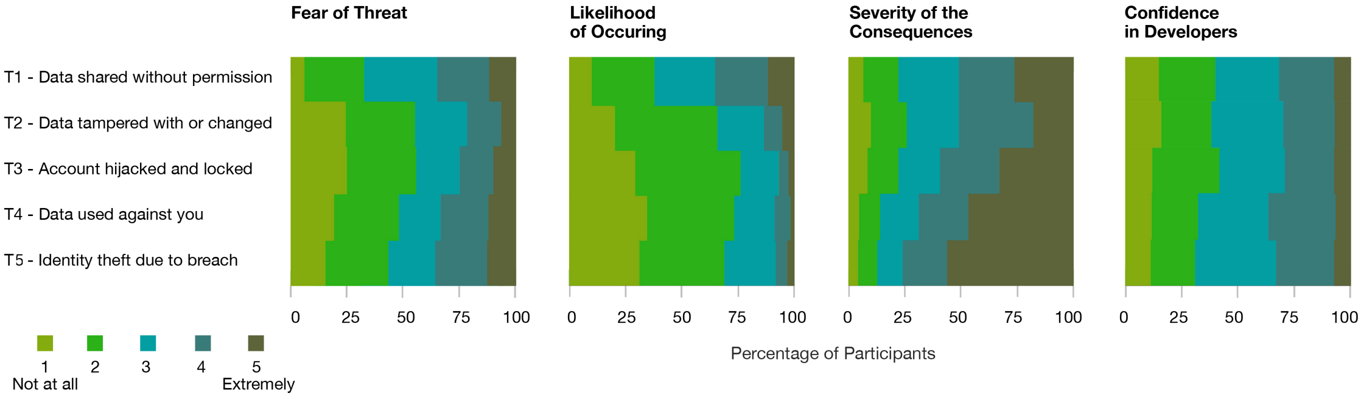

Figure 3. Likert scale responses for participants' reaction to five specific concerns, based on four different measures.

responses for "extremely fearful"(Figure 3), although a distinct pattern emerged for T1, with most participants expressing some fear about unauthorized data sharing.

Likelihood that it will occur – The median responses to Concerns T1 – T5, respectively, were 3, 2, 2, 2, 2 (where 1 is "not at all likely" and 5 is "extremely likely"). Participants rated the likelihood that the situations/threats will occur towards lower points of the Likert scale for most concerns. A visual scan of an area plot shows very few responses for "extremely likely"(Figure 3). This result aligns with responses to the scenarios above. We again notice a distinct pattern for T1, with participants feeling that it is at least somewhat likely that their data is being shared without their permission.

Severity of the consequences – The median responses to Concerns T1 – T5, respectively, were 4, 4, 4, 4, 5 (where 1 is "not at all severe" and 5 is "extremely severe"). The responses, most of which occur between the mid to high points of the scale, suggest that participants felt that the consequences were quite severe for all threats. A visual scan of the plots suggests that participants were most concerned about T4 and T5, both questions implying a direct negative consequence for the user.

Confidence in developers – The median responses to Concerns T1 – T5, respectively, were 3, 3, 3, 3, 3 (where 1 is "not at all confident" and 5 is "extremely confident"). Participants rated their confidence in developers at the mid-point of the Likert scale for all concerns. The area plot shows fewer responses at the two extremes ("not at all confident" and "extremely confident") and a relatively even distribution across the mid-points of the scale (Figure 3), suggesting ambivalence or uncertainty that developers have safeguarded their privacy and security.

Interest in seeking out more information – On a 5-point Likert scale, from 1 - "not at all interested" to 5- "extremely interested") participants indicated their interest in seeking out more information about security and privacy in relation to their fitness trackers. The question was posed both at the beginning of the questionnaire and then again at the end. A Wilcoxon Signed-rank Test showed a significant difference in interest ($W = 860.5, Z = -7.80, p < .001, r = 0.54$). The median scores increased from 3 to 4 between the two iterations, indicating that participants' interest was heightened by completing the survey (Figure 4).

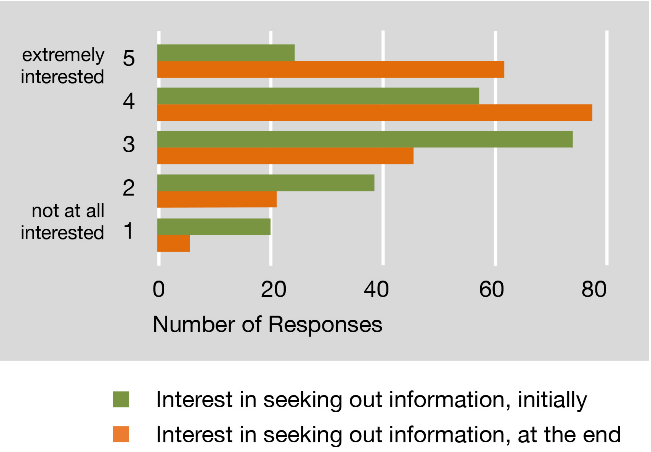

Figure 4. Interest in security and privacy information

Behaviours

Current security and privacy practices – Participants responded to five questions about how they manage their fitness tracker security and privacy with "yes", "no" or "don't remember". Responses are shown in Figure 5. The results show that, in general, most participants do not take steps to ensure their data is secure and private. They do not *change the default security and privacy settings*, do not *read the terms and conditions*, and do not *read the privacy policy*. Only half of participants reported *setting their preferences for sharing data*.

Data sharing with recipients – As summarized in Figure 6, participants indicated their comfort level sharing their data with various recipients. Responses used a 5-point Likert scale, from 1 - "extremely uncomfortable" to 5 - "extremely comfortable". It is noteworthy that very few participants were 'extremely comfortable' sharing data with any recipient. However, participants were most comfortable sharing with the tracker itself and their friends, followed by colleagues, then employers, the public, and insurance companies. They were least comfortable sharing with advertisers.

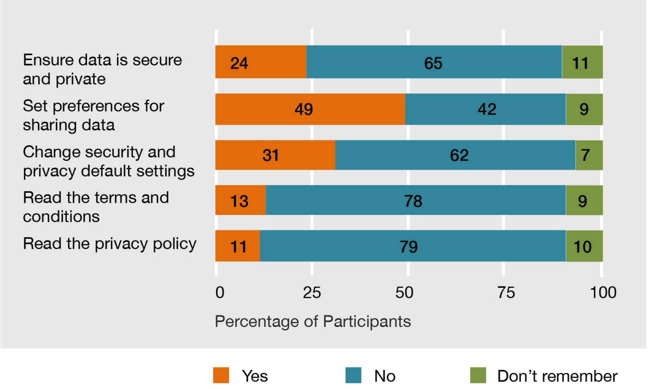

Figure 5. Percentage of participants who reported doing each security and privacy behaviour.

A Friedman rank sum test revealed a significant difference among the recipients with whom participants were comfortable sharing data, $(\chi^2(2) = 619.09, df = 6, p < .001)$. Post-hoc testing with Pairwise comparisons using Nemenyi multiple comparison test with q approximation for unreplicated blocked data revealed significant differences between all pairs $(p < 0.05)$, *except* for: [Fitness Trackers and Friends], [Employers and the General Public], [Employers and Insurance Companies], [General Public and Insurance Companies], and [Insurance Companies and Advertisers].

Types of data shared with recipients – Participants were presented with a grid and checked the individual types of data they are willing to share with each type of recipient. We used Fitbit fitness tracker data items categorized under "Personal Data", "Graph Data" and "Statistical Data", and adapted vague or Fitbit-specific terminology (for example, "Badges, Awards, Trophies" was changed to "Milestones"). The summary (Figure 7) shows that, in general, participants were relatively comfortable sharing most types of data with friends, but that their comfort level quickly decreases as the recipient becomes further removed from the participant.

Considering personal data, participants are generally comfortable sharing their gender, height and birthday with several groups, and are more reluctant to share their pictures, location and friends list. For graph data, participants seem to be more comfortable sharing the Steps, Distance, Floors Graph than their Sleep or Weight Graphs. Participants were mostly comfortable sharing aggregate statistical data with friends, but less so with the other recipients. They appear to attribute similar sensitivity to all three types of statistical data.

INTERPRETATION OF RESULTS

We draw the following seven main insights from our results.

Knowledge

1. Users believe they know what's collected but are unsure how it's used – Participants feel quite confident they know what data is being collected by their fitness trackers but they are less confident of how the data is used. Given that most also do not read their tracker's privacy policy or its terms and conditions, a larger concern arises: do users really know the extent to which their data is collected?

2. Users' understanding of possible threats is limited – Participants thought many of the threat scenarios were possible, but they were less inclined to believe that these would actually occur. Of the top 4 scenarios where participants indicated they were both highly likely and highly possible, three scenarios were situations that had actually occurred and users may have seen these reported in the news: (i) Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of users' movements [30], (ii) Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual's health and fitness information [8] (iii) Fitness tracker data linked to time stamped video footage was used in a murder investigation to arrest a murder suspect [14]. The fourth represents a situation that commonly occurs with other technologies: (iv) An advertising agency targeted specific brands of running shoes suited to a long distance runner. Participants' knowledge about threats is heightened in instances where data breaches have actually occurred and have been reported, or in instances where parallel threats occur with other technologies.

Attitudes

3. Users are interested in seeking out more information on security and privacy – Participants showed an increased interest in learning additional security and privacy information after having completed the survey. This result could plausibly suggest that given some information to raise their awareness, users have an interest in finding out more. However, we must qualify this response because others have noted that users generally became more concerned about privacy simply as a result of their participation in a study which primes them to consider the topic [22].

4. Security and privacy concerns are inconsistent – Participants are not very fearful of security and privacy threats, and believe them unlikely to occur. However, if these actually occurred, participants believe the consequences would be quite severe. This result aligns with Krasnova et al.'s [20] finding that it is the perceived *likelihood* rather than the perceived *damage* of privacy breaches plays a more important role in the formation of online privacy concerns. At the same time, our participants were ambivalent about their confidence in the security protections provided by developers. This lack of confidence may be a reflection of the high number of recent media reports about data breaches exposing personal information.

Behaviours

5. Users take few protective actions against potential threats – Participants reported taking few steps to protect themselves from privacy and security threats. This confirms Zimmer, et al.'s [44] study that found many participants had not checked their privacy settings since the initial setup of their device. Those who did adjust settings tended to further limit what they shared.

6. Users are most comfortable sharing with friends – Participants indicated that they are most comfortable sharing

			Fitness Trackers	Friends	Work Colleagues	Employers	General Public	Insurance Companies	Advertisers
Sharing Data	Not at all Comfortable	1	2	7	19	34	35	42	56
		2	9	12	25	31	30	26	23
		3	28	16	21	17	22	19	15
		4	41	46	25	14	8	8	4
	Extremely Comfortable	5	20	19	9	4	3	5	2
	Median Score		4	4	3	2	2	2	1

Figure 6. Percentage of participants selecting each comfort level for sharing data with various recipients, using a 5-point Likert-scale, ordered by least to most comfortable recipient. Darker cells indicate higher percentages of respondents in those cells.

		Friends	Work Colleagues	Employers	General Public	Insurance Companies	Advertisers	Not comfortable sharing with anyone
Personal Data	Gender	92	83	79	75	75	67	5
	Height	86	69	62	54	58	51	13
	Birthday	89	64	51	29	41	25	10
	Pictures	73	31	10	8	8	6	27
	Location	61	26	15	5	10	8	38
	My Friends List	56	18	8	7	7	6	44
Graph Data	Steps, Distance, Floors Graph	78	46	32	27	30	26	21
	Time Active Graph	66	37	27	22	27	25	32
	Calories Intake and Burn Graph	60	33	23	18	23	19	38
	Sleep Graph	47	23	19	18	19	18	52
	Weight Graph	38	19	17	15	17	16	61
Statistical Data	Average Daily Step Count	78	48	33	30	33	27	20
	Lifetime Steps, Distance and Floors	77	46	33	31	32	26	22
	Milestones	80	45	31	28	28	25	18

Figure 7. The percentage of participants willing to share each type of data with each recipient. Darker cells represent a higher percentage of participants willing to share.

with the tracker itself and their friends, less so with work colleagues and employers, and least comfortable sharing with strangers (the public, insurance companies and advertisers). Interestingly, participants are more comfortable sharing with the general public (anyone) than with advertisers. This may be attributed to the persistent and common practice of data sharing that occurs with other types of media.

7. Users distinguish which data they are willing to share with whom – Participants made distinctions in terms of the type of data they were willing to share with each recipient. Overall, they are willing to share information with those who are closest to them. They are comfortable sharing demographic data (Gender; Height; Birthday), with a greater number of groups, but not information that may be more revealing or more personal in nature (Pictures; Location; Friends List). Demographic data can be seen as being rather generic, whereas, pictures and friends lists could more easily be attributed to or used to identify a specific person. For graph data, participants were willing to share data focusing on their fitness accomplishments (Steps, Distance, Floors Graph; Time Active Graph; Calories Intake and Burn Graph) but less willing to share non-fitness related data that is more intimate or sensitive in nature (Sleep Graph; Weight Graph). Participants appeared to be most comfortable sharing statistical data (Step Counts, Milestones) with friends. Participants did not distinguish between the individual types of statistical data.

DISCUSSION

Our results suggest that users' knowledge, behaviours and attitudes towards security and privacy are complex, not always rational, often contradictory, and can be attributed, in part, to the opaque and inaccessible privacy practices of device manufacturers.

Addressing Gaps

In our literature review, we identified several gaps related to users' understanding and use of fitness trackers. This study was intended to partially address these gaps.

Data sharing and recipients

Previous work by Prasad et al. [31] studied novice users' sharing preferences, but it is unclear whether their results hold for more experienced users. A study by Lowens et al. indicated users want granular control of their data [22]. In Alqhatani et al. [3]'s study, participants were not asked about specific recipients but, rather, these emerged through the interview process. Using our survey instrument, we extend the research in this area by quantifying sharing preferences and providing detailed information about what users are willing to disclose to the groups of recipients for specific data types. We found clear relationships between these two factors: users have distinct sharing preferences for different data and different recipients.

Understandably, users are most comfortable sharing with those closest to them. Interestingly, they are also comfortable sharing with the fitness tracker itself and by extension the device manufacturer. This suggests that they are not aware of harm that could come to them simply by having their data collected. They are least comfortable sharing with advertisers. This result is likely because users are familiar with business models that use advertising to generate revenue and understand that their online activity makes them a target for such behavioral tracking. It might also be explained by the *fuzzy boundary heuristic* which describes how people are uneasy knowing their information is being shared with a third-party [19].

This study also shows that users value types of data differently. Users were more selective in sharing personal/identifiable and sensitive fitness data than in sharing aggregate (and perhaps, seemingly more anonymous) data. We believe that users should be more clearly made aware of available options for setting their sharing preferences so they can better manage their fitness data. Furthermore, we identified a need for easily accessible and more granular options for what users can share and with whom.

Knowledge of threats

We noted a literature gap relating to knowledge of how much users understood about the risks and threats affecting their fitness data. Our study is the first to explore scenarios in the context of fitness trackers as a way to consider both the *likelihood* and *plausibility* of threats and note relationships between them. We found that generally users seem unaware how easily fitness tracker data can be manipulated, combined with other data, and used in negative ways. They seem unaware of potential threats associated with the collection of personal fitness data. An effort towards bridging the gap between what users believe is credible and conceivable is essential for developing awareness campaigns or educational materials. It is worth pursuing how information could be shaped to convince users of such threats.

Complex security and privacy behaviours

Privacy attitudes and behaviours are complex, often contradictory, and difficult to explain [13, 19]. Our survey study demonstrates the inconsistencies in users' concerns about security privacy threats associated with the use of fitness tracker. Users are not very fearful of threats, believe them unlikely to happen, but believe the consequences would be severe should they occur. They also exhibited little confidence that developers were ensuring their safety against threats. Participants' lack of concern may partially explain why they reported taking little action to protect their data. They feel safe and are not motivated to act, even knowing a breach could cause significant harm. While researchers typically attribute contradictory behaviours to the *privacy paradox*, one of a number of alternative theories such as the *privacy calculus* might better capture the complexities of the relationship between attitudes and behaviours [13, 19].

Understanding these nuances and working towards supporting fitness tracker users on their own terms with relevant, timely information could help minimize inconsistencies between concerns, attitudes, intent, and actual behaviours.

Recommendations

Based on the results of our study, we recommend designers and developers work towards:

Designing for awareness/education – Awareness and education should consider the context of use and encourage users to take control of their data. Users do not seem to be aware of the potential uses of their personal data. Awareness campaigns or educational materials should focus on the principle of informed consent. Users should understand how enabling specific functionalities and data sharing options impacts what data is collected and how that data may be used/misused, and they should be empowered to specify their preferences. This is especially pertinent with wearable devices such as fitness trackers because of the nature of the personal information collected. Previous research indicates that users' understanding is enhanced when information intended to educate them about the privacy implications associated with the collection of their data is visualized [1, 33, 41], therefore we are optimistic about the benefits of such efforts.

Furthermore, customized notifications could be developed based on the type of activities users engage in most often and the information their tracker discloses. For example, those who habitually follow the same running route at the same time of day could be prompted with information about surveillance and risks involved with having their GPS enabled.

Giving users more control over collection and sharing – Given participants' varying comfort levels with sharing, it is evident that users should be supported in specifying what and with whom they want to share. Users should be able to opt out of collecting particular kinds of data and be able to control sharing for specific people or groups.

While some level of personalization of data types is currently available with sharing settings on most fitness trackers, the choice of recipients is limited. Furthermore, privacy settings are usually accessed by a mobile app or by logging into websites rather than directly from the device, making these settings virtually "invisible" to users. Users need to make a conscious effort to change or update settings.

We recommend designing fitness tracker interfaces to provide flexibility and more granularity by allowing users to select individual recipients with whom to share rather than simply offering general categories such as “friends” and “the public”. From our data, it appears that the flexibility to create custom groups would also be beneficial. We further recommend implementing reminders or nudges prompting users to revisit their sharing preferences from time to time to ensure their settings match their current preferences. Almuhimedi et al. [2] found nudges helped users make better privacy decisions and make adjustments to permissions settings when necessary. They suggest these be personalized according to users’ preferences, configurable so users can decide their frequency, and made salient but not annoying. Given the small screens available on fitness trackers, it is likely infeasible for settings to be changed on the device itself, but the nudges could appear on the device, or it could be possible to turn the device into “private” mode to disallow recording or sharing of data for a specific time.

Designing for timely informed consent – Efforts towards “just in time” information related to sharing and informed consent should be considered, where users provide permission when and where the sharing of their data may be applicable or relevant to them. Ideally, this should be applied without punishing users by blocking them if they do not consent. Given the user interface constraints of fitness trackers, this is a challenging design problem, but one worth exploring.

This study highlights the gaps relating to the security and privacy of new pervasive, interconnected technologies. We must go beyond the functional aspects of human computer interaction and user experience and try to anticipate the unintended consequences of introducing new technologies that collect great amounts of personal data. Furthermore, we must consider the larger implications to respect users’ security and privacy by prioritizing these within the design workflow.

Limitations

Our sample may not be representative of the entire population of fitness tracker users. Our participants ranged in age from 18 – 73 , however, 90% were between the ages of 18 – 44 and thus, do not necessarily reflect the views of older users. Our survey collects self-reported subjective responses and may not reflect participants’ actual behaviours. While a questionnaire allowed us to establish trends in terms of knowledge, attitudes and behaviours, adding user interviews might result in more nuanced responses. We also note, for the question about data recipients, we did not specify a separate category for "family" because we thought "friends" (as is the norm with social media accounts) implied the inclusion of those related to users. Also absent from the list of potential recipients are physicians.

CONCLUSIONS

Our survey results have provided an understanding of what fitness tracker users know about security and privacy practices and their attitudes and behaviour associated with using their devices. Users expressed confidence in their knowledge of what their fitness tracker collects, yet they were unsure how this data was being used or what types of threats may result from its collection. While they thought some threats were plausible, they believed them to be unlikely and, as such, users were not fearful and reported taking little action to protect their personal data. They did, however, have distinct preferences for sharing specific types of data with different groups of people. Extending previous research in this area, our Likert scale questions provided nuanced responses where participants expressed their comfort level sharing with each type of recipient. The study has revealed the importance of attending to individual knowledge, attitudes and behaviours. Overall, our findings lead us to believe that fitness tracker users require a greater awareness of the collection, ownership, storage, and sharing practices related to the tracking of their data.

ACKNOWLEDGMENTS

We thank our study participants and paper reviewers for their time. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair and Discovery Grant.

REFERENCES

[1] J. R. C. Aktypi, A.and Nurse and M. Goldsmith. 2017. Unwinding Ariadne’s identity thread: Privacy risks with fitness trackers and online social networks. In *Multimedia Privacy and Security*. ACM.

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, 787–796.

[3] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. “There is nothing that I need to keep secret”: Sharing Practices and Concerns of Wearable Fitness Data. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*. USENIX.

[4] A. I. Antón, J. B. Earp, and J. D. Young. 2010. How internet users’ privacy concerns have evolved since 2002. *Security & Privacy* 8, 1 (2010).

[5] S. Barth and M. D. T. De Jong. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics* 34, 7 (2017).

[6] J. Bian, K. Yoshigoe, A. Hicks, J. Yuan, Z. He, M. Xie, Y. Guo, M. Prosperi, R. Salloum, and F. Modave. 2016. Mining twitter to Assess the public perception of the “Internet of Things”. *PloS one* 11, 7 (2016).

[7] I. Bilogrevic and M. Ortlieb. 2016. If you put all the pieces together...: Attitudes towards data combination and sharing across services and companies. In *Conf. on Human Factors in Computing Systems*. ACM.

[8] Elizabeth A Brown. 2016. The Fitbit fault line: two proposals to protect health and fitness data at work. *Yale J. Health Pol’y L. & Ethics* 16 (2016), 1–49.

[9] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[10] L. F. Cranor, J. Reagle, and M. S. Ackerman. 2000. Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy* (2000).

[11] A. V. Dhukaram, C. Baber, B.-J. Elloumi, L.and van Beijnum, and P. De Stefanis. 2011. End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust. In *Pervasive Comp. Tech. for Healthcare*. IEEE.

[12] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. J. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, and M. De Choudhury. 2017. What (or who) is public?: Privacy settings and social media content sharing. In *Computer Supported Cooperative Work and Social Computing*. ACM.

[13] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261.

[14] Christine Hauser. 2018. Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing. (Oct 2018). https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

[15] A. Hilts, C. Parsons, and J. Knockel. 2016. Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security. (Feb 2016). https://openeffect.ca/reports/Every_Step_You_Fake.pdf

[16] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 571–582.

[17] C. Jensen and C. Potts. 2004. Privacy policies as decision- making tools: an evaluation of online privacy notices. In *Conf. on Human Factors in Computing Systems*. ACM.

[18] C. Jensen and C. Potts. 2005. Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63, 1-2 (2005).

[19] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[20] H. Krasnova, E. Kolesnikova, and O. Guenther. 2009. " It won't happen to me!": self-disclosure in online social networks. In *Americas Conference on Information Systems*. AIS/ICIS.

[21] L. Lee, J. Lee, S. Egelman, and D. Wagner. 2016. Information disclosure concerns in the age of wearable computing. In *Workshop on Usable Security*. Internet Society.

[22] B. Lowens, V. G. Motti, and K. Caine. 2017. Wearable privacy: Skeletons in the data closet. In *Int. Conference on Healthcare Informatics*. IEEE.

[23] C. Mancini, K. Thomas, Y. Rogers, B. A. Price, L. Jedrzejczyk, A. K. Bandara, A. N. Joinson, and B. Nuseibeh. 2009. From spaces to places: emerging contexts in mobile privacy. In *Ubiquitous Computing*. ACM.

[24] Michelle L Mazurek, Peter F Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. 2011. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2085–2094.

[25] L. Mirabella. 2018. Under Armour announces significant data breach of its MyFitnessPal app. (Mar 2018). https://www.baltimoresun.com/business/under-armour-blog/bs-bz-under-armour-myfitnesspal-breach-20180329-story.html

[26] V. G. Motti and K. Caine. 2015. Users' privacy concerns about wearables. In *Financial Cryptography and Data Security*. Springer.

[27] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs* 41, 1 (Summer 2007), 100–126.

[28] Office of the Privacy Commissioner of Canada. 2018. PIPEDA Fair Information Principle 9 – Individual Access. (Jan 2018). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda

[29] Guy Paré, Chad Leaver, and Claire Bourget. 2018. Diffusion of the digital health self-tracking movement in Canada: results of a national survey. *Journal of medical Internet research* 20, 5 (2018), e177.

[30] R. Pérez-Peña and M. Rosenberg. 2018. Strava Fitness App Can Reveal Military Sites, Analysts Say. (Jan 2018). https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

[31] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. 2012. Understanding sharing preferences and behavior for mHealth devices. In *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 117–128.

[32] E. Rader and J. Slaker. 2017. The importance of visibility for folk theories of sensor data. In *Symposium on Usable Privacy and Security*. USENIX.

[33] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. 2011. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Conf. on Human Factors in Computing Systems*. ACM.

[34] M. D. Rice and E. Bogdanov. 2018. Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices. *Canadian Journal of Administrative Sciences* (2018).

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

[36] Stefan Schneegass, Romina Poguntke, and Tonja 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*. ACM, 523.

[37] Tali Sharot. 2011. The optimism bias. *Current biology* 21, 23 (2011), R941–R945.

[38] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson. 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Conf. on Human Factors in Computing Systems*. ACM.

[39] M. W. Skirpan, T. Yeh, and C. Fiesler. 2018. What's at Stake: Characterizing Risk Perceptions of Emerging Technologies. In *Conf. on Human Factors in Computing Systems*. ACM.

[40] W. R. Thompson. 2018. Worldwide survey of fitness trends for 2019. *Health & Fitness Journal* 22, 6 (2018).

[41] M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt. 2017. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Conf. on Human Factors in Computing Systems*. ACM.

[42] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, and K. Kritikos. 2018. Privacy Attitudes and Data Valuation Among Fitness Tracker Users. In *International Conference on Information*. Springer, 229–239.

[43] G. Wolf. 2010. The Data-Driven Life. (Apr 2010). https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html

[44] M. Zimmer, P. Kumar, J. Vitak, Y. Liao, and K. Chamberlain Kritikos. 2018. "There's nothing really they can do with this information": unpacking how users manage privacy boundaries for personal fitness information. *Info., Comm. & Society* (2018).