USER AWARENESS OF PRIVACY RISKS RELATED TO THE COLLECTION OF FITNESS TRACKER DATA

by

Sandra Gabriele

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF APPLIED SCIENCE

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2020

Abstract

Personal data collected by fitness trackers can leave users open to security and privacy threats, often without their knowledge. We explored whether increasing user awareness of security and privacy risks might prompt users to take action to protect their personal information. First, we conducted an online survey with 212 fitness tracker users to understand participants' knowledge, attitudes and behaviours related to security and privacy with their fitness trackers. We designed information posters based on our results and conducted a second in-person study with 34 participants. Overall, we found users have distinct sharing preferences for specific types of data and for specific recipients; and they exhibit contradictory behaviour. We demonstrate that it is possible to change fitness tracker users' reported privacy behaviours by showing them information posters. Overall, our findings show fitness tracker users require a greater awareness of protection practices and can benefit, if provided with information.

Acknowledgements

First and foremost, I would like to thank my supervisor, Dr. Sonia Chiasson for her dedication and patience, throughout this “adventure”. Without her guidance, this master’s work would not have been possible. She is a consummate scholar and an inspiring mentor.

I would also like to thank the defence committee examiners, Kasia Muldner and Elizabeth Stobert for their thoughtful questions and discussion about this work and the Chair, David Barrera, for presiding over the process.

Finally, I would like to thank my mother, Anna Maria Colucci Gabriele and my father, Domenico Gabriele for encouraging and supporting me in my educational pursuits, throughout my life.

I would also like to thank the Natural Sciences and Engineering Research Council of Canada (NSERC) for funding the research.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

According to an American College of Sports Medicine survey [74], the top fitness trend for 2019 was 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 [54]. 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 [77]. A 2017 survey on physical activity in Alberta, Canada [45] reported that 21% of Albertans own and use a fitness tracker. Among the top three functions considered useful to users who own (or plan to own) are tracking steps, distance and types of activities.

While fitness trackers have proven useful to increase self-awareness and encourage behaviour change, they are also useful in medicine, to monitor patient health [14]. 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 [50].

Recent events highlight potential risks. In 2018, Strava uploaded a heat map of users' anonymous and aggregate fitness tracking data on their website [56]. The emerging usage patterns revealed the locations and habits of troops using their fitness app at secret military bases in Iraq, Afghanistan and Syria [56]. The same year, hackers gained unauthorized access to data, breaching fitness tracker accounts of 150 million MyFitnessPal users [49]. They accessed names, usernames, and passwords that could be used to obtain more sensitive personal information or to break into other accounts [49]. A recent news item [62] 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.

1.1 Research Objectives and Questions

The incidents described above demonstrate the importance of user awareness of the risks associated with the use of fitness trackers, and reveal a need to protect personal data. This prompted us to think about designing materials to inform fitness tracker users about security and privacy. The main objective for this thesis work is to enhance user awareness of the security and privacy risks related to the collection of their fitness data. We conducted two studies in pursuit of this objective.

For the first study, our interest lay in understanding users' knowledge, attitudes and behaviour towards security and privacy with the use of fitness trackers. Three questions guided this study.

Survey-RQ1: Do users willingly or unknowingly share their fitness tracker data?

Survey-RQ2: Are they comfortable with this data collection and sharing?

Survey-RQ3: Do they understand the potential implications of this type of data collection and sharing?

For the second study, we designed and evaluated the effectiveness of information posters designed to make users aware of privacy risks and to promote good safety and security practices. The following three research questions guide our work:

Poster-RQ1: Does presenting information about fitness tracker security/privacy affect users' knowledge, attitude and behaviours?

Poster-RQ2: Does visual design and messaging affect users' knowledge, attitude and behaviours?

Poster-RQ3: Which poster type do users deem most usable?

1.2 Contributions

This thesis contributes several findings related to fitness tracker users' knowledge, attitudes and behaviours.

- Through our survey study, we extend previous literature by providing new insights on sharing preferences and behaviours of fitness tracker users. Users have distinct sharing preferences for specific types of data and for specific recipients, and they attribute different value to different types of data.
- We also provide fitness tracker-specific evidence of the complexities of privacy preferences and behaviours. Users exhibit contradictory behaviour: they are not very fearful of threats, believe they are unlikely to occur but know that they can cause substantial harm.
- Through our poster study, we demonstrate that it is possible to change fitness trackers' reported privacy behaviours by showing them information posters. We also demonstrate a method to evaluate whether privacy intentions translate to reported privacy behaviours.

1.3 Related Publications

Chapter 3 of this thesis has been accepted for publication:

Sandra Gabriele, Sonia Chiasson. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours, SIGCHI Conference on Human Factors in Computing Systems (CHI). ACM, 2020.

1.4 Thesis Outline

In Chapter 2, we examine the literature related to security and privacy with a focus on wearables and fitness trackers. Chapter 3 presents the findings of the survey study, designed to give us an understanding of users' security and privacy knowledge, attitudes and behaviours. Chapter 4 describes the rationale for the design of four prototypes (including two control prototypes). Chapter 5 presents the results of the poster study to determine whether the presentation of privacy information had the potential to affect a change in privacy behaviour. Chapter 6 provides a discussion of the thesis, recommendations, contributions and suggestions for future work.

Chapter 2

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, 7, 10, 18, 36] or mobile technologies [46, 67]. Some researchers have examined security and privacy more broadly, by looking at a range of existing and emerging technologies [61, 69], while others have focused on digital apps [67, 75] and social media contexts [24]. Less studied are IoT devices [9], wearables [21, 33, 50, 55, 59], and fitness trackers [1, 3, 42, 57, 58, 76, 82].

We focus our literature review on topics most directly relevant to users' understanding and attitudes on the privacy and security of fitness trackers. We begin by giving an overview of work with wearables and fitness trackers. Next, we review the literature on user knowledge, attitudes and behaviour in the context of privacy and security. Finally, we discuss the privacy paradox and other theoretical explanations for contradictions in user attitudes and behaviours.

In this literature review, we define *wearables* as devices connected to the body that uses sensors to collect a variety of personal data. We distinguish between wearables and fitness trackers. For the purposes of our work, *fitness trackers* are wrist-worn wearable devices or other wearable sensors specifically collecting fitness-related data. Our literature review primarily focuses on research with fitness trackers. In instances where a particular paper or concept refers to a technology other than a fitness tracker, it is explicitly specified.

2.1 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 [50]; the sharing of physiological, psychological and behavioral data collected by sensors [59]; how users' knowledge and experience help them make privacy decisions [58] and user preferences for managing their privacy while wearing a lifelogging camera [33]. Within the context of healthcare, researchers gauged cardiac patients' interest in monitoring devices designed to manage their care [21].

We first briefly introduce the main research studies relating to wearables used in this review. The more detailed findings for each of these are integrated into later portions of the chapter under different sections, as appropriate.

In 2014, Motti and Caine [50] collected over 2,000 public online commentaries from users and prospective users of wrist mounted and head mounted wearables from 59 online sources. To understand users' privacy concerns, they conducted qualitative analysis on the data. Generally, users were concerned about sensor data compromising privacy but were unaware of how it can be misused.

Raij et al. [59] conducted a user study with 66 university students. 30 of the participants wore a set of sensors which collected continuous data for three days. After three days, they were shown visualizations of their physiological, psychological and behavioural data. The remaining 36 users had no interaction with the sensors or the visualizations. All 66 participants completed questionnaires about their privacy concerns relating to wearables. Comparison of the two groups allowed the researchers to understand if having a stake in the data would affect their concerns about disclosure with different types of data and whether visualizations of the data impacts users perceptions.

Hoyle et al. [33] had 36 undergraduate students wear lifelogging cameras, collecting images for one week, to see how they would manage their privacy. Participants tagged and managed the images taken then answered questions about the saved images. The researchers also collected data through a questionnaire and exit interviews to capture participants' experience and privacy concerns.

In 2011, Dhukaram et al. [21] conducted focus groups and administered questionnaires to gather patient opinions of the BRAVEHEALTH system, a concept for a wearable device to collect physiological data. BRAVEHEALTH would have capacity to monitor, analyze and transmit health data to physicians. Patients expressed an interest in the benefits, but were not yet willing to adopt these devices [21].

2.2 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, 42, 76, 82]; the perception of risk with various data an assessment of the sensitivity of their data [82]; the valuation of their personal fitness information [76] and knowledge of company data collection policies [3,76]; their perceptions of the benefits and drawbacks of using fitness trackers [3,42,82]; misconceptions associated with the collection of data [42]; willingness to share sensor data versus derived information (for example, accelerometer data versus step information) [64]; sharing preferences and behaviours of fitness and health information [57]; 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 [58]. Others demonstrated to users how their identity can be revealed when fitness tracker and online social network data is merged [1]. We briefly describe the main studies relating to fitness trackers that are used throughout the remainder of this chapter.

Lowens and Motti [42] recruited 20 fitness tracker users from a university campus. Using semi-structured interviews, they investigated these fitness tracker users' perceptions of privacy of health related data collected through wearables. The interviews probed about concerns, misconceptions, and perceptions relating to the costs, benefits, and sharing of such data.

Alqhatani et al. [3] conducted 30 semi-structured interviews to investigate fitness tracker user concerns about data disclosure, their sharing practices and the steps they take to protect their data. The researchers used qualitative data analysis primarily to identify participants' sharing goals and the reasons why they choose to share with various recipients.

Zimmer et al. [82] conducted interviews with 33 Fitbit and Jawbone users. They used criterion sampling to ensure that they had participants with different levels of privacy concern and internet skills. Using the theory of Communication Privacy Management as a framework, the researchers conducted qualitative analysis of their data. They sought to understand users' concerns, the benefits and drawbacks of fitness tracker use and the actions they take to manage their data.

Rader and Slaker [58] conducted semi-structured interviews with free listing activities with 30 participants to investigate how folk theories (beliefs and understanding that guide decision-making) influence fitness tracker privacy management. The researchers analyzed the data using inductive coding to identify the types of data discussed by participants and the types of words used to describe each. They also coded for users' understanding of how the fitness tracker tracks the different types of data, and any identified relationships between the different data types. The researchers were then able to visualize these findings through directed graphs and propose that interfaces more explicitly show these relationships.

2.3 Knowledge

2.3.1 Data Collection Practices

Users are generally ill-informed about digital data collection practices associated with fitness and health related wearables [1, 42, 50, 82] and how data can be misused when collected long-term or combined with other data [50]. They are unaware or unsure of what data is collected, how it is used, who owns the data, with whom it is shared [42, 76], what is shared and when it is accessed [42], how it is stored [42, 76], for how long [42] and if it is anonymized [1].

2.3.2 Trust in Providers and Manufacturers

Research indicates participants trust the companies collecting their data [1, 3, 82] and would not be concerned about their privacy unless they found reason to doubt them [82].

Aktypi et al. [1] designed a digital identity tool to show users how their fitness tracker data could be compromised. They interviewed participants and presented the tool, showing them the privacy implications with the collection of their fitness data. Users claimed the tracking device manufacturers' reputation gave them confidence that their data was not at risk. However, they were uncertain whether steps are taken to maintain their anonymity. Aside from raising user awareness, Aktypi et al. believes it is important to inform manufacturers about the potential risks their devices pose. They hope to encourage manufacturers to be proactive in mitigating risks and thus, gain the trust of users.

2.4 Attitudes

2.4.1 Studying User Attitudes and Behaviours

Privacy attitudes and behaviour with the use of digital technologies is complex and often contradictory, as demonstrated in two recent extensive reviews of privacy literature [27, 37]. Gerber et. al. [27] and Kokolakis [37] contribute to privacy research by challenging the *privacy paradox*, a phenomenon popularly used to characterize the dichotomy between privacy attitudes and privacy behaviours (e.g. users express concern about the privacy of their data but do not take action to protect it). They present various alternative theories and heuristics for decision-making to explain these behaviours (these are detailed in Table 2.2 and Table 2.1).

For ease of analysis, both Gerber et al. [27] and Kokolakis [37] operationalize the terms "behaviour" and "privacy" and related concepts. Kokolakis [37] distinguishes *privacy concerns* and *privacy attitudes.* He feels *privacy concerns* can be quite general and not contextual, while *privacy attitudes* are opinions of specific behaviours. Both Gerber et al. and Kokolakis make a distinction between *privacy intentions* (what users say they will do) from *privacy behaviour* (what users actually do). Gerber et al. [27] go further. They believe a multidimensional approach, presented by Dienlin and Trepte [22], can help to dispel the privacy paradox. They found privacy concerns have an indirect effect on behaviour and explain the results of their research: "privacy concerns had an effect on privacy attitudes, which in turn influenced privacy intentions, which finally influenced privacy behavior". In our studies, we categorize security and privacy concerns as attitudes, justifying this by posing questions referring to specific contexts.

2.4.2 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, 42, 82]. In Lowens and Motti's [42] study, users' deemed wearing a device that tracked health information beneficial to their health and well-being. Zimmer et al. [82] 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. [82] 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.

2.4.3 Privacy Concerns

The literature shows variety in the level and type of privacy concerns. Zimmer et al. [82] found users of fitness trackers have minimal privacy concerns but users would be concerned if data beyond their steps was shared [82]. Vitak et al. [76] 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 [76]. Motti and Caine [50] 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. [64] 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. Furthermore, they found users are more apt to share positive information (e.g., training intensity) than information with negative connotations (e.g., stress).

Lowens et al. [42] 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 share their data because of the benefits they receive. Users in Lowen et al.'s study were also concerned about the lack of control they have over how their data is used.

2.4.4 Risk Perception

Recently, Skripan et al. [69] conducted a risk perception study focusing on emerging technologies, based on a classic risk perception experiments [71]. Slovic et al. [71] conducted a series of studies, asking participants to rate various common environmental and health hazards. They asked experts and students to use a risk assessment instrument for ranking (from "very risky" to "not risky"). They found people are more apt to accept risk when the activity is voluntary. They also found experts tend to underestimate risks.

A central focus of risk perception studies is the application of a set of psychological factors to characterize risk perception. Skirpan et al. [69] used six factors, based on the work by Slovic et al. (who used 18 or 9 factors in their work) [71]: voluntariness, fear of risk, severity of consequence, perceived self understanding of risk, perceived understanding of risks by domain experts and likelihood of the risk happening). Comparatively, expert participants saw risks as posing a bigger threat, than non-experts. Skirpan et al.'s study resulted in the development of a model, *risk-sensitive design*, to help developers and designers identify and overcome the gaps in risk perception.

In Chapter 3, we used some of these risk factors to frame questions to elicit user opinions surrounding the threats associated with fitness trackers.

2.5 Behaviour

2.5.1 Sharing Data

Research shows that users' sharing depends on the type of information being disclosed and the recipient [57]. Furthermore, sharing preferences are dynamic and change over time [47,57]. In a 2012 study by Prasad et al. [57] participants were given a Fitbit to use over a period of one week. These new users shared less demographic information than sensed information, and they shared more with strangers than with family and friends. None of the participants had ever used a fitness tracker (Fitbit) before the study, and 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. [59] report that participants expressed concerns with sharing sensor data that discloses conversations, commuting habits, and psychological states. They also found that sharing data with the general public was of significant concern to participants; they were less concerned with sharing data with other study participants and researchers, regardless of whether their identity was shared with the data.

2.5.2 Taking Action

Users report that they care about their privacy [76], but in practice, they do little to protect their fitness data [1,42]. As mentioned previously, the privacy paradox is commonly used to describe this behaviour. However, Gerber et al. [27] make a case for the *privacy calculus* (a calculation of the risks and benefit of use) along with other factors to explain privacy attitudes and behaviours. These are described in section 2.6.

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 [58] concluded that fitness tracker users have difficulty reasoning about privacy because interfaces tend to obscure the complexities involved in data collection [58]. 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.

2.5.3 Privacy Policies

Users rarely read privacy policies because they are lengthy, complicated, use legal language [1], and do not facilitate decision-making based on user privacy concerns [35]. Others suggest that overexposure to 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, their 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 [53]. Hilts et al. [32] asked Canadian participants to wear a fitness tracker for two 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 five of the nine companies replied formally, and only one company (Apple) fulfilled all requests.

2.6 Theoretical Explanations for Attitudes and Behaviours

Based on the literature, Gerber et al. [27] and Kokolakis [37] put forward the most popular theories to dispute the existence of the privacy paradox. These theories originate in psychology, social theory, behavioural economics and quantum theory and attempt to explain the complexity of security and privacy attitudes and behaviours. They dissect the literature to extract alternative explanations for the contradictions between privacy attitudes and behaviours. They consider the theoretical explanations, the methodological approaches, the context [27, 37] and predictor variables [27] and present several nuanced explanations for privacy behaviours.

Both Gerber et al. [27] and Kokolakis [37] present several theories, cognitive biases (errors in thinking), and heuristics (rules of thumb) to explain the process of decision-making in relation to privacy. Tables 2.1 and 2.2 summarize these theories with a brief description for each and an example in the context of privacy privacy-related decision-making. Both authors conclude by describing the *privacy paradox* as a complex phenomenon, requiring further scrutiny by the research community.

Table 2.1: Theories of decision-making

Name	Description	Example
Privacy calculus theory [37]	Privacy decisions are made based on expected loss of privacy and potential benefits	People are willing to give up their privacy if they deem the gains to be greater than expected cost of disclosure
Social Collectives [37]	Community-based collectives are characterized by emotional connections and decision-making. Society-based collectives are characterized by rational decision-making	People disclose data because of a personal desire to belong to a social group while others make calculations of risks associated with data disclosure using reason and logic
Structuration Theory [37]	People's ability to act freely is bound by social structures	Privacy decisions are shaped by contextual factors such as social norms and trust
Bounded rationality, Incomplete information [27, 37]	Rational decision-making is limited by the information users have available and limitations in cognitive processing	In assessing privacy risks, people are not able to make fully informed decisions, due to a lack of understanding of the consequences and limitations in their capacity to process information
Indeterminacy effect [27, 37]	The outcome of a decision is not known ahead of when the decision is actually made (this has implications when attitude is assessed, rather than behaviour where the response and actual decision outcome can vary)	A user's intent about privacy protection does not necessarily reflect their decision of whether or not to protect their data
Lack of personal experience and protection knowledge [27]	Personal experiences are deemed the most reliable way of establishing an attitude that in turn, influences behaviour. In addition, users may simply have a limited knowledge of protective actions	If a users has never experienced a privacy breach, they may not be compelled to protect their personal information
Trust and risk model [27]	Trustworthiness of the recipient has a direct influence on people's behaviour, whereas, perceived risk has an influence on attitude and behavioural intention	A user might feel there is great risk in disclosing their data but does so anyway because they trust the recipient

Table 2.2: Summary of cognitive biases and heuristics in privacy decision-making

Name	Description	Example
Availability bias [27]	People tend to overestimate the likelihood of events that come to mind easily	Overestimation of privacy threats due to breaches reported in the media
Optimism bias [27,37]	People tend to believe they are less likely to experience a negative event than are others	Belief that privacy breaches happen to others
Overconfidence [37]	People tend to overestimate their skills and knowledge	When given control of their privacy, people tend to unknowingly give up more personal information
Affect bias [27,37]	People act based on emotional feelings	They underestimate privacy risks if they have a favourable impression and overestimate risks if the impression is negative
Fuzzy boundary heuristic [37]	People are uneasy knowing their information is being shared with a third-party	Users of technology are less likely to disclose personal information if they know it will be shared by providers.
Benefit heuristic [37]	People react in a positive manner when they are presented with a message pointing out benefits	Users are more likely to disclose personal information about themselves if the device they are using provides some type of "reward" for their actions
Hyperbolic discounting / Immediate gratification bias [27,37]	People tend to place a greater value or prioritize the present situation and discount future developments	Users are likely to make poor privacy decisions that have more impact over time by overestimating current risks and underestimating long-term consequences
Valence effect [27,28]	People overestimate the likelihood that they personally will experience positive outcomes compared to the average person, and this is more prevalent with negative events than with positive events (related to the optimism bias)	When informed of a data breach, a user will think that the data of others' will be compromised, but their own data will be safe.
Confirmation bias [27]	People tend to interpret new information according to their own beliefs	Education may not convince users of the privacy threats they may face while using digital technologies because of their pre-existing beliefs
Framing effect [27]	People will respond differently, depending on how information is presented to them	Users will act/react differently to advice about privacy and security protection when framed in a negative or positive way
Rational ignorance [27]	People do not educate themselves because they feel the cost of learning exceeds the benefit	The time and effort it takes to read privacy policies is greater than the cost of sharing data
Illusion of control [27]	People overestimate the amount of control they actually have in a situation	Given the ability to manage their privacy settings, users are given the false sense of control over how the data is used by third-parties

2.7 Gaps and Opportunities

We found only a few studies specifically about fitness trackers [1,3,42,57,58,76,82] as opposed to wearables in general. Furthermore, the literature studying participants' concerns about sharing types of data collected by fitness trackers is limited. Users generally do not believe fitness tracker data is sensitive [3,82]. One of the few studies specifically studying fitness tracker users' concerns [82] 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 explore in substantial detail the type of data fitness trackers users are willing to share. With these studies in mind, in Chapter 3, 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).

Previous research [82] 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 [49, 56, 62] 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 in Chapter 3 extends 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.

Studies examining sharing behaviour present limited groups of people with whom participants might knowingly or unknowingly disclose data collected by wearables in general [41, 59]. Interviews with 30 participants conducted by Alqhatani and Lipford [3] identified audiences with whom users share their fitness data (friends, family, strangers, physicians, financial incentive programs and co-workers). In Chapter 3, we ask each participant how comfortable they would be sharing with six groups of recipients. Our survey tool allowed us to quantify the responses, and gain insight into which group they are most and least comfortable sharing their fitness data.

Overwhelmingly, the literature consulted in this review calls for future work to inform users about data security and privacy [1] [16] [42] [58] [75] [82] to support them in making well-informed choices with the use of their fitness tracker. While the literature recognizes the need for awareness and education, there is limited evidence of tools and support materials designed specifically for fitness tracker users. There is, however, some support showing users perceive threats in relation to their data when it is contextualized and presented visually [1, 59, 75, 76]. We see an opportunity to develop information materials to inform users about security and privacy threats and offer protection strategies to mitigate risk. In response, our information poster designs are discussed in Chapter 4, an the corresponding user study is available in Chapter 5.

Chapter 3

Online Survey Study

We conducted a survey with 212 fitness tracker users to understand their knowledge, attitudes, and behaviours related to security and privacy.

3.1 Research Questions

We had three main research questions for this study:

RQ1: Do users willingly or unknowingly share their fitness tracker data?

RQ2: Are they comfortable with this data collection and sharing?

RQ3: Do they understand the potential implications of this type of data collection and sharing?

3.2 Methodology

Our study was reviewed and cleared by our Research Ethics Board. We conducted an online survey with fitness tracker users to determine their:

1. confidence in their 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.

3.2.1 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].

[1] https://prolific.ac/

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

International[3] participants were pre-screened using a 5-question survey that took approximately two 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 $0.22 USD for the pre-screen survey and $2.19 USD for the full survey.

3.2.2 Survey Structure

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

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

Knowledge of Data Collection and Use: 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 discussed in the literature and news reports of actual breaches, we developed scenarios describing potential risks and threats relating to fitness trackers. 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. The scenarios were briefly

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

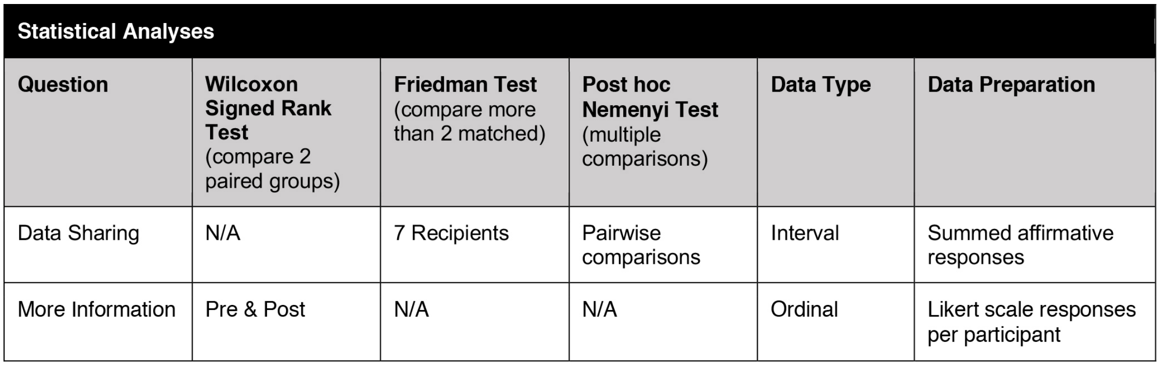
described, and participants answered ‘yes’, ‘no’, ‘don’t know’ to whether the scenario “could possibly occur” and whether it “would likely occur”. For example: *An employer fired an employee because they could tell from the employee’s fitness tracker data that she was coming to work late, leaving early, and taking multiple unwarranted breaks throughout the day.*

Attitudes: Concerns about security and privacy associated with fitness tracker use. Skirpan, et al. [69] used a set of six 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 14 different types of data based on data collected and represented by Fitbit devices, and six different sharing recipients.

3.3 Analysis

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 also used non-parametric statistical methods (Figure 3.1). To see if there was a difference in sharing with specific recipient groups, we summed affirmative responses for each group, used a Friedman Rank Sum Test to determine if there was a difference, and used Nemenyi post-hoc tests for pairwise comparisons. To establish if there was a change in the response for the question about interest in seeking out more information about security and privacy, we compared participants Likert scale responses at the beginning and end of the questionnaire using a Wilcoxon Signed-rank test. We expected a difference in sharing preferences and a positive change in interest in seeking out information.



Statistical Analyses					
Question	**Wilcoxon Signed Rank Test** (compare 2 paired groups)	**Friedman Test** (compare more than 2 matched)	**Post hoc Nemenyi Test** (multiple comparisons)	**Data Type**	**Data Preparation**
Data Sharing	N/A	7 Recipients	Pairwise comparisons	Interval	Summed affirmative responses
More Information	Pre & Post	N/A	N/A	Ordinal	Likert scale responses per participant

Figure 3.1: Breakdown of analyses for the survey study

.

3.4 Results

3.4.1 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% 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 3.1).

Table 3.1: 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%

3.4.2 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 3.2 demonstrates that participants feel fairly confident in their knowledge of what data is collected but are less confident in how their 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.

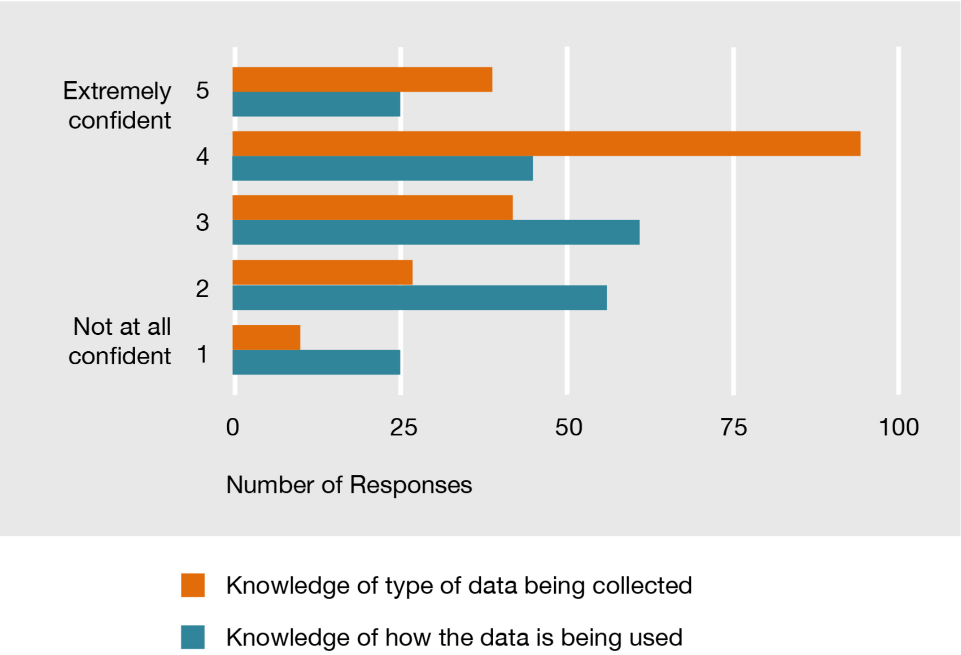


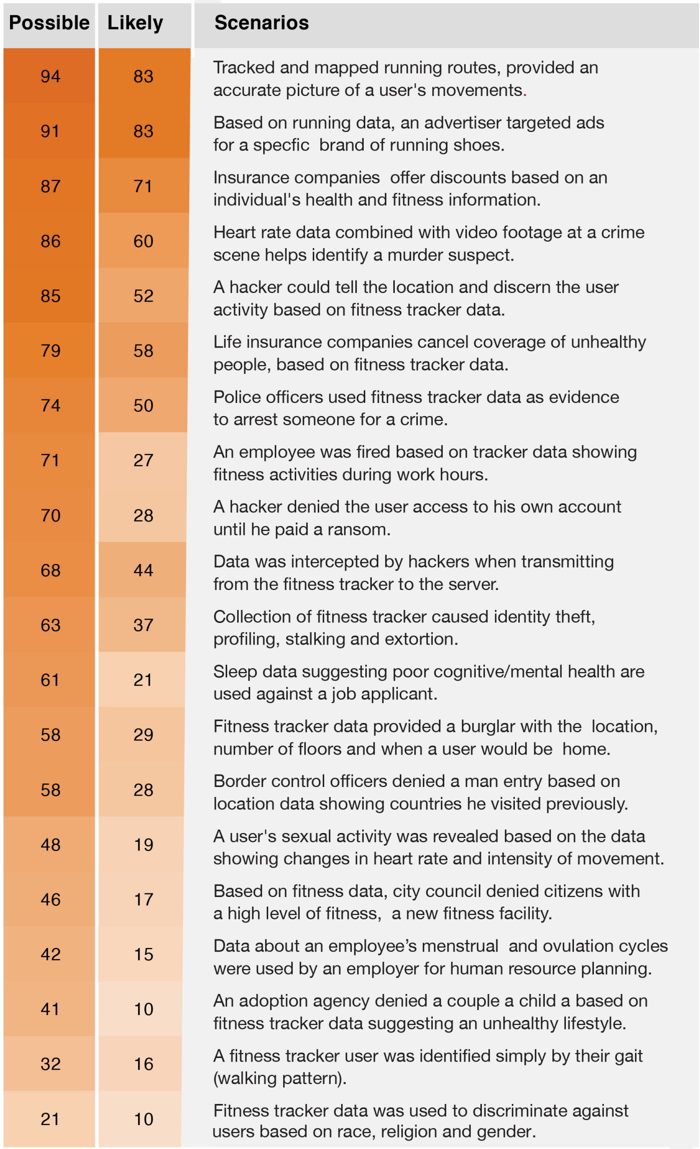
Figure 3.2: Perceived knowledge of fitness tracker data collection and use, reported using a 5-point Likert scale.

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 3.3) 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 [66].

3.4.3 Attitudes

Security and Privacy Concerns – As summarized in Figure 3.4), 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:



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 specfic 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 on 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 3.3: Percentage of participants who responded “yes” to whether each scenario describing threats associated with fitness data collection was *possible* and *likely*.

- their fear of each threat;
- the likelihood that the threat would occur;
- the severity of the consequences, should the threat occur; and
- 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

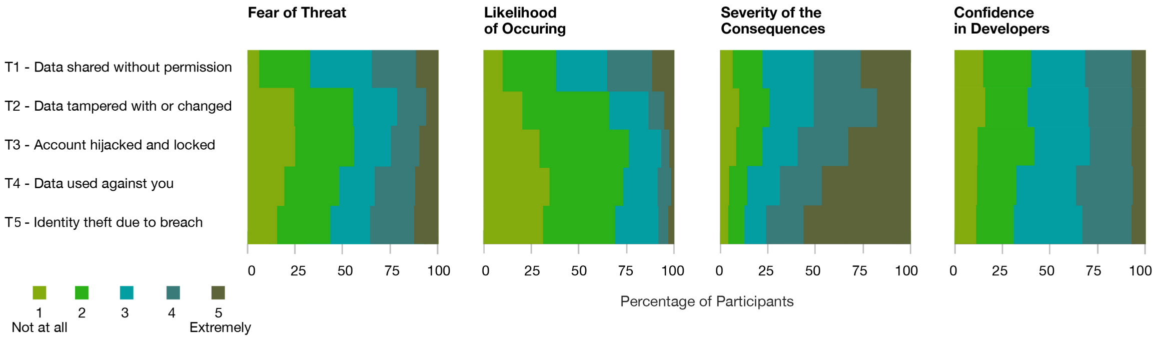


Figure 3.4: Likert scale responses for participants' reaction to five specific concerns, based on four different measures.

rated their fearfulness at the lower-to-mid points of the Likert scale for most concerns, indicating a weak/neutral response for most threats. A visual scan of an area plot confirms this result, showing few responses for "extremely fearful" (Figure 3.4), 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 3.4). 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 3.4), 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 3.5).

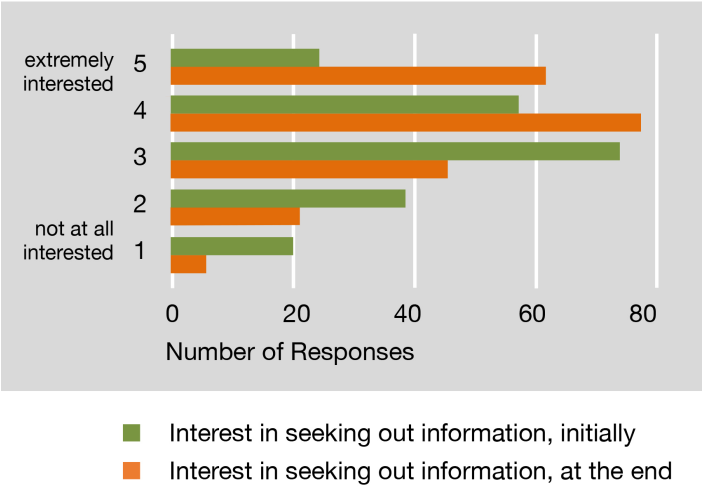


Figure 3.5: Interest in security and privacy information

3.4.4 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 3.6. The results show that, in general, most participants do little 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*. Half of participants reported *setting their preferences for sharing data*.

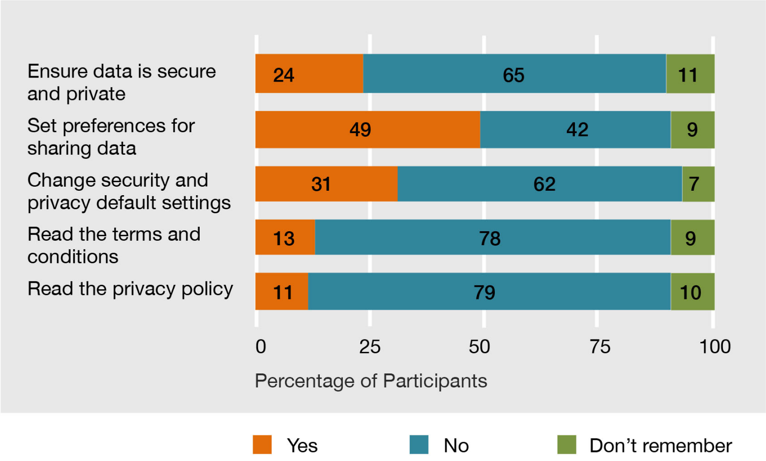
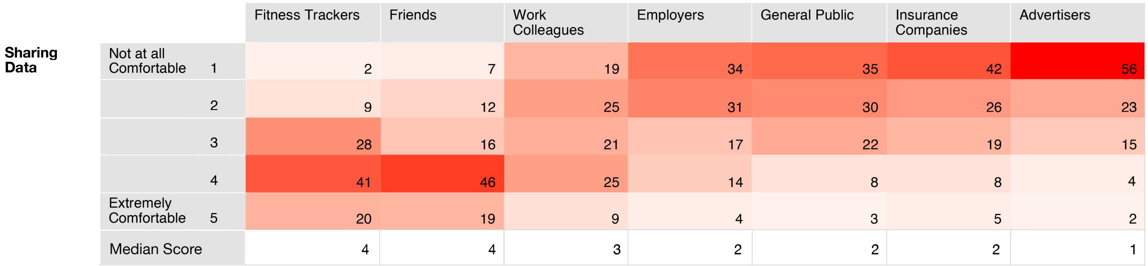


Figure 3.6: Percentage of participants who reported doing each security and privacy behaviour.

Data Sharing With Recipients – As summarized in Figure 3.7, 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”). 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.

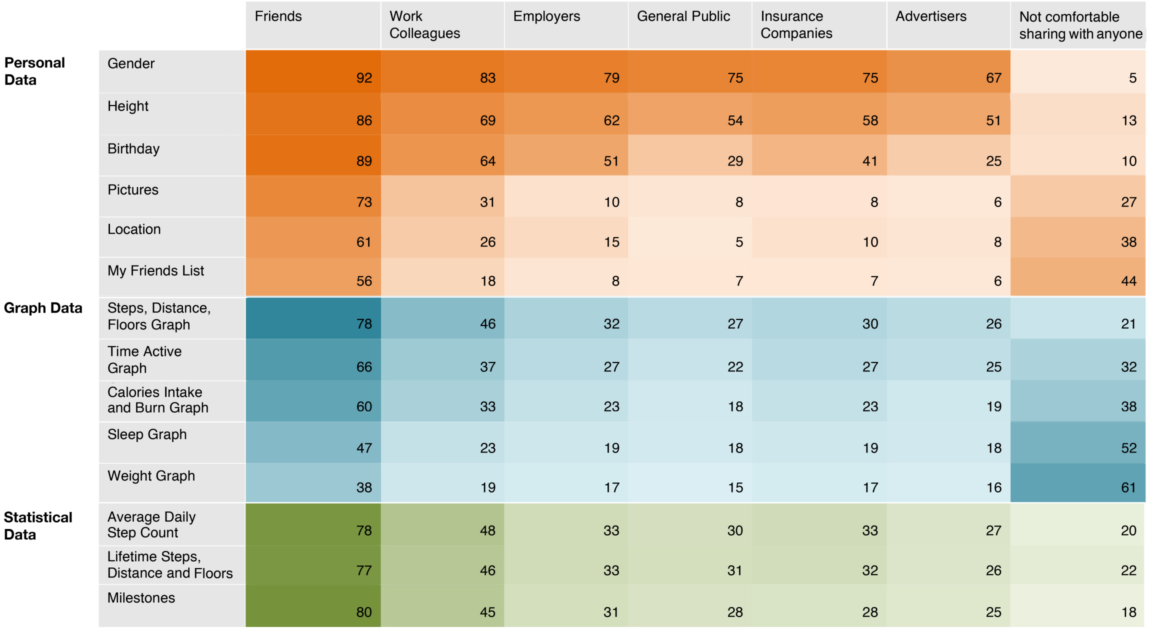
A Friedman rank sum test revealed a significant difference among the recipients with whom participants were comfortable sharing data, ($\chi^2(2) = 619.09, df = 6, p < .001$). Post-hoc testing with Pairwise comparisons using Nemenyi multiple comparison test with q approximation for unreplicated blocked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



		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 3.7: 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 responses in those cells.

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 3.8) 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.



		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 3.8: The percentage of participants willing to share each type of data with each recipient. Darker cells indicate higher percentages of responses in those cells.

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.

3.5 Interpretation of Results

We draw the following seven main insights from our results.

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? Without further probing about exactly what they do know, it is difficult to theorize further.

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 four 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 [56], (ii) Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual's health and fitness information [14] (iii) Fitness tracker data linked to time stamped video footage was used in a murder investigation to arrest a murder suspect [31]. 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.

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 [42].

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 [38] 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.

5. Users do little to protect themselves from threats – Participants are taking few steps to protect themselves from privacy and security threats. This confirms Zimmer, et al.'s [82] study that found many participants had not checked their privacy settings since the initial setup of their device. Those who adjusted settings tended to further limit what they shared.

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

3.6 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 opaque and inaccessible privacy practices from device manufacturers.

3.6.1 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: First, we now have detailed data about what types of data users are comfortable sharing and with whom. We found clear relationships between these two factors: users have distinct sharing preferences for different data and different recipients. Understandably, they 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.

This study also shows that users value types of data differently. Understandably, 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. For example, sharing preferences can only be accessed by logging on to the website of some providers; ideally these would also be integrated into the corresponding smartphone apps.

Knowledge of threats: Secondly, 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 users' combined understanding of both the *plausibility* and *likelihood* of various threat scenarios related to fitness data. 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 also seem unaware of potential threats associated with the collection of personal fitness data.

Furthermore, users exhibited an "optimistic bias effect" [66]: they are not very fearful of threats, believe them unlikely to happen, but believe the consequences would be severe should they occur. Their lack of concern may partially explain why our participants do not take 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 [27, 37]. These disclosures are especially concerning considering the sensitivity of the data collected. Similar to users of other technologies [1], our participants are not consulting privacy policies and terms and conditions for their fitness tracking device and, therefore, know little about data collection. This is unlikely to change until problems with the usability of privacy documents are addressed. There is little motivation, however, for companies to make their data collection practices more transparent.

3.6.2 Recommendations

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

Designing education/awareness campaigns – Users do not seem to be aware of the potential uses of their personal data. Users should understand how enabling specific functionalities and data sharing options impacts what data is collected and how that data may be used/misused. 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 respond positively to information intended to educate them about privacy [1, 59, 75]. Therefore, we are optimistic about the benefits of such efforts.

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.

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.

3.6.3 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. 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. We also acknowledge that the change in responses for questions presented at the beginning and the end of the questionnaire could be due simply to raising awareness about privacy and security.

3.7 Summary

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 did little to protect their personal data. They did, however, have distinct preferences for sharing specific types of data, with different groups of people. 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.

Chapter 4

Design of Prototypes

We designed two sets of posters and their control counterparts to understand if visual design and messaging would affect fitness tracker users' privacy knowledge, attitude and behaviours. We begin the chapter by giving an overview of information design and the visual communication strategies used in the field. Next, we introduce a framework for understanding privacy risks and describe the decisions that guided the design of the poster prototypes.

4.1 Information Design

Information design is a field of study concerned with representing information in a visual way [40]. Sless argues that information design has its roots in 40,000 year-old drawings of lunar calendars drawn on animal bones [70]. While we cannot explain the reasons for producing early drawings with certainty, we know as civilized societies developed, visuals became necessary to communicate complex ideas and concepts. Stiff [73] suggests information design, as we know it today, came about early in the 20th century because of the emergence of scientific, technological and financial capitalism. Corporations required the organization and display of facts to grow and thrive. Furthermore, a rich economy and prosperity brought about a need for public information.

Erik Spiekermann [72] believes that information designers are in a golden age, given the proliferation of digital media. He explains the change in a designer's activities, by providing a description of the current state of the practice of information design:

> Identifying the problem and analysing the context and audience before shaping the message: this used to be what information design was all about. And whatever the medium, substrate, or location, this is what

> we are still called upon to do. Information design can show the way through–and perhaps out of–the jungle that is our modern world. Applied properly, it can turn data into information and information into effective communication and appropriate action.

Importantly, Spiekermann's definition includes a reference to "action", distinguishing information design today from that of the past. For this thesis, we attempted to: *shape messages* into *effective communications* for *encouraging good security and privacy protection practices* for users of fitness trackers.

4.1.1 Strategies for Information Design

Because humans perceive and understand information in many different ways, designers have developed various visual and verbal communication tactics to make information meaningful [5]. Lankow et al. [40] believes successful information design is appealing, understandable and memorable. They describe three provisions necessary for effective verbal and visual communication:

1. *Appeal:* Communication should engage a voluntary audience

2. *Comprehension:* Communication should effectively provide knowledge that enables a clear understanding of the information

3. *Retention:* Communication should impart memorable knowledge

Appeal

Information that communicates effectively attracts and maintains attention. The harmonious arrangement of images and text can capture the attention of the viewer and guide them through a composition. Bowers [12] describes harmony as "a grouping of related components that make sense together". Dair [19] explains that harmony can be achieved through either concordance (uniformity of appearance) or contrast (unity in differences) or the interweaving of both. He goes on to say, while concordance strives for uniformity and uninterrupted reading of text and images, contrast punctuates by placing elements in opposition to each other. For example, while we may use only one typeface (concordance) in a composition, we can change the type size to emphasize the title (contrast). Dondis [23] asserts concordance and contrast are expressed through the manipulation of the basic elements: line, shape, tone, colour, direction, movement, proportion and scale. We can argue that while contrast is useful for attracting attention, concordance works to maintain attention.

Comprehension

Using principles in visual communication design, we can facilitate understanding. Müller-Brockman [51] explains:

> Information presented with clear logically set out titles, subtitles, texts, illustrations and captions will not only be read more quickly and easily but the information will also be better understood and retained in memory.

Visual hierarchy affects how images and text are read. Bowers [13] claims because we are accustomed to reading left to right and top to bottom, placing images and text using this convention promotes ease in reading. By isolating visual and text information with distance, size, colour, texture, we can call attention to items of interest and guide viewers through a composition.

Retention

Information that is meaningful is more easily retained and retrieved [17]. Thus, by presenting relevant content, the likelihood of committing it to memory increases. A study by Bateman et al. [8] shows the use of images and supporting content and the presence of visual embellishments promote understanding and retention of information. Furthermore, they found emotional response and aesthetic preference may affect the encoding of information into long-term memory. Using devices such as visual metaphor, symbols and iconography and visual embellishments fosters retention of information [40]. Information is more memorable if it is relevant to users.

The Nature of Infographics

Infographics/Information graphics refer to a multifaceted visual representation of information that contains explanations of insightful descriptions [40]. Lankow, et al. [40] suggest infographics are either *explorative* or *narrative* in nature[1]. *Explorative*

[1] The categories were originally described by Nichani and Rjamanickam along with two other categories to describe interactive graphics: *exploratives, narratives, instructives and simulatives.* While cited in a number of studies, the online link is no longer available (`http://www.elearningpost.com/articles/archives/interactive_visual_explainers_a_simple_classification/`).

infographics provide factual information where the viewer is invited to examine and make their own interpretation of the facts. *Narrative* infographics provide a specific message and pre-determined conclusion and are more relevant when audience appeal and retention are essential.

Storytelling in Information Design

Stories have the power to influence interpretation of facts, contextualize information and make it relevant to people [68]. The use of *storytelling* in information design was popularized through journalism with the use of visualization to explain complex concepts. Journalists recognize the value of using visuals to impart the news of the day as evidenced by news organizations such as the New York Times, the Washington Post and the Guardian, who regularly include infographics to convey messages. With online platforms, journalists have integrated interaction to bolster static infographics to produce complex, information-rich visual to inform readers [65].

Storytelling is inherent to both the *explorative* and the *narrative* approaches to information visualization and is either author/designer-driven or user-driven. With narrative infographics, the storytelling is explicit while with explorative infographic, storytelling is implicit and determind by the user.

Visual Communication

Dondis [23] explains the three ways in which humans express and receive visual messages:

- *Representationally* – What we see and recognize from the environment and our experiences. Representational imagery depicts reality through emphasis on details and distinguishing features (e.g., photographs, illustrations)
- *Symbolically* – What we see based on meaning that is assigned and agreed upon by groups of people. Symbolic imagery is a distillation, reduction or simplification of only the most essential features to convey complex ideas. Symbols can be representational (e.g., a simplified picture of a bird) or abstract and arbitrary (e.g., alphabetic characters).
- *Abstractly* – What we experience viscerally, that does not draw upon familiar visual information from our environment or experiences. Abstract imagery is

> a reduction or simplification to basic visual elements, and is concerned with colour, shape, tone, texture and composition.

The visual imagery in each category is progressively more abstract in nature as we move from representational to symbolic to abstract: from the highly recognizable to a simplified interpretation (but still recognizable) to the non-identifiable. However, depictions of images can vary in their degree of simplification/abstraction, even within the representational and symbolic categories.

4.2 Our Framework for Understanding Privacy Risks

Our goal for this study was to examine ways of making users aware of the risks associated with the use of fitness trackers. We developed a framework to structure security and privacy information. As described below, this was informed by previous educational tools developed by other researchers and the findings from our first study. Ideas for a framework emerged through iterative visualizing, during the design process.

4.2.1 Existing Visualizations for Data Disclosure

Work by other researchers [1, 59, 75, 76] provide a variety of ways to make data collection more understandable for users. Previous research [1, 59, 75, 76] indicates that users perceive threats in relation to their data when it is contextualized and presented visually. Raij [59] et al. have studied the effects of showing participants visualizations of their physiological, psychological and behavioural data collected by wearable sensors. When shown behaviours combined with temporal and spatial information, participants were better at estimating threats surrounding the disclosure of the data [59]. Within the context of data collection of smartphone apps, Van Kleek et al. [75] evaluated an interface that displays the relationships between various organizations who collect/share data, the data types, the data uses/purposes, permissions and data leaks. Being transparent in the tracking behaviours of the apps helped participants find and choose apps that disclosed minimally only to trusted companies and they reported being more confident about using these apps. Aktypi et al. [1]

developed a digital identity exposure tool. In one view they showed users the data collected by : 1) various online social networks and 2) fitness trackers. Another view showed 1) data collected by their devices; 2) what could be inferred from the data; 3) the potential risk; and 4) an explanation of the implications.

We found little research evaluating visual interventions for educating users about security and privacy. A recent example includes Zhang et al.'s work showing how comics can improve users' understanding of security and motivate them to protect themselves [79–81]; they also explore the role of interactive e-books in children's privacy education [78].

4.2.2 Relevant Findings From Our First Study

Our study from Chapter 3 suggests that fitness tracker users:

- are confident in their knowledge of what their fitness tracker collects;
- are unsure about how their data is being used;
- have limited understanding of potential threats;
- have inconsistent security and privacy concerns;
- do little to protect themselves from threats;
- are most comfortable sharing data with friends;
- distinguish which data they are willing to share with whom; and
- are interested in seeking out more information about security and privacy.

Our first study indicated fitness tracker users require a greater awareness of what data is collected, sharing practices related to the tracking of their data, and how their choices have the potential to compromise their privacy.

4.2.3 Conceptualizing Through Design

With the information gleaned from our first study and the related literature, we began digitally sketching to formulate ideas for how to express security and privacy concerns. Through the process of visualizing, important relationships between data collection, the use of data, the threats, and ways to mitigate risk became visible (Figure 4.1).

One of the sketches incorporated a series of questions a user might ask when using their fitness tracker: What type of functionality do I want? Who do I share my data with? What type of data is collected by my fitness tracker? What are the possible threats related to the collection of data? How can I keep my data secure and private?

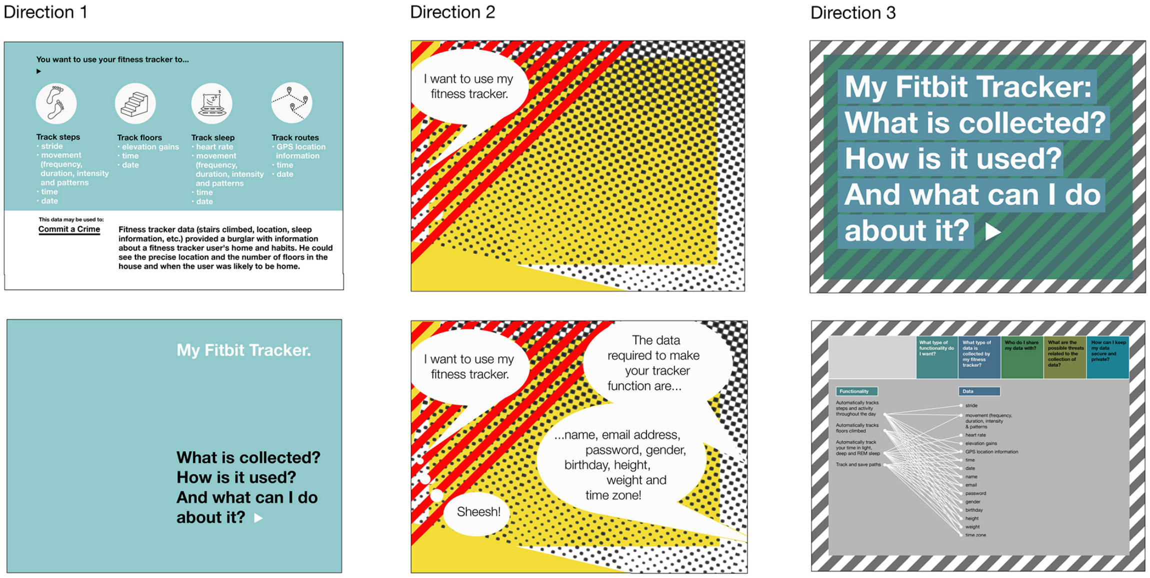
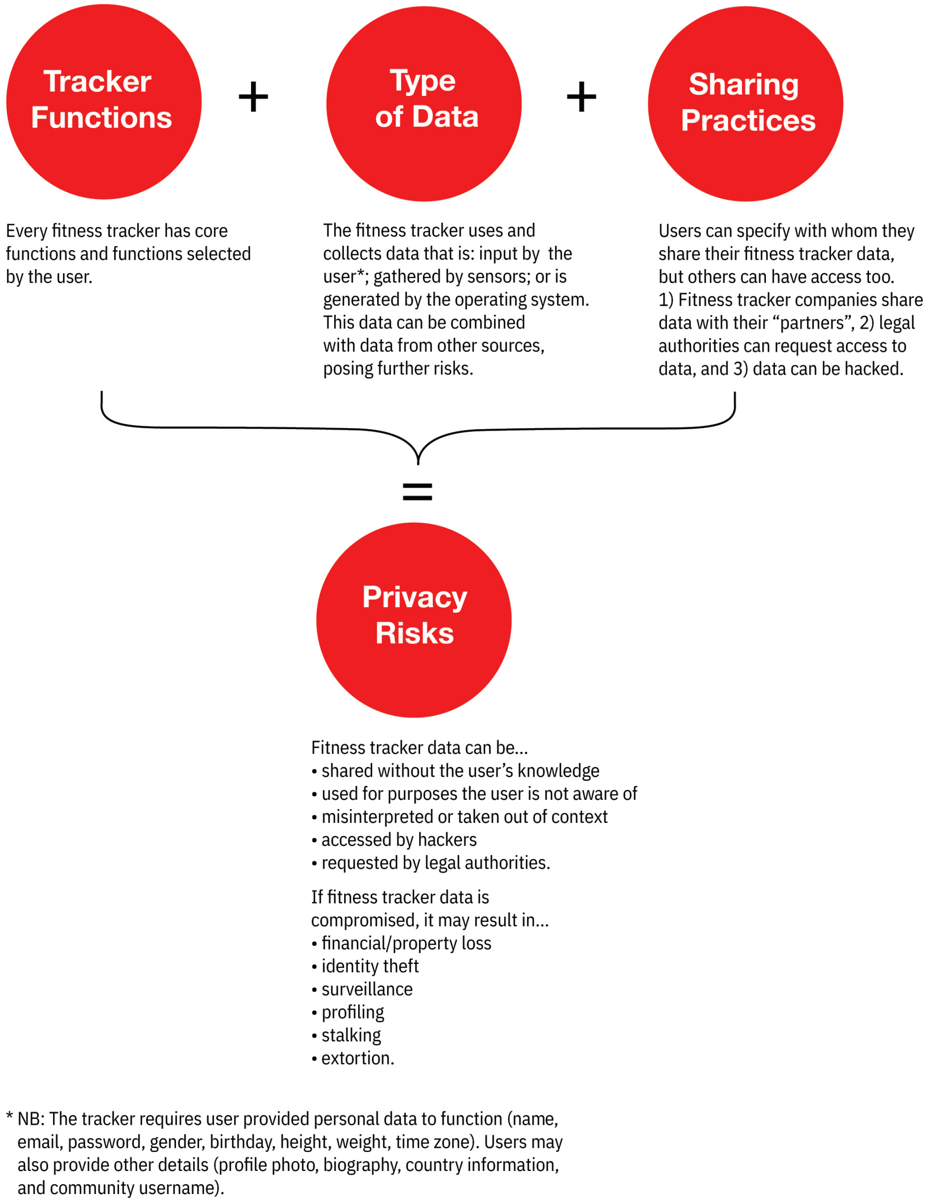

Direction 1
You want to use your fitness tracker to...
Track steps
· stride
· movement (frequency, duration, intensity and patterns
· time
· date
Track floors
· elevation gains
· time
· date
Track sleep
· heart rate
· movement (frequency, duration, intensity and patterns
· time
· date
Track routes
· GPS location information
· time
· date
This data may be used to:
Commit a Crime
Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user's home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.
My Fitbit Tracker.
What is collected?
How is it used?
And what can I do about it?
Direction 2
I want to use my fitness tracker.
I want to use my fitness tracker.
The data required to make your tracker function are...
...name, email address, password, gender, birthday, height, weight and time zone!
Sheesh!
Direction 3
My Fitbit Tracker:
What is collected?
How is it used?
And what can I do about it?
What type of functionality do I want?
What type of data is collected by my fitness tracker?
Who do I share my data with?
What are the possible threats related to the collection of data?
How can I keep my data secure and private?
Functionality
Automatically tracks steps and activity throughout the day
Automatically tracks floors climbed
Automatically track your time in light, deep and REM sleep
Track and save paths
Data
stride
movement (frequency, duration, intensity & patterns
heart rate
elevation gains
GPS location information
time
date
name
email
password
gender
birthday
height
weight
time zone

Figure 4.1: By sketching ideas for an educational tool, the content emerged.

These questions contributed directly to the conceptualization of the Fitness Tracker Privacy Risk Framework (FTPR Framework), showing the factors that contribute to privacy risks. These are: tracker functions that are activated, the type of data required or generated by the tracker, and the data sharing practices (Figure 4.2). We used this framework to develop content and to structure information for the posters.



Every fitness tracker has core functions and functions selected by the user.

The fitness tracker uses and collects data that is: input by the user*; gathered by sensors; or is generated by the operating system. This data can be combined with data from other sources, posing further risks.

Users can specify with whom they share their fitness tracker data, but others can have access too. 1) Fitness tracker companies share data with their "partners", 2) legal authorities can request access to data, and 3) data can be hacked.

Fitness tracker data can be...
- shared without the user's knowledge
- used for purposes the user is not aware of
- misinterpreted or taken out of context
- accessed by hackers
- requested by legal authorities.

If fitness tracker data is compromised, it may result in...
- financial/property loss
- identity theft
- surveillance
- profiling
- stalking
- extortion.

* NB: The tracker requires user provided personal data to function (name, email, password, gender, birthday, height, weight, time zone). Users may also provide other details (profile photo, biography, country information, and community username).

Figure 4.2: The 4-part FTPR framework used to communicate potential risk with fitness tracker use

4.3 Prototype Development

The tracking of fitness data is usually an invisible operation that is not easily discernible. By making it visual and visible, it is our hope that users will better understand the process. We designed two distinctly different sets of posters (*Narrative* and

Explorative) to see what type of visuals and content might increase awareness about privacy threats and encourage users to take protective measures (Figure 4.3). We are unaware of any other empirical testing of the explorative and narrative approaches in the usable security domain, nor in the literature on information design.

In addition to the two visual posters, we designed a control set of posters (*Narrative Control* and *Explorative Control*) for each, which included the same textual content but lacked most of the visual components (Figure 4.4). Each set contained a series of five related posters:

- The first poster in each set contained the FTPR Framework and an overview of the risks involved with the use of a fitness tracker.
- The next three posters introduced the types of violations that are possible with the use of fitness trackers, information about tracker functions, the type of data collected, data sharing practices, and potential implications (Figure 4.5). These were presented as scenarios.
- The final poster contained protection strategies for users.

The posters designed for this study were presented to participants one after another in a lab setting,but in practice, we envision that these would be introduced as a longer term educational campaign. They could be posted one at a time, for a specified time period, in public spaces over a number of weeks or months.

We designed the posters with Adobe InDesign and Adobe Illustrator. They were printed on a colour laser printer on 100lb. cover stock, 11 × 17 inches in dimension. For a larger version of the posters, see: Appendix F, Appendix G, Appendix H, Appendix I.

4.3.1 The Scenarios

We used scenarios to help communicate the risks associated with fitness tracker use and to contextualize information about data collection. Our intention was to make it relevant for fitness tracker users, knowing that meaningful information is more easily retained. We selected three scenarios from our first study, where participants rated each based on the questions about *plausibility* and *likelihood* that each threat would occur.

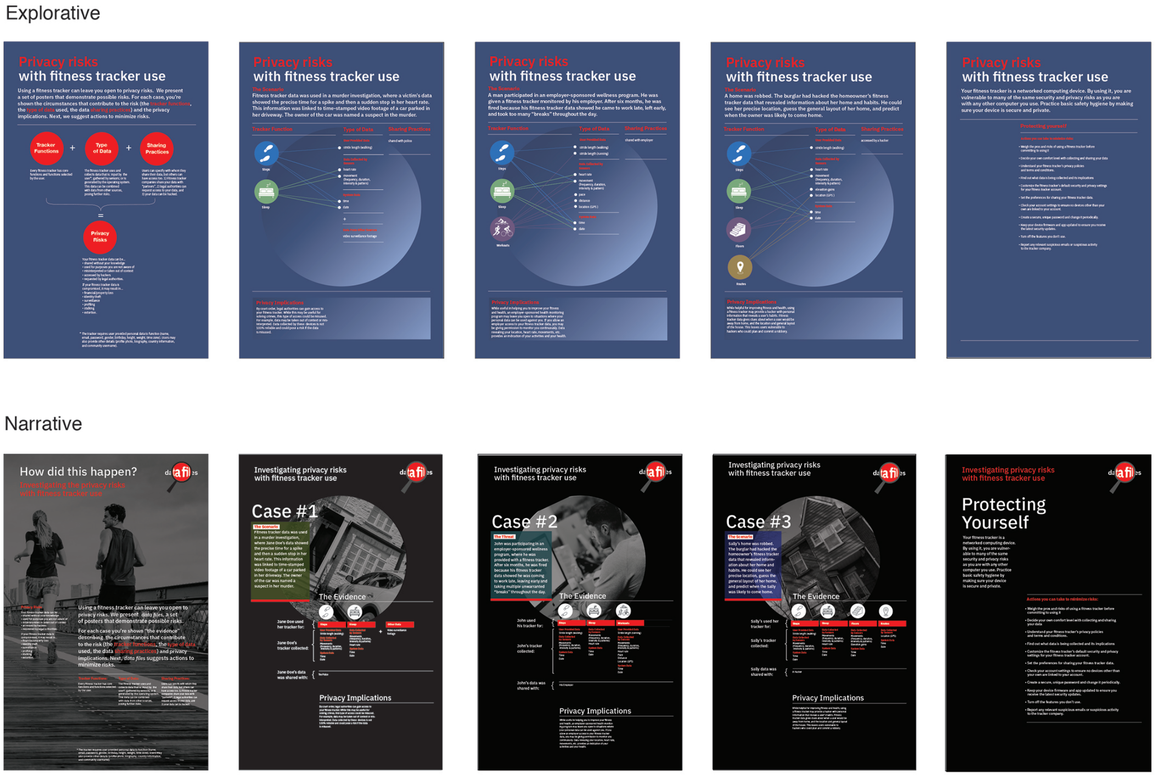


Figure 4.3: Overview of the Explorative (top) and Narrative (bottom) posters.

Scenario 1 – In this scenario, fitness tracker data was used in a murder investigation, where a victim's data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder. This scenario is based on a true story reported in the mainstream news (CNN) [30]. In our first study, the majority of participants rated the scenario as both plausible and likely to occur.

Scenario 2 – The scenario describes an employer who fired an employee because they could tell from the employees fitness tracker data that she was coming to work late, leaving early and taking multiple unwarranted breaks throughout the day. This fictitious scenario was developed based on information from a law journal article [14] discussing ways to protect employees from the vulnerabilities and potential misuse of fitness and health data. In our first study, the majority of participants rated this scenario as plausible but unlikely to occur.

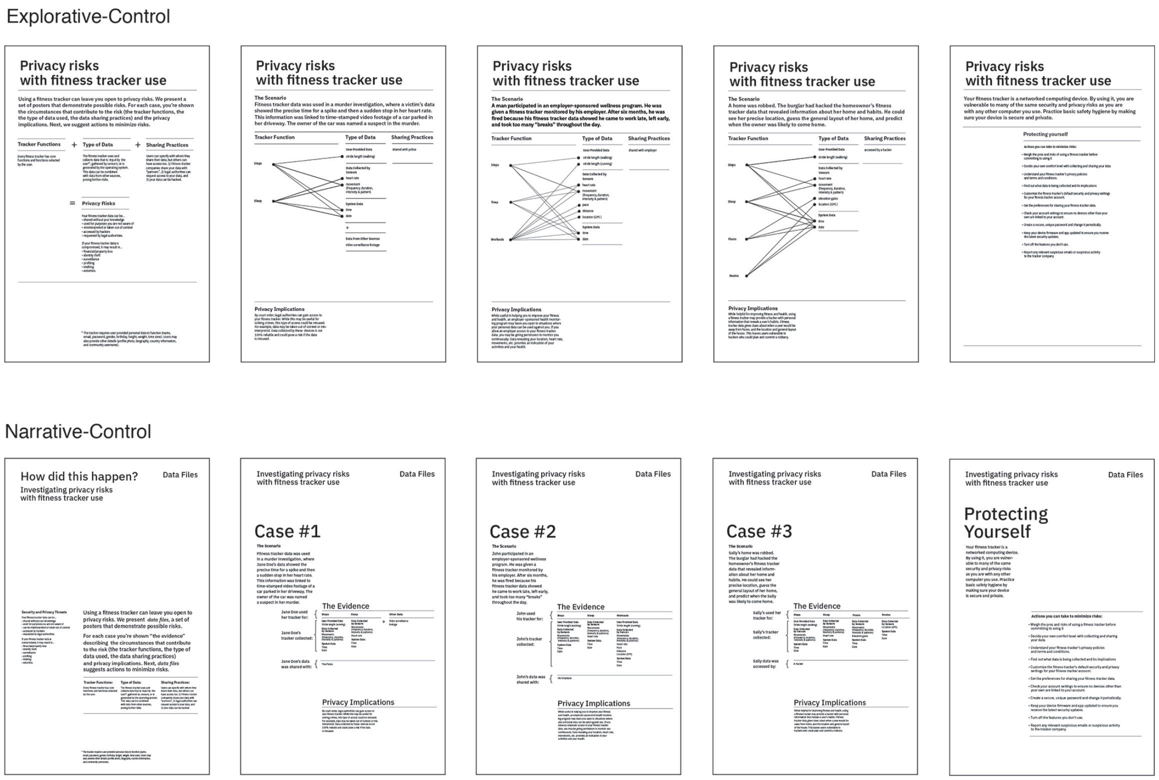
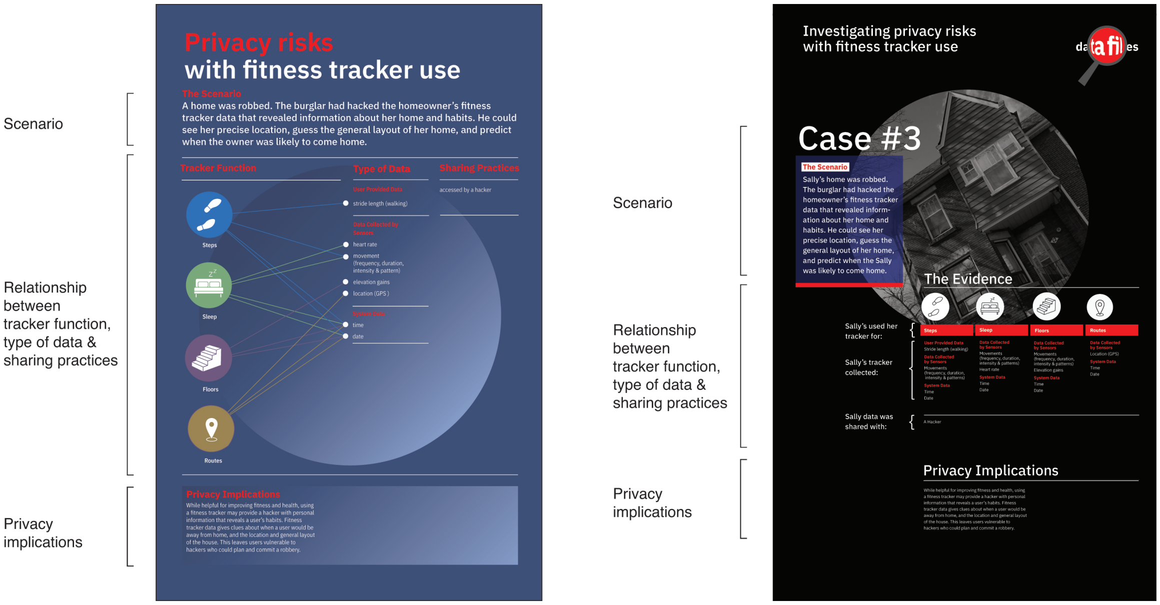

Explorative-Control
Privacy risks with fitness tracker use
Privacy risks with fitness tracker use
Privacy risks with fitness tracker use
Privacy risks with fitness tracker use
Privacy risks with fitness tracker use
Narrative-Control
How did this happen? Investigating privacy risks with fitness tracker use
Data Files
Investigating privacy risks with fitness tracker use
Case #1
The Evidence
Privacy Implications
Investigating privacy risks with fitness tracker use
Case #2
The Evidence
Privacy Implications
Investigating privacy risks with fitness tracker use
Case #3
The Evidence
Privacy Implications
Investigating privacy risks with fitness tracker use
Protecting Yourself

Figure 4.4: Overview of the Explorative Control (top) and Narrative Control (bottom) posters.

Scenario 3 – In this scenario, hacked fitness tracker data (e.g., stairs climbed, location, and sleep information) provided a burglar with information about a fitness tracker user's home and habits. He could see the precise location and the general layout of the house, and determine when the user was likely to be home. This fictitious scenario was based on assumptions of what would happen when combining different types of data. In our first study, approximately half of participants rated this scenario as both plausible and likely to occur.

While the content is the same for the visual two approaches, they differed in style. The Narrative posters emphasize the storytelling capacity of information graphics to appeal to the users' imagination, while the Explorative posters present a factual description of the scenario. These are described in the next section.



A home was robbed. The burglar had hacked the homeowner's fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the owner was likely to come home.

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user's habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Sally's home was robbed. The burglar had hacked the homeowner's fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the Sally was likely to come home.

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user's habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Figure 4.5: Each scenario poster was made up of three components, 1) A scenario; 2) information showing the relationship between tracker function, type of data and sharing practices; and 3) privacy implications.

4.3.2 Visual Approaches

We used two approaches for the information posters, *Narrative* and *Explorative*, to see how these distinctly different ways of presenting information would affect participants' understanding of privacy and if they might influence their behaviour. We designed the *Narrative* posters to guide the user through "stories", while the *Explorative* posters allowed users to explore and interpret information in a more diagrammatic way.

The structure of information and the use of pictograms was similar for both approaches, as follows:

Structure: We structured textual information from top to bottom for ease in reading and promote comprehension. The scenario posters were made up of three main components: scenario descriptions were positioned at the top to introduce the violation; information about tracker function, data collection, and sharing were situated in the middle; and the privacy implications were located at the bottom. In addition, particularly salient information was highlighted with colour and/or a change in text size to provide contrast.

Pictograms: We designed a set of pictograms using Adobe Illustrator. Pictograms were supported by text labels to help facilitate comprehension in relation to each of the tracker functions (steps, sleep, floors, workouts, routes) and foster retention of information. We experimented with various line qualities, shapes and colours.

For the Explorative posters, we used solid coloured circles and solid white symbols. Because of the complexity of the bipartite graph, we assigned contrasting colours for pictograms to: 1) attract attention and 2) assist the user in distinguishing the tracker functions.

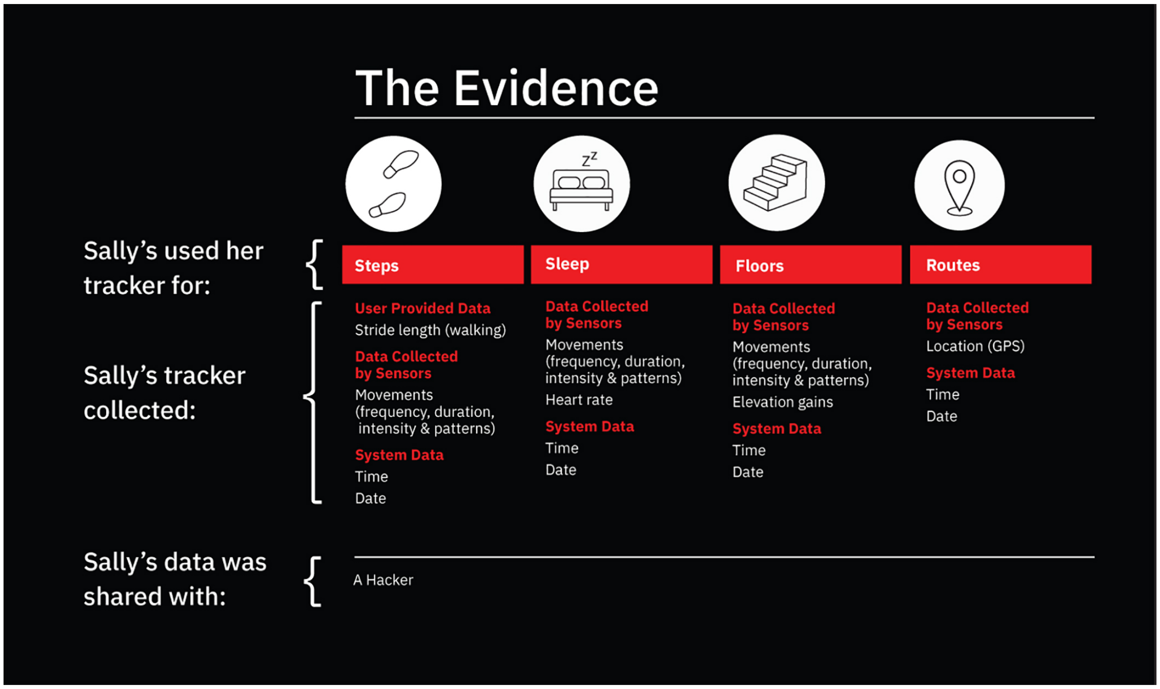
On the Narrative posters, we used white circles and black lines to delineate the symbols (instead of solid colour) because the positioning of each function on the table and the listing of data below were sufficiently separated and could be easily distinguished. This made additional colour unnecessary.

In the descriptions below, we explain the overall concept and strategies behind the Narrative and Explorative posters, beginning with the scenario posters because they formed the basis for the design. Then we explain the initial overview poster and the final poster containing protection strategies.

4.3.3 Narrative Posters

Appendix F contains full-page versions of each Narrative poster. The Narrative scenario posters displayed the information using the metaphor of a detective story, both to engage viewers by treating the text as evidence for investigating a crime and to make the information memorable. The theme was carried throughout, beginning with the title, “data files”, and depicting a magnifying glass. Information on the scenario posters were treated as “cases” (scenarios) with “evidence” (tracker functions, the type of data collected, data sharing) and the privacy implications posed by the crime. We named the human subject for each scenario (Sally, John, Jane Doe) to personalize each case and support the concept of an investigation. The tabular information showed the relationship between the tracker functions, the type of data collected, and data sharing. Figure 4.6 illustrates one of the these tables.

The Narrative posters use a representational approach to visual communication, relying on what is seen and recognized from the environment and experiences. We used photography as the main focal point for these posters. The posters had a



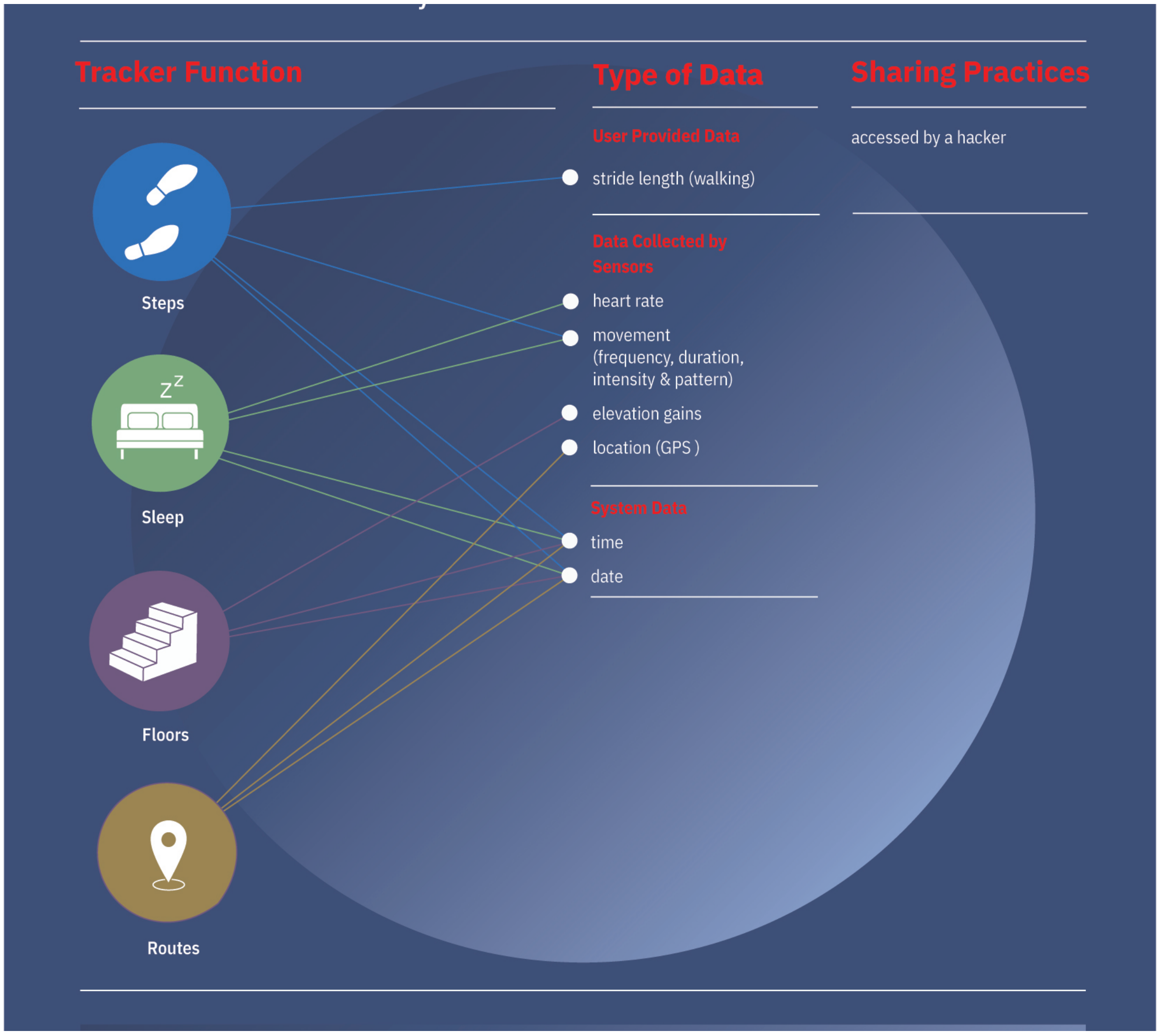
The Evidence

Sally's used her tracker for:	Steps	Sleep	Floors	Routes
Sally's tracker collected:	User Provided Data Stride length (walking) Data Collected by Sensors Movements (frequency, duration, intensity & patterns) System Data Time Date	Data Collected by Sensors Movements (frequency, duration, intensity & patterns) Heart rate System Data Time Date	Data Collected by Sensors Movements (frequency, duration, intensity & patterns) Elevation gains System Data Time Date	Data Collected by Sensors Location (GPS) System Data Time Date
Sally's data was shared with:	A Hacker			

Figure 4.6: A table illustrating the relationship between tracker function and data collected (Narrative Poster).

monochromatic colour scheme (a black background with black and white images). The photographs had a dark gray tint overlay, to suggest an air of mystery and reflect the seriousness of the subject matter. The content of the photography for three scenario posters showed literal representations of the privacy violation: the scenario describing the employee dismissal depicted an office worker; a car, parked in a driveway represented the murder scenario; and the home burglary portrayed an image of a residence. The photograph in the circular disc provided a "binocular" view of the "scene of the crime". The angled placement of photographs creates a feeling of unease that one would experience with an undesirable event. The majority of the text was white, in contrast to the dark background. We used red to highlight portions of the text and a contrasting colour for each scenario description.

The first Narrative poster provides an overview of privacy issues associated with the use of fitness trackers and illustrates the FTPR Framework in tabular format. These are layered over a photograph depicting two runners in an urban environment (a common characterization of a fitness tracker user). The image is the dominant



Tracker Function

Type of Data

Sharing Practices

User Provided Data

stride length (walking)

accessed by a hacker

Data Collected by Sensors

heart rate

movement (frequency, duration, intensity & pattern)

elevation gains

location (GPS)

System Data

time

date

Steps

Sleep

Floors

Routes

Figure 4.7: A bipartite network visualization illustrating the relationship between tracker function and data collected (Explorative Posters).

visual and the FTPR framework occupies two-thirds of the page.

The final Narrative poster consisted of two main elements: a general statement about protecting against security and privacy and a set of actions to minimize risks. While this poster contains only text, it followed the same structure and format as other posters in the set.

4.3.4 Explorative Posters

Appendix G contains full-page versions of each Explorative poster. The Explorative scenario posters contained a factual description of the scenario. These posters take an abstract approach to visual communication, using simplification of basic visual elements. The posters reply upon basic shapes and contrasting colours to draw attention to the text. The text describing the scenario was treated in a similar fashion; the language was straightforward and direct and did not embellish the information. The Explorative scenario posters emphasized the relationships between tracker functions and the data collected. The information was visualized using a bipartite network diagram, as shown in Figure 4.7. It was made of connecting lines to show the relationship between the tracker functions, the type of data collected, and data sharing. Placing the diagram on a circular shape and occupying approximately half of the space made it the dominant visual and provided contrast to the rectangular shapes used for the overview above and the privacy implications, below. The dark purple background colour expressed the serious tone of the subject matter and the gradation provided depth for the composition and helped separate the three main components.

The first Explorative poster provides: an overview explaining the subsequent posters; a brief overview of security and privacy threats associated with the use of fitness trackers; and the FTPR Framework in a diagrammatic format. In contrast to the Narrative poster, the framework occupies two-thirds of the page and serves as the focal point.

The final Explorative poster consisted of two main elements: a general statement about protecting against security and privacy and recommended actions to minimize risks. This poster contains only text, but it followed the same structure and format as the other Explorative posters.

4.3.5 Control Posters

We designed two sets of control posters, one mirroring the Narrative posters and one mirroring the Explorative posters. The control posters were exact replicas of their visual counterpart, except they did not contain photographs, pictograms or colour. They consisted of black text on a plain white background.

The Narrative-Control posters are in Appendix H and the Explorative-Control posters are in Appendix I.

4.4 Summary

In summary, we have described the design approach for our four prototypes. In the following chapter, we present the user study evaluating the effectiveness of the posters.

Chapter 5

Poster Usability Study

The results of our first study 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 the types of threats that may result from its collection. Furthermore, they did little to protect their data. Our findings lead us to believe that fitness tracker users require a greater awareness of the collection, ownership, storage, sharing practices and threats related to the tracking of their data. For the second study, we designed and evaluated the effectiveness of four sets of posters to make users aware of privacy risks and to promote good safety and security practices.

5.1 Research Questions

Two main research questions guided this study:

RQ1 Effect of Presenting Information – Does presenting information about fitness tracker security/privacy affect users' knowledge, attitude and behaviours?

RQ2 Effect of Poster Type – Does visual design and messaging affect users' knowledge, attitude and behaviours?

In addition, we asked:

RQ3 Usability – Which poster type do users deem most usable?

5.2 Methodology

The Carleton University Research Ethics Board-B (CUREB-B) granted ethics clearance for this study. We asked participants to read and sign an informed consent form.

For this study, we were interested in prompting a change in fitness tracker users' security and privacy protection behaviour with the presentation of information posters. In describing the literature on privacy attitudes and behaviour, Kokolakis [37] makes a distinction between privacy intention and privacy behaviour and notes that much of the research confounds intention and behaviour. We developed a series of questions and posed them at three different points in our study (pre, post and follow-up test) to capture baseline behaviour, intention to act after viewing the posters, and reported behaviour after a week. In addition, we asked questions about knowledge and attitudes to understand if presenting security and privacy information would affect their post test and one week follow-up responses. To see if participants retained information after one week, we compared post to follow-up test responses. All responses were self-reported. We expected a positive change in participants' intent and behaviour after the viewing the posters.

The study consisted of two parts: a lab session and follow-up online session. The lab session included a pretest questionnaire, the presentation of five information posters and a post test questionnaire. Before beginning, we explained to participants that the purpose of the study was to evaluate the effectiveness of education posters to inform users about data collection practices associated with fitness tracker use.

We used a mixed study design. We had a between-subjects variable, *Poster Type*, with four poster conditions. Participants were assigned to one of four poster conditions: *Explorative*, *Narrative*, *Explorative-Control*, and *Narrative-Control*. We assigned posters to participants by cycling through the four poster conditions, in order of attendance. We also had a within-subjects variable, *Presenting Information*, where participants were tested at three different times during the study. The study design is described more fully in the "Analysis" section, below. After a week, participants completed an online follow-up questionnaire. The lab session took 35 to 45 minutes and the online follow-up questionnaire took 5 to 10 minutes.

We collected data for the questionnaires with the online survey platform, Qualtrics [1] and audio recorded participants' verbal responses about their experience viewing the

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

posters.

5.2.1 Questionnaires

Pretest Questionnaire

The pretest questionnaire was derived from questions used in Study 1, with some minor adjustments. The pretest had 44 questions, including 3 attention-check questions. It consisted of "yes/no/don't remember", multiple choice, single answer, 5-point Likert scales questions, and open-ended text questions. We asked questions about:

A. *Demographics* – Age, education, work experience, expertise, the brand of fitness tracker and the tracking functions they use;

B. *Confidence in Knowledge of Data Collection and Use* – Confidence in their knowledge of what is collected by their fitness trackers and how it is used;

C. *Knowledge of Potential Risks* – The plausibility and likelihood of 20 scenarios used in the first study. We developed 20 scenarios describing potential risks and threats relating to fitness trackers based on the literature and news reports of actual breaches;

D. *Attitudes* – The degree of concern about the security and privacy of their fitness tracker data; and

E. *Behaviours* – Current security and privacy practices relating to their fitness tracker.

The pretest questionnaire is included in Appendix B.

Presentation of Information Posters

The type of poster represented our between-subjects treatment variable. Participants viewed one of the four sets of posters (*Explorative*, *Narrative*, *Explorative-Control*, and *Narrative-Control*). We instructed participants to view and read the five posters, one after another, taking as much time as they required. The posters were laser printed in colour on 11×17 inch, uncoated, matte paper.

Post test Questionnaire

After participants viewed the posters, we conducted a post test questionnaire to understand how the experience affected their knowledge, attitudes, behaviours and content retention. In addition, participants assessed the usability of the posters. The questionnaire had 65 questions, including 3 attention-check questions. It consisted of “yes/no/don’t know”, “true/false”, 5-point Likert scales questions, and open-ended text questions. We repeated Sections B – E from the pretest questionnaire for comparison and added two extra sections. We additionally wanted to understand users’:

F. *Retention of information* – Threats and risks associated with fitness tracker use and facts about data collection and use of data; and

G. *Opinions concerning the prototype’s usability* – Usefulness, learnability, ability to capture and maintain attention, enjoyment in reading, appropriateness of visuals and content.

We had two versions of the post test questionnaire, modified slightly to address the presence or lack of visuals in the assigned posters. These are available in Appendix C and Appendix D.

One Week Follow-up Questionnaire

The one week follow-up questionnaire had 50 questions, including 3 attention-check questions. It consisted of “yes/no/don’t know”, “true/false”, 5-point Likert scales questions, and open-ended text questions. We repeated Sections B – F from the pretest and post test questionnaires to compare participants’ responses after one week. The follow-up questionnaire is in Appendix E.

5.2.2 Pilot Testing and Recruitment

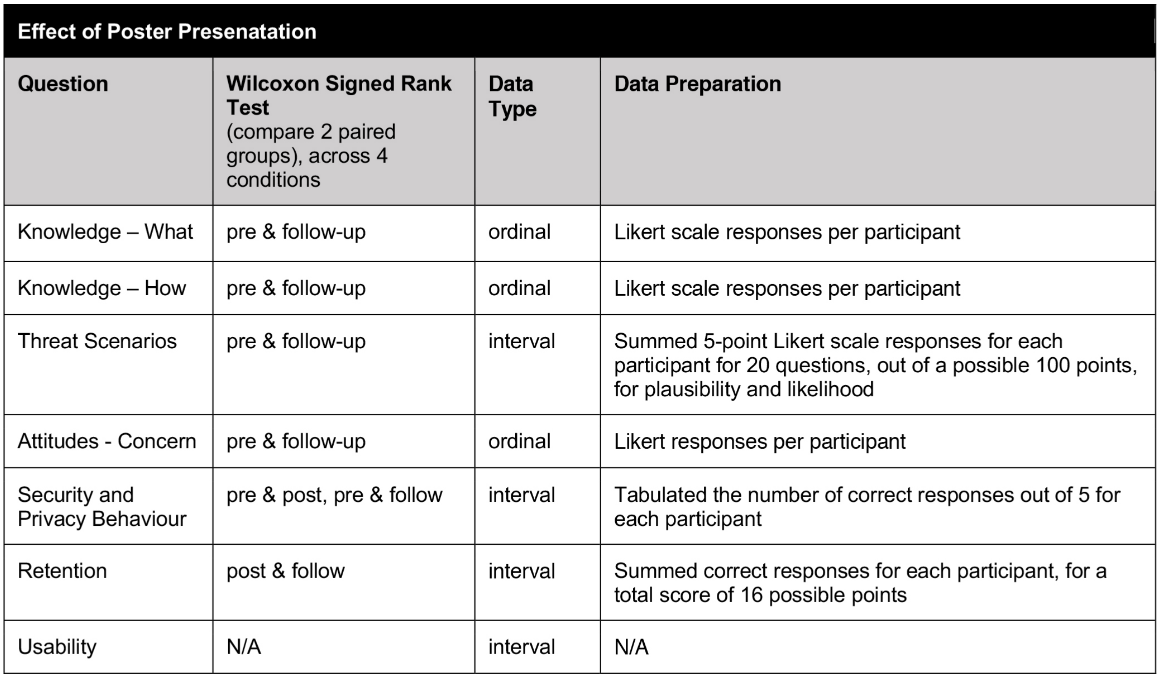
We conducted pilot tests with two participants to identify technical concerns, verify the appropriateness of wording, and test completion time of the questionnaires and posters. None of the materials required adjustment.

We recruited fitness tracker users through social media (Facebook groups), flyers posted around Carleton University campus and by word of mouth. All participants met the following criteria: were over 18 years of age, felt comfortable completing a survey in English, and regularly used a fitness tracker. We paid participants $20 CDN to complete both the lab session and follow-up session.

5.2.3 Analysis

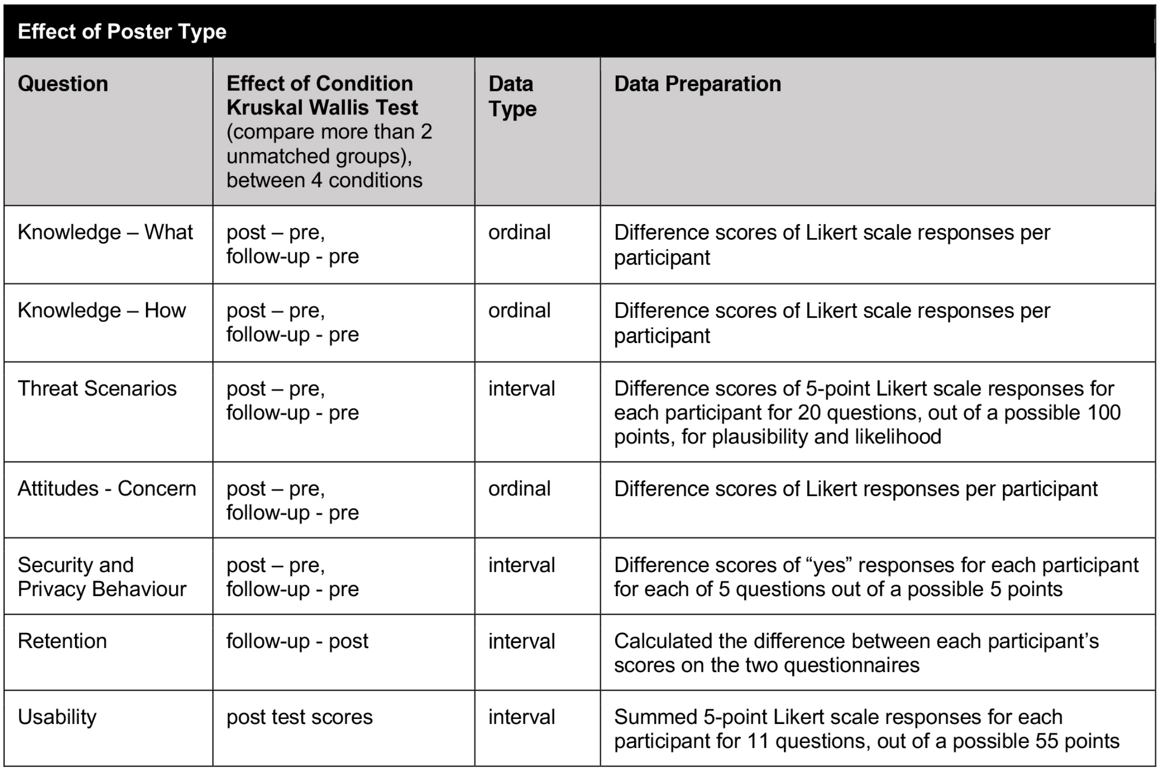
Our independent variables are: 1) Provision of information (within-subjects; measured at three times: pre, post, 1-week follow-up) and 2) Poster type (between-subjects; Explorative, Narrative, Explorative-Control, and Narrative-Control). The dependent variables in each instance are the survey questions. We expected a change from pre to follow-up test responses and an indication of which poster would best lead to a change.

We used descriptive statistics and graphic representations to summarize responses and draw insights. We also used non-parametric statistical methods to test for significant differences in participant responses. To establish if there was an *effect of presenting information*, we used data from all poster conditions combined and conducted Wilcoxon Signed-rank Test looking for differences between the pre, post, and follow-up questionnaire responses. We used participants' Likert scale responses or summed responses and compared them at the different time points (Figure 5.1). To establish if there was an *effect of poster type*, we conducted Kruskal Wallis Tests between the four poster conditions. We calculated the difference scores between time points, then used these scores to compare poster conditions. For the usability questions, we totalled scores for each participant and compared the poster conditions (Figure 5.2).



Effect of Poster Presenatation			
Question	**Wilcoxon Signed Rank Test** (compare 2 paired groups), across 4 conditions	**Data Type**	**Data Preparation**
Knowledge – What	pre & follow-up	ordinal	Likert scale responses per participant
Knowledge – How	pre & follow-up	ordinal	Likert scale responses per participant
Threat Scenarios	pre & follow-up	interval	Summed 5-point Likert scale responses for each participant for 20 questions, out of a possible 100 points, for plausibility and likelihood
Attitudes - Concern	pre & follow-up	ordinal	Likert responses per participant
Security and Privacy Behaviour	pre & post, pre & follow	interval	Tabulated the number of correct responses out of 5 for each participant
Retention	post & follow	interval	Summed correct responses for each participant, for a total score of 16 possible points
Usability	N/A	interval	N/A

Figure 5.1: Breakdown for effect of presenting information analyses



Effect of Poster Type			
Question	**Effect of Condition Kruskal Wallis Test** (compare more than 2 unmatched groups), between 4 conditions	**Data Type**	**Data Preparation**
Knowledge – What	post – pre, follow-up - pre	ordinal	Difference scores of Likert scale responses per participant
Knowledge – How	post – pre, follow-up - pre	ordinal	Difference scores of Likert scale responses per participant
Threat Scenarios	post – pre, follow-up - pre	interval	Difference scores of 5-point Likert scale responses for each participant for 20 questions, out of a possible 100 points, for plausibility and likelihood
Attitudes - Concern	post – pre, follow-up - pre	ordinal	Difference scores of Likert responses per participant
Security and Privacy Behaviour	post – pre, follow-up - pre	interval	Difference scores of “yes” responses for each participant for each of 5 questions out of a possible 5 points
Retention	follow-up - post	interval	Calculated the difference between each participant’s scores on the two questionnaires
Usability	post test scores	interval	Summed 5-point Likert scale responses for each participant for 11 questions, out of a possible 55 points

Figure 5.2: Breakdown for effect of poster type analyses

5.3 Results

We begin by presenting responses to demographic questions along with questions about fitness tracker brand and usage, to provide context. Next, we report the findings of our study in response to the three main research questions. We organize the results based on the section of the questionnaires and address the research questions within each section, as appropriate.

5.3.1 Demographics

We had a total of 34 participants from Ottawa, Toronto and Guelph, Ontario. 23 identified as female, 11 as male. They ranged in age from 19 – 70 years old. 12 participants had studied in a technology-related field (computer science, IT/digital media, graphic/advertising design, communications, media studies). Participants used a variety of fitness tracker brands or digital apps meant for tracking fitness directly from their smart phone to track a variety of activities and biometrics. Counting steps was reported as the most common use of fitness trackers (31/34 participants). Figure 5.3 summarizes participants' reported uses of their fitness trackers.

5.3.2 Confidence in Knowledge

i) Type of Data Collected

On a 5-point Likert scale (from 1, not at all confident to 5, extremely confident) participants rated the confidence they had in their knowledge of the types of data collected by their fitness tracker during the pre, post and follow-up tests. Figure 5.4 provides an overview of responses for the pre, post and one-week follow-up questions combining all conditions. Figure 5.5 illustrates responses to the confidence question per poster condition, for all three questionnaires.

Effect of Presenting Information: The boxplot of the Likert scale responses combining all poster conditions (Figure 5.4) shows the largest interquartile range (IQR) in the pretest, a smaller IQR in the post test and the smallest IQR in the follow-up, with median responses of 3, 4, 4, respectively. These observations suggest an increase in confidence from pre to post and follow-up tests.

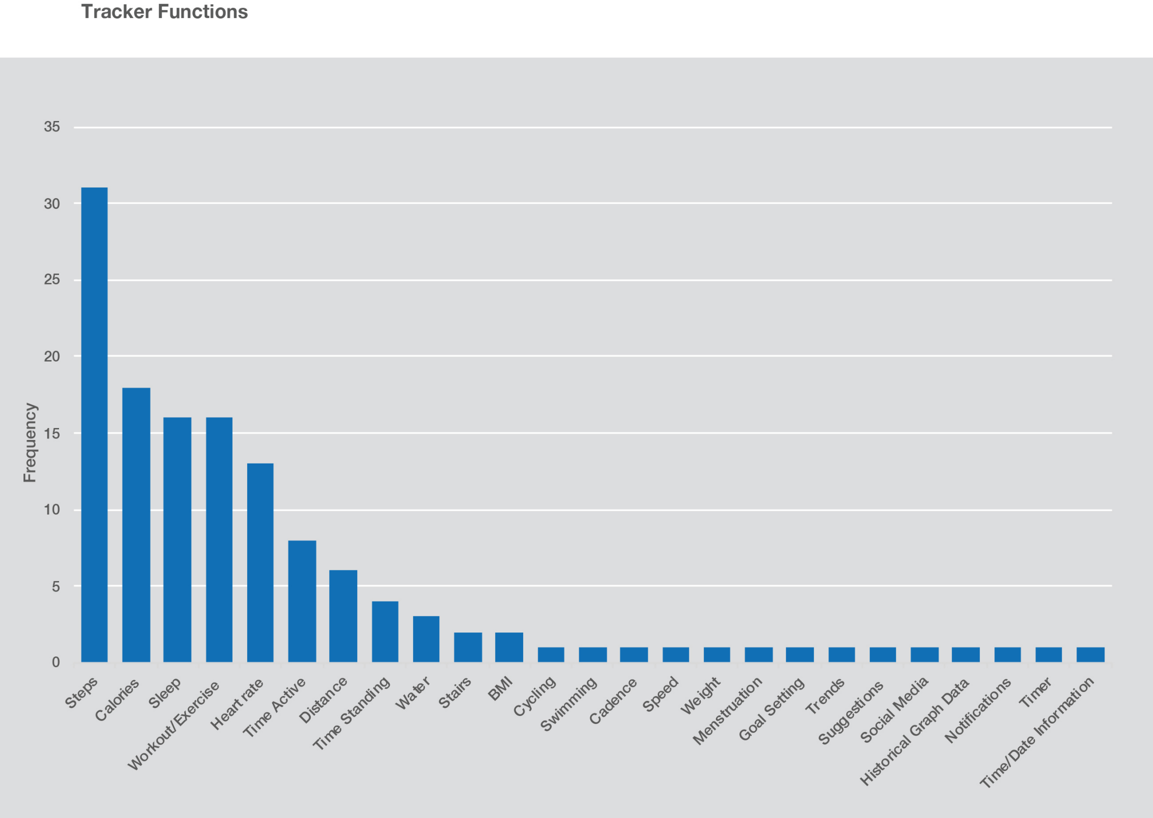


Figure 5.3: Participants' reported uses of their fitness trackers.

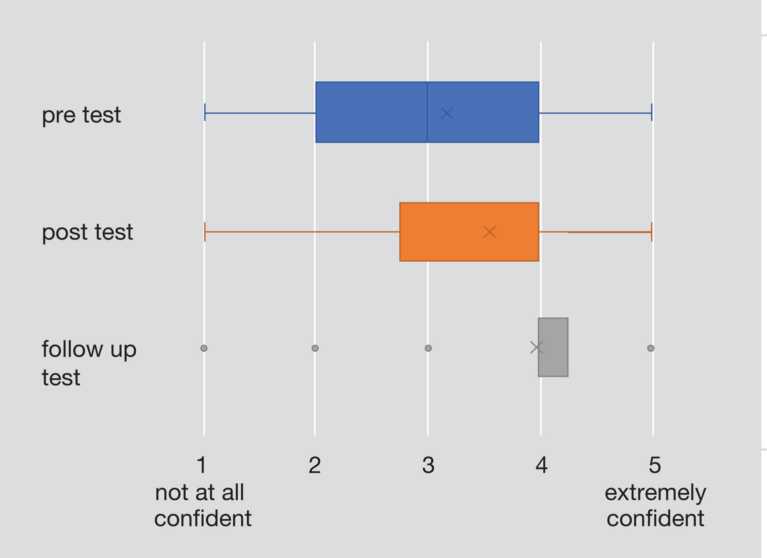


Figure 5.4: Likert scale responses showing participants' confidence in their knowledge of the type of data collected by their fitness trackers

We conducted a Wilcoxon Signed-rank test to compare each participants' pretest and one week follow-up responses for confidence across all poster conditions. The results showed a significant and large effect of presenting information (W = 17, Z = -3.90, p < 0.0001, r = 0.47). We saw a positive effect on participants' confidence in their knowledge of the type of data collected one week after the posters were presented.

Effect of Poster Type: Horizontal stacked bar plots (Figure 5.5) show that participants' confidence increased over time for three of the four poster conditions, except for Explorative-Control, where their level of confidence increased from pre to post test and then decreased for the follow-up test. However, the Explorative-Control follow-up test still showed a high level of confidence. All four poster conditions yielded approximately the same level of confidence for both the post and follow-up tests.

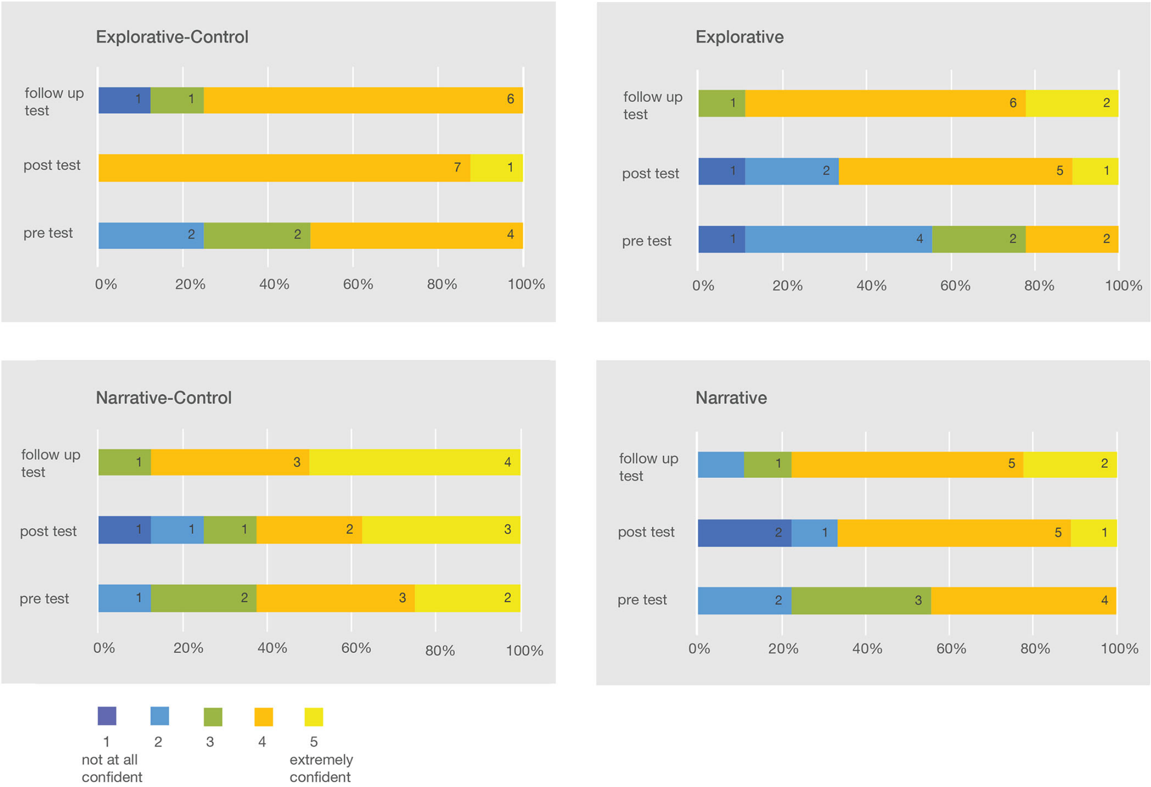


Figure 5.5: Participants' confidence in knowing the type of data collected by their fitness tracker for each poster condition

To assess the change in confidence, we calculated two difference scores for each participant: post minus pretest and follow-up minus pretest. We conducted Kruskal Wallis Rank Sum Tests to compare change in confidence between the four poster conditions. The results show no significant effect of poster type between pretest and post test, ($\chi^2(2)$ = 3.9395, df = 3, p = 0.2681) and between the pre and follow-up tests, ($\chi^2(2)$ = 6.5301), df = 3, p = 0.08848. The type of poster did not affect participants' confidence in knowing the type of data collected.

ii) How Data is Used

On a 5-point Likert scale (from 1, not at all confident to 5, extremely confident) participants rated their confidence in knowing of how their fitness tracker data is used. Figure 5.6 offers a boxplot of Likert scale responses across all poster conditions while Figure 5.7 breaks down the results per condition.

Effect of Presenting Information: Figure 5.6 shows an increase from the pre to post to one week follow-up tests, with median responses of 2, 4, 4, respectively. The largest IQR is evident in the post test, while similar sized are ranges are apparent for both the pre and follow-up tests.

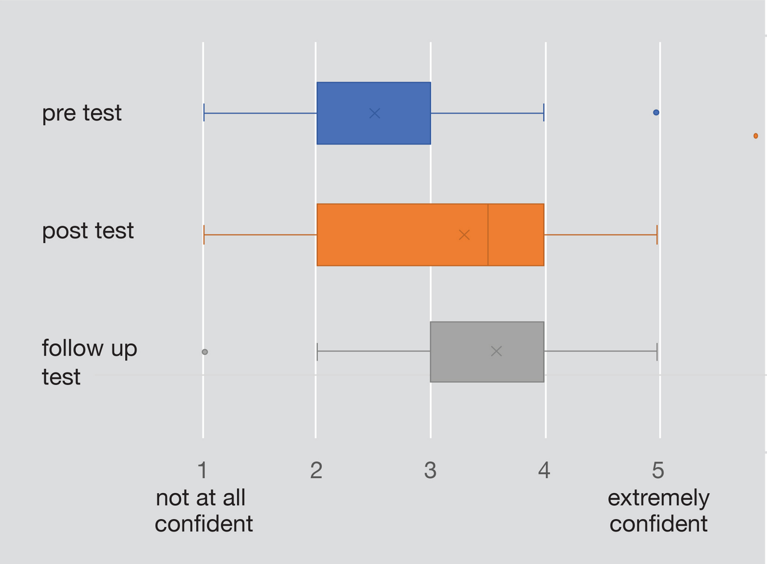


Figure 5.6: Likert scale responses showing participants' confidence in knowing how the data collected by their fitness trackers is used

A Wilcoxon Signed-rank test was conducted using each participants' pretest and follow-up responses across all poster conditions. The test showed a significant and large effect of presenting information (W = 53, Z = -3.99, p < 0.0001, r = 0.48).

We saw a positive effect on the participants' confidence in knowing how their fitness tracker data is used one week after viewing the posters.

Effect of Poster Type: Horizontal stacked bar plots (Figure 5.7) show that participants' confidence in how data is used increased from pre to post to follow-up tests. On visual inspection, it seems that the two Narrative poster conditions show a higher level of confidence for the follow-up test than their Explorative counterparts.

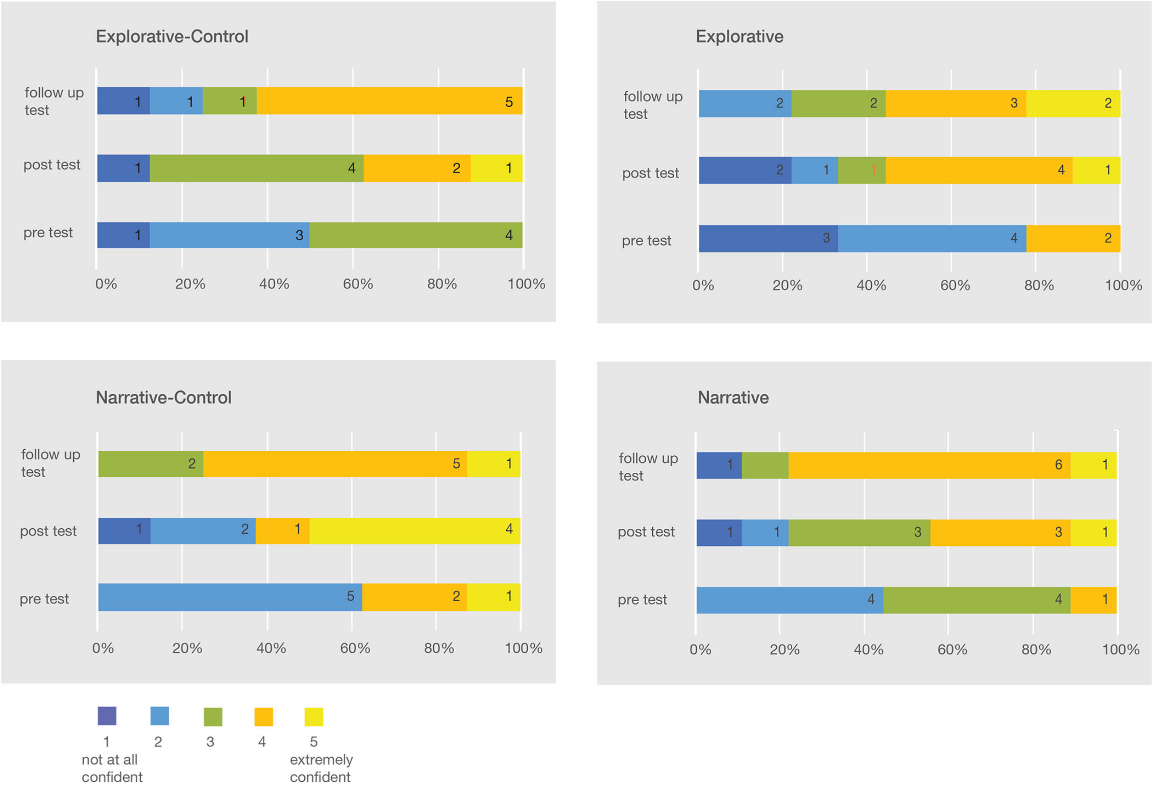


Figure 5.7: Participants' confidence in knowing how the data collected by their fitness trackers is used for each poster condition

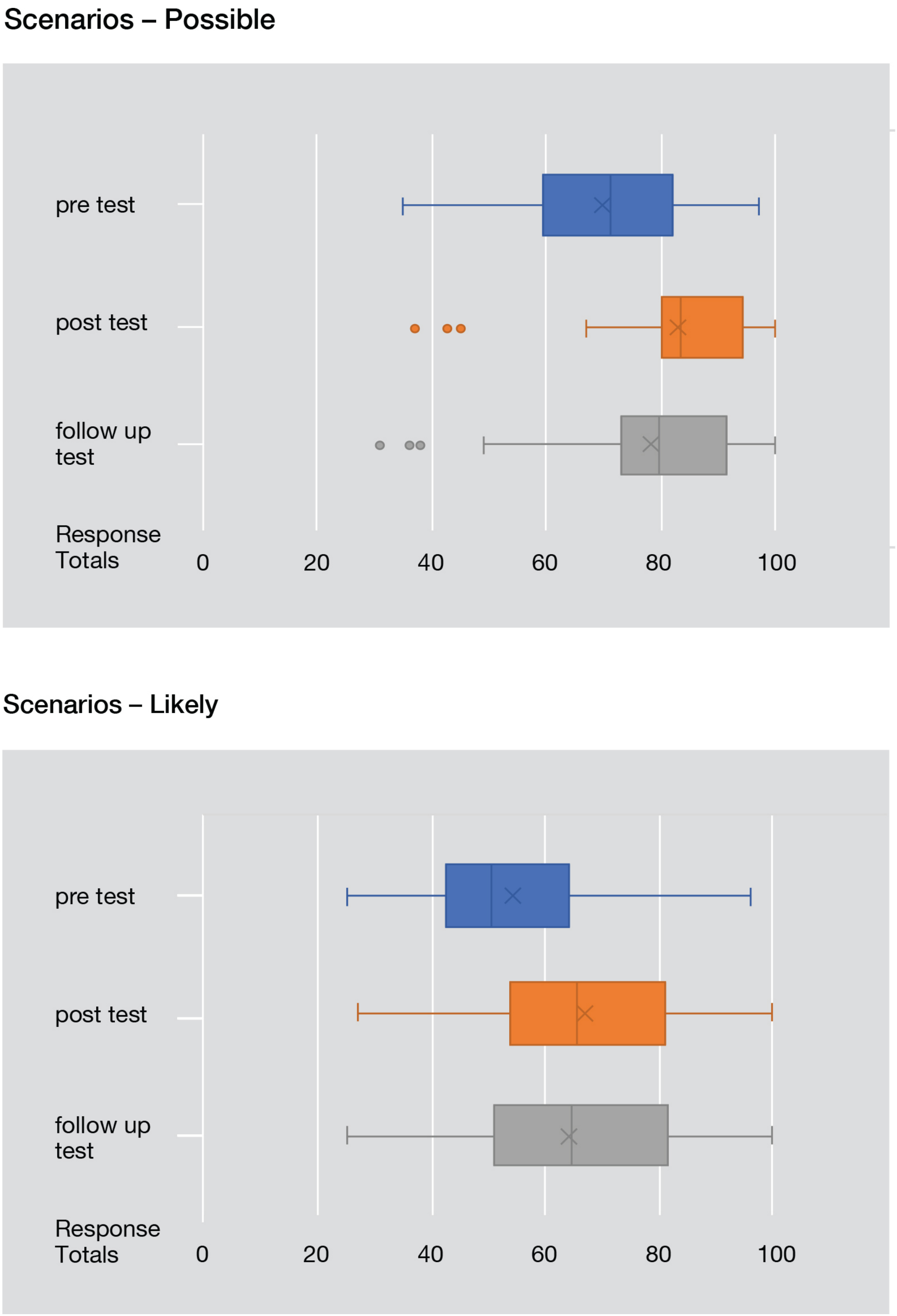
To assess the change in confidence, we again calculated two scores for each participant: post minus pretest and follow-up minus pretest responses. We conducted Kruskal Wallis Rank Sum Tests to compare the change in confidence scores between the four conditions. The test showed no significant effect between pre and post tests, ($\chi^2(2) = 0.7085, df = 3, p = 0.8712$) and the pre and follow-up tests, ($\chi^2(2) = 0.88452, df = 3, p = 0.8292$.) We found no statistical evidence that the type of poster affected participants' confidence in knowing how their fitness tracker data is used.

5.3.3 Knowledge of Potential Threats

We asked participants to rate the plausibility and likelihood of 20 scenarios on a 5-point Likert scale (plausibility from 1, not at all possible to 5, extremely possible and likelihood from from 1, not at all likely to 5, extremely likely) during the pre, post and one week follow-up tests.

We summed the responses to all 20 questions for each participant, out of a possible total of 100 (20 questions × 5-point Likert scale), giving one total for plausibility and one total for likelihood. Figure 5.8 shows boxplots of the pre, post and follow-up totals, combining data across all poster conditions. Overall, participants thought scenarios were plausible but not as likely to occur. There was increase in both plausibility and likelihood from pre to post totals and then a decrease from post to follow-up but not returning to the level of the pretest. The data is also fairly evenly distributed in both plots but likelihood shows a larger IQR and more variance in responses. Figure 5.9 shows heatmaps of the median responses for each of the four poster conditions. Overall, the responses for plausibility are higher than those for likelihood. We see an increase in both plausibility and likelihood from pre to post totals and then a decrease from post to follow-up totals for all four poster conditions. While similar to the other conditions, the Narrative-Control condition shows higher scores, overall for pre, post and follow-up totals for both plausibility and likelihood.

Effect of Presenting Information: A Wilcoxon Signed-rank test was conducted using pretest and follow-up totals to determine if the presentation of posters affected participants' ratings of the plausibility and likelihood of threats. For plausibility, the medians of the pre and follow-up totals were 71.0 and 79.5, respectively. The test showed a significant and large effect of presenting information for plausibility ($W = 77$, $Z = -3.69$, $p = 0.0002$, $r = 0.45$). For likelihood, the medians of the pretest and follow-up totals were 50.5 and 64.5, respectively. The test showed a significant and large effect of presenting information for likelihood ($W = 64.5$, $Z = -41.\ 4$, $p < 0.0001$, $r = 0.50$). We saw a positive change in participants' ratings of the plausibility and likelihood of threats, one week after viewing the posters.



Scenarios – Possible

Scenarios – Likely

Figure 5.8: Pre, post and follow-up total responses to 20 5-point Likert scale questions (for a possible total of 100 points per participant) for the plausibility (top) and likelihood (bottom) of threat scenarios

Effect of Poster Type: We again calculated two difference scores to measure participants' change in perception: post minus pre total and follow-up minus pre total. We used Kruskal Wallis Rank Sum Tests to compare the plausibility and likelihood scores for each poster condition. The tests showed:

- *Plausibility pre–post:* no significant effect of poster type in pre to post totals for plausibility, $\chi^2(2) = 1.7717, df = 3, p = 0.6211$;
- *Plausibility pre–follow-up:* no significant effect of poster type in pre to follow-up totals for plausibility, $\chi^2(2) = 1.5974, df = 3, p = 0.66$;
- *Likelihood pre–post:* no significant effect of poster type in pre to post totals for likelihood, $\chi^2(2) = 2.4131, df = 3, p = 0.4912$; and
- *Likelihood pre–follow-up:* no significant effect of poster type in pre to follow-up totals for likelihood, $\chi^2(2) = 1.6594, df = 3, p = 0.646$.

We saw no statistical evidence that the type of poster affected participants' ratings of plausibility and likelihood of threats.

Explorative-Control

	POSSIBLE			LIKELY		
	Pre	Post	Follow	Pre	Post	Follow
14. A fitness tracker user was identified simply by their gait (walking pattern).	2.5	2.5	3	1	2.5	3
20. Fitness tracker data was used to discriminate users based on race, religion and gender.	2	3.5	3	1.5	2	1.5
4. Data about a woman's menstrual and ovulation cycles were used by an employer for human resource planning.	2.5	4	3	1.5	2.5	2
3. A user's sexual activity was revealed based on the data showing changes in heart rate and intensity of movement.	2.5	4	3	1.5	2	2
17. An adoption agency denied a couple a child a based on fitness tracker data suggesting unhealthy lifestyle.	2.5	4	3	2	2.5	2.5
16. Based on fitness data, city council denied citizens with a high level of fitness, a new fitness facility and running track.	3	4	3.5	2	2	2
5. A hacker denied the user access to his own account until he paid a ransom.	3.5	4	4	1	3	2.5
19. Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.	3.5	4	4.5	3	4	3.5
11. Sleep data suggesting poor cognitive/mental health are used against a job applicant.	3.5	4.5	3.5	1.5	2	2
18. Police officers used fitness tracker data as evidence to arrest someone for a crime.	4	4.5	4	2	3	3
10. Fitness tracker data provided a burglar with the location, number of floors and when a user would be home.	4	4.5	4	2.5	3.5	3
7. Border control officers denied a man entry based on location data showing countries he visited in the past.	3.5	4.5	4	2.5	2.5	3.5
12. Data was intercepted by hackers when transmitting from the fitness tracker device to the server.	4	4.5	4	3.5	4	4
13. Insurance companies offer discounts based on an individual's health and fitness information.	4	4.5	4	4	3	3
1. An employer fired an employee based on tracker data showing fitness activities during work hours.	2.5	5	4	2	3.5	2
2. Life insurance companies cancel coverage of unhealthy people, based on their fitness tracker data.	4	5	3.5	2	2	2
8. A hacker gained access user data and could tell the location and discern the user activity.	4	5	4	2.5	4.5	3.5
9. Heart rate data combined with video footage at the scene helps identify a murder suspect.	4	5	4	2.5	3.5	4
6. Based on running data, an advertiser targeted ads for a specific brand of running shoes.	4	5	4	3.5	4	4
15. Running routes were tracked and mapped, providing an accurate picture of a user's movements.	5	5	4	4.5	5	4

Narrative Control

	POSSIBLE			LIKELY		
	Pre	Post	Follow	Pre	Post	Follow
14. A fitness tracker user was identified simply by their gait (walking pattern).	3.5	4	3.5	2	3	2.5
20. Fitness tracker data was used to discriminate users based on race, religion and gender.	3.5	4	5	2.5	3	3.5
4. Data about a woman's menstrual and ovulation cycles were used by an employer for human resource planning.	4	5	4.5	3.5	4.5	4
3. A user's sexual activity was revealed based on the data showing changes in heart rate and intensity of movement.	3	4	4	3	2.5	3
17. An adoption agency denied a couple a child a based on fitness tracker data suggesting unhealthy lifestyle.	3.5	4	4.5	2	3.5	3.5
16. Based on fitness data, city council denied citizens with a high level of fitness, a new fitness facility and running track.	5	5	5	4	4.5	4
5. A hacker denied the user access to his own account until he paid a ransom.	5	5	4.5	3.5	4	3
19. Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.	4	5	5	3	4	4.5
11. Sleep data suggesting poor cognitive/mental health are used against a job applicant.	4	4.5	4.5	2	2.5	3.5
18. Police officers used fitness tracker data as evidence to arrest someone for a crime.	4.5	5	5	4	5	4
10. Fitness tracker data provided a burglar with the location, number of floors and when a user would be home.	4	4.5	4.5	2.5	3.5	4
7. Border control officers denied a man entry based on location data showing countries he visited in the past.	4	4.5	4.5	3.5	4	4
12. Data was intercepted by hackers when transmitting from the fitness tracker device to the server.	4	5	4.5	3	4	4
13. Insurance companies offer discounts based on an individual's health and fitness information.	5	5	5	4.5	5	5
1. An employer fired an employee based on tracker data showing fitness activities during work hours.	4	5	5	2.5	4	3.5
2. Life insurance companies cancel coverage of unhealthy people, based on their fitness tracker data.	4.5	5	5	3.5	4	4
8. A hacker gained access user data and could tell the location and discern the user activity.	5	5	4.5	3	4.5	3.5
9. Heart rate data combined with video footage at the scene helps identify a murder suspect.	5	5	5	4	5	3.5
6. Based on running data, an advertiser targeted ads for a specific brand of running shoes.	5	5	5	5	5	5
15. Running routes were tracked and mapped, providing an accurate picture of a user's movements.	5	5	5	5	4.5	4.5

Explorative

	POSSIBLE			LIKELY		
	Pre	Post	Follow	Pre	Post	Follow
14. A fitness tracker user was identified simply by their gait (walking pattern).	3	3	3	2	3	3
20. Fitness tracker data was used to discriminate users based on race, religion and gender.	3	3	3	3	2	2
4. Data about a woman's menstrual and ovulation cycles were used by an employer for human resource planning.	4	4	4	2	2	2
3. A user's sexual activity was revealed based on the data showing changes in heart rate and intensity of movement.	3	4	3	2	2	2
17. An adoption agency denied a couple a child a based on fitness tracker data suggesting unhealthy lifestyle.	2	4	3	2	2	2
16. Based on fitness data, city council denied citizens with a high level of fitness, a new fitness facility and running track.	3	4	4	2	2	3
5. A hacker denied the user access to his own account until he paid a ransom.	3	5	4	2	3	4
19. Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.	3	5	5	2	4	5
11. Sleep data suggesting poor cognitive/mental health are used against a job applicant.	3	4	4	2	2	2
18. Police officers used fitness tracker data as evidence to arrest someone for a crime.	3	5	4	2	4	4
10. Fitness tracker data provided a burglar with the location, number of floors and when a user would be home.	4	4	4	2	3	3
7. Border control officers denied a man entry based on location data showing countries he visited in the past.	3	4	4	2	3	3
12. Data was intercepted by hackers when transmitting from the fitness tracker device to the server.	3	5	4	3	4	4
13. Insurance companies offer discounts based on an individual's health and fitness information.	4	5	5	3	4	4
1. An employer fired an employee based on tracker data showing fitness activities during work hours.	3	5	4	2	4	3
2. Life insurance companies cancel coverage of unhealthy people, based on their fitness tracker data.	4	5	4	4	4	4
8. A hacker gained access user data and could tell the location and discern the user activity.	4	5	4	2	4	4
9. Heart rate data combined with video footage at the scene helps identify a murder suspect.	3	4	4	3	4	4
6. Based on running data, an advertiser targeted ads for a specific brand of running shoes.	5	5	5	5	5	5
15. Running routes were tracked and mapped, providing an accurate picture of a user's movements.	5	5	4	4	4	4

Narrative

	POSSIBLE			LIKELY		
	Pre	Post	Follow	Pre	Post	Follow
14. A fitness tracker user was identified simply by their gait (walking pattern).	3	4	4	2	4	4
20. Fitness tracker data was used to discriminate users based on race, religion and gender.	2	4	4	1	2	3
4. Data about a woman's menstrual and ovulation cycles were used by an employer for human resource planning.	3	4	3	1	2	2
3. A user's sexual activity was revealed based on the data showing changes in heart rate and intensity of movement.	2	4	3	2	2	2
17. An adoption agency denied a couple a child a based on fitness tracker data suggesting unhealthy lifestyle.	4	4	4	2	2	2
16. Based on fitness data, city council denied citizens with a high level of fitness, a new fitness facility and running track.	4	4	4	2	2	2
5. A hacker denied the user access to his own account until he paid a ransom.	4	4	4	2	3	3
19. Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.	3	5	4	3	5	4
11. Sleep data suggesting poor cognitive/mental health are used against a job applicant.	4	4	4	2	2	2
18. Police officers used fitness tracker data as evidence to arrest someone for a crime.	3	5	4	2	4	3
10. Fitness tracker data provided a burglar with the location, number of floors and when a user would be home.	4	5	4	2	4	3
7. Border control officers denied a man entry based on location data showing countries he visited in the past.	4	4	4	3	4	3
12. Data was intercepted by hackers when transmitting from the fitness tracker device to the server.	4	4	4	3	4	4
13. Insurance companies offer discounts based on an individual's health and fitness information.	4	5	4	3	4	4
1. An employer fired an employee based on tracker data showing fitness activities during work hours.	3	4	4	2	3	3
2. Life insurance companies cancel coverage of unhealthy people, based on their fitness tracker data.	3	4	4	2	3	3
8. A hacker gained access user data and could tell the location and discern the user activity.	4	5	4	3	4	4
9. Heart rate data combined with video footage at the scene helps identify a murder suspect.	4	5	4	4	5	4
6. Based on running data, an advertiser targeted ads for a specific brand of running shoes.	4	4	4	4	4	4
15. Running routes were tracked and mapped, providing an accurate picture of a user's movements.	4	4	4	4	4	4

Figure 5.9: Median responses for Pre, post, and follow-up test Likert scale questions about plausibility and likelihood of threat scenarios for each condition

5.3.4 Attitudes

On a 5-point Likert scale (from 1, not at all concerned to 5, extremely concerned) participants rated their concern about the security and privacy of their fitness data during the pre, post and follow-up tests. Boxplots combining data across all poster conditions (Figure 5.10) show an increase in concern from pre to post tests and then a levelling off for the follow-up tests (medians: 2, 4, 4, respectively). However, the smaller overall range and IQR range for the follow-up indicates less variation in the responses at that point. Figure 5.11 shows stacked horizontal bar graphs of participants' Likert responses per poster condition. Participants who viewed the two Control posters show an increase in concern for security and privacy from the pre to post test and a drop in concern from the post to one week follow-up test, but not to the level of the pretest.

Participants who viewed the Explorative and Narrative posters also showed an increase in concern from pre to post test but the change was not as substantial as the Control posters. Instead, there was a slight increase in concern from post to one week follow-up. In addition, the Narrative and Narrative-Control responses for both the post and one week follow-up test were more weighted toward extremely concerned. Interestingly, Narrative-Control shows the greatest increase from pre to post test.

Effect of Presenting Information: We used a Wilcoxon Signed-rank test to compare users' concern in the pretest and one week follow-up responses across all poster conditions. The test showed a significant and large effect of presenting information (W = 77, Z = -4.9, p < 0.0001, r = 0.59). We saw a significant increase in the participants' concern about security and privacy one week after viewing the posters.

Effect of Poster Type: To assess participants' change in concern, we calculated two difference scores for each participant: post minus pretest and follow-up minus pretest responses. We used Kruskal Wallis Rank Sum Tests to compare the change in concern between the four poster conditions. The test showed no significant effect of poster type between pretest and post tests, $(\chi^2(2) = 0.81315, df = 3, p = 0.8463)$, nor between the pre and follow-up tests, $(\chi^2(2) = 2.5012, df = 3, p = 0.4751$. We saw no changes in concern between the four poster conditions.

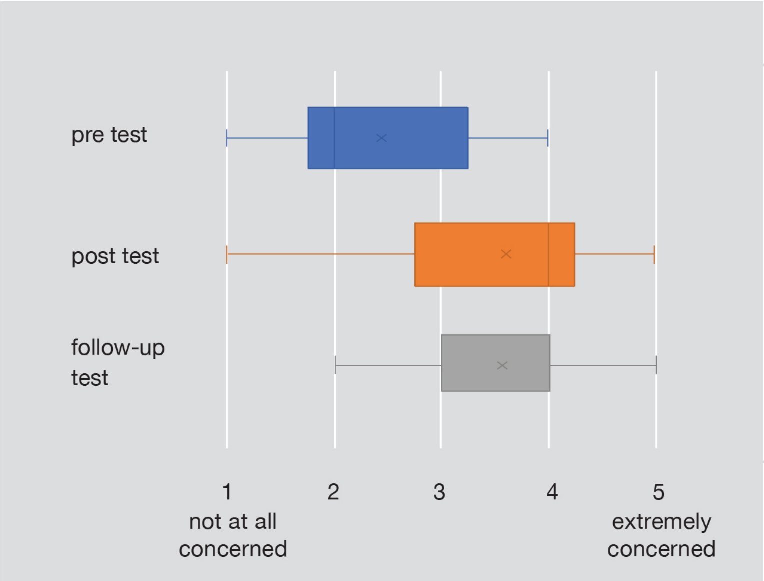


Figure 5.10: Likert scale responses showing participants' concern about security and privacy

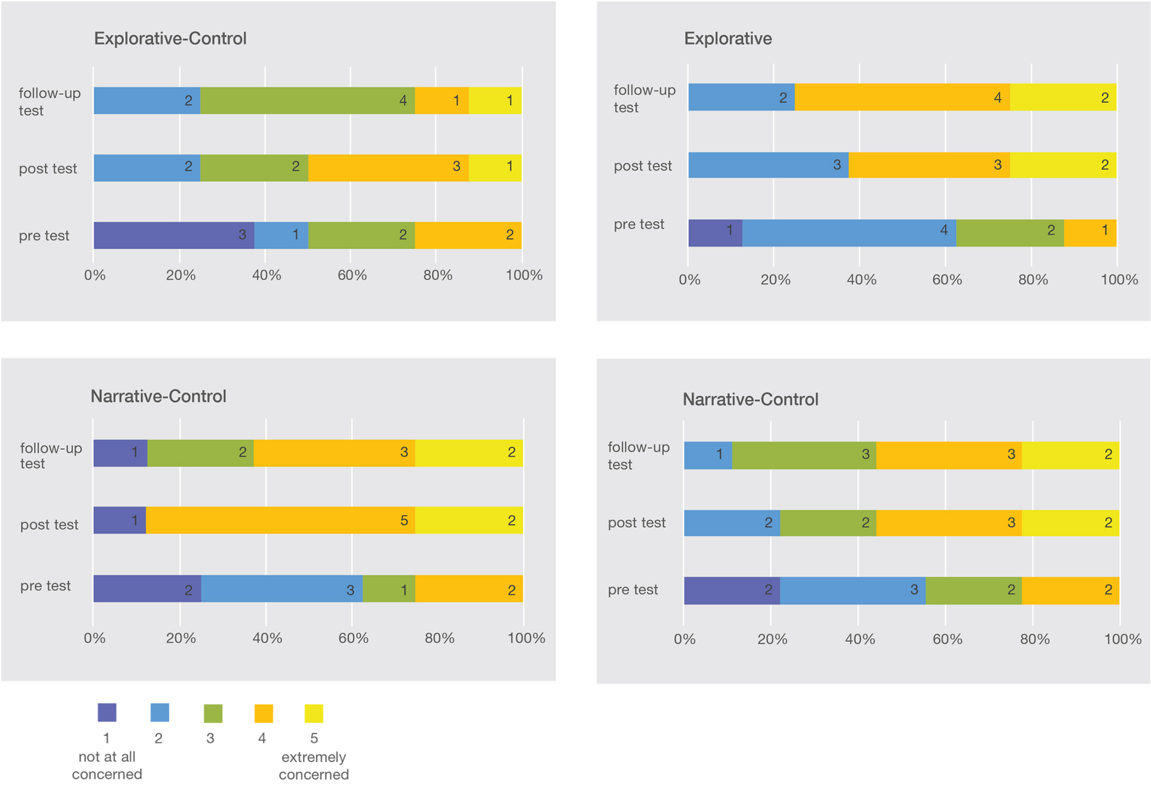


Figure 5.11: Participants' level of concern for security and privacy by poster type

5.3.5 Behaviour

To distinguish between privacy intentions and reported behaviours, we asked participants to respond to five questions about managing their fitness tracker security and privacy with “yes”, “no” or “don’t remember” /“don’t know” at three different points during the study: before the viewing of posters (“have you...”), immediately after (“will you...”, and one week later “did you...”). Stacked bar graphs (Figure 5.12) show a spike in reported intention to take action to protect their security and privacy in the post test, then a reduction in the follow-up test when reporting what they actually did, but remaining above the pretest level. Figure 5.13 provides heatmaps of the percentages of “yes” responses for each of the four poster conditions. As was the case with the combined results, each condition showed an increase in “yes” responses from the pre to post scores for all questions. For the one week follow-up scores, most conditions show a slight decline. Approximately one-third show a return to pretest levels for questions about changing default security and privacy settings and setting preferences for sharing data, except for the Narrative-Control condition which shows only a small reduction.

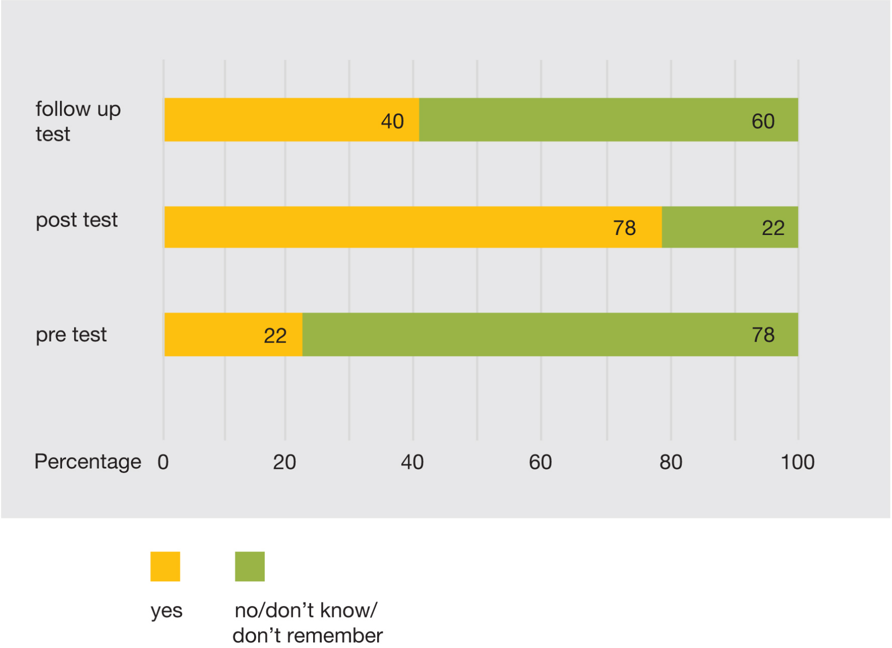
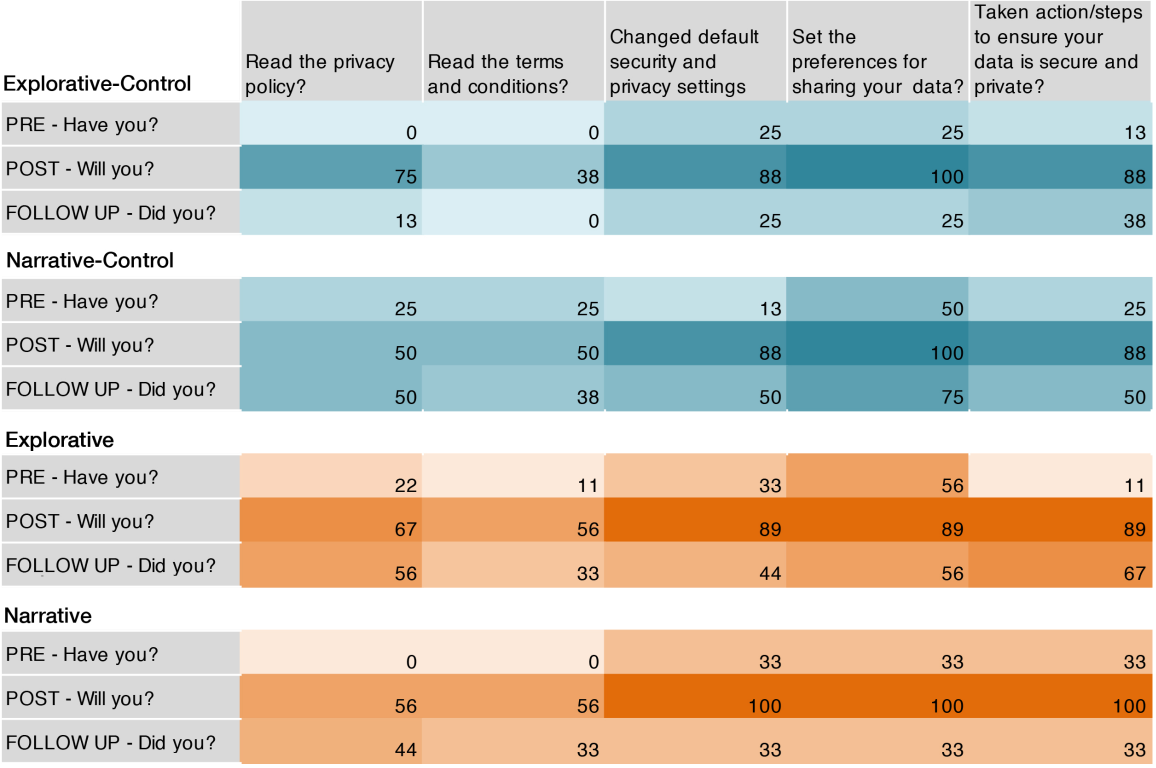


Figure 5.12: Percentage of of total “yes” and “no” and “don’t remember’/“don’t know’ responses for questions about security and privacy behaviours

In preparation for the inferential statistics, we totalled each participant's "yes" responses for a score of 5 possible points (5 questions) for the pre, post and follow-up tests.

Effect of Presenting Information: We used a Wilcoxon Signed-rank test to compare the pre and post scores and one to compare pre and follow-up scores across all poster conditions. The results showed a large effect of presenting information over the short-term, (W = 6.5, Z = -5.52, $p < 0.0001$, r = 0.67), and a moderate effect of presenting information over the longer term, (W = 23.5, Z = -2.58, p = 0.01, r = 0.31). We found a statistically significant improvement in participants' reported intended security/privacy behaviours after viewing the posters. This effect was largest immediately after viewing but persisted one week later. The follow-up test asks participants "did you...", so any improvement over the pretest scores suggests that participants actually took steps to enhance their privacy in the week after viewing the posters.



Explorative-Control	Read the privacy policy?	Read the terms and conditions?	Changed default security and privacy settings	Set the preferences for sharing your data?	Taken action/steps to ensure your data is secure and private?
PRE - Have you?	0	0	25	25	13
POST - Will you?	75	38	88	100	88
FOLLOW UP - Did you?	13	0	25	25	38
Narrative-Control					
PRE - Have you?	25	25	13	50	25
POST - Will you?	50	50	88	100	88
FOLLOW UP - Did you?	50	38	50	75	50
Explorative					
PRE - Have you?	22	11	33	56	11
POST - Will you?	67	56	89	89	89
FOLLOW UP - Did you?	56	33	44	56	67
Narrative					
PRE - Have you?	0	0	33	33	33
POST - Will you?	56	56	100	100	100
FOLLOW UP - Did you?	44	33	33	33	33

Figure 5.13: Percentage of "yes" responses for security and privacy behaviours by poster condition

Effect of Poster Type: Using the three reported behaviour scores, we calculated the change between the post minus pre score and between the follow-up minus pre score. We used Kruskal Wallis Rank Sum Tests to compare the change in behaviour scores between the four poster conditions. The first test showed no significant effect of poster type for the pre/post change, ($\chi^2(2) = 1.4907, df = 3, p = 0.6844$) and no significant effect of poster type for the pre/follow-up change, ($\chi^2(2) = 1.8802, df = 3, p = 0.5976$). The type of poster did not affect participants' reported security and privacy behaviours.

5.3.6 Retention of Information

To evaluate retention of the information on the posters, we asked participants to respond to sixteen "true/false" questions, immediately after viewing the prototypes and one week later with a follow-up questionnaire. Correct responses for each participant were totalled for a score of 16 possible points for each of the post and follow-up tests.

Figure 5.14 shows boxplots of the number of correct responses across all conditions combined. It shows a high number of correct responses for both the post and follow-up tests. The median number of correct responses is 16 and 15, respectively, with responses ranging from 11-16 but the IQR's for both are between 14 and 16. Figure 5.15 shows the number of correct responses per poster condition. In examining the boxplots, all versions of the posters yielded a high retention rate in both the post and follow-up tests. In each case, one-half of the responses was 15/16 or better. The Narrative-Control condition yielded the highest responses in the post test.

Effect of Presenting Information: We could not assess the effect of presenting information from the pre to follow-up tests since we did not ask these questions in the pretest. We did, however, explore whether participants retained the information between the post and follow-up tests, one week later. We used a Wilcoxon Signed-rank test to compare users' retention of information for the post and follow-up responses across all poster conditions. The test showed no significant difference (W = 105, Z = -0.38, p = 0.70, r = 0.05). There was no change in retention of information from the post to one week follow-up tests.

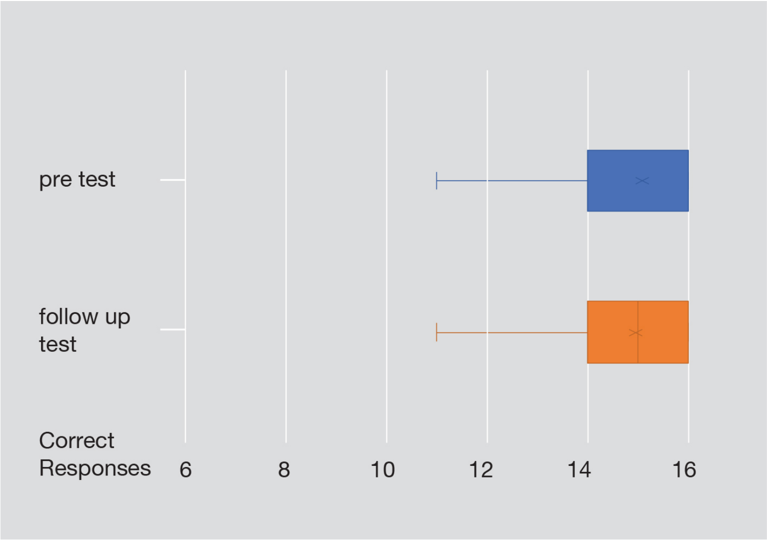


Figure 5.14: Total number of correct responses (out of 16) for the retention of information questions on the post and follow-up tests

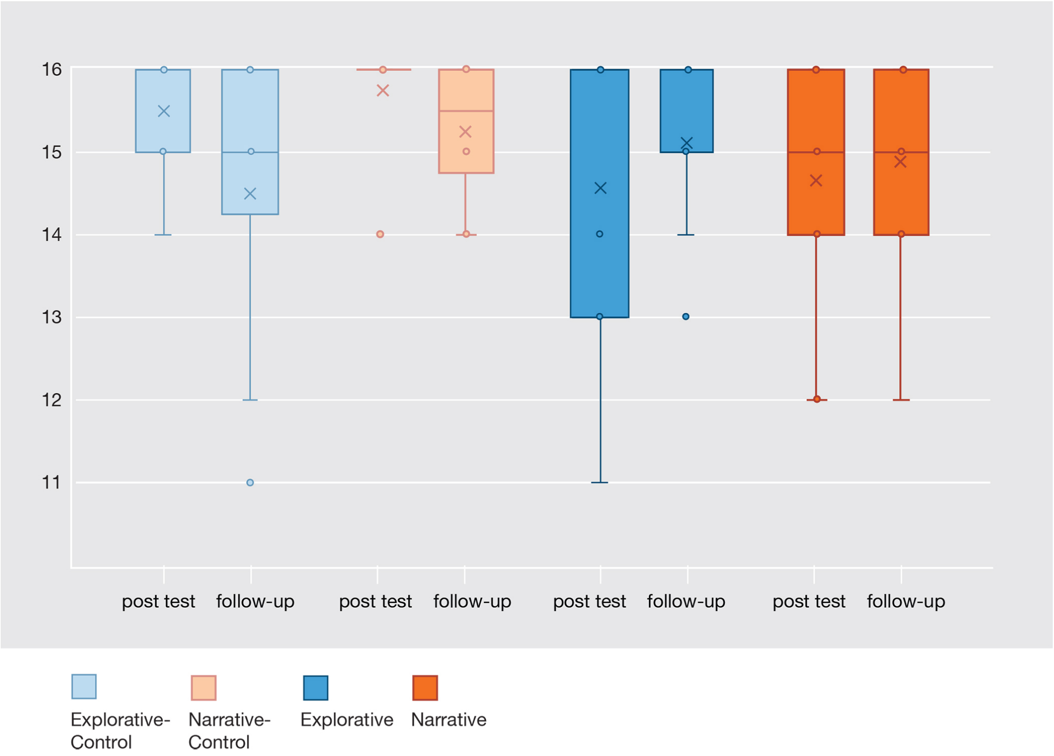


Figure 5.15: Correct responses out of 16, indicating retention of information for post and follow-up tests by poster type

Effect of Poster Type: We calculated the difference in retention for each participant by subtracting the follow-up score minus the post test score. We used a Kruskal Wallis Rank Sum Test to compare retention between the four poster conditions. The test revealed no significant effect of poster type for retention ($\chi^2(2) = 4.8843, df = 3, p = 0.1805$). We saw no difference in how much information participants retained based on which posters they viewed.

5.3.7 Usability

On a 5-point Likert scale (from 1, strongly disagree to 5, strongly agree) participants responded to questions about the usability of the posters. Participant responses were totalled for a score of 55 possible points (11 questions × 5-point Likert scales). Figure 5.16 indicates the median scores are quite high and similar in all four poster conditions, except for the Explorative-Control version, which is approximately 5 points lower. Explorative-Control also has a larger IQR range, showing more variability.

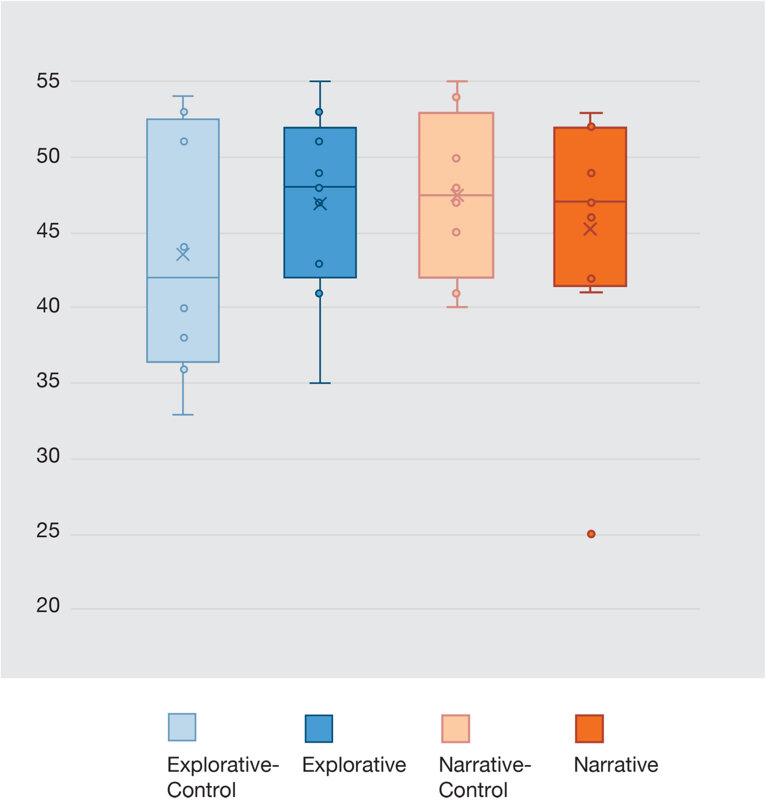
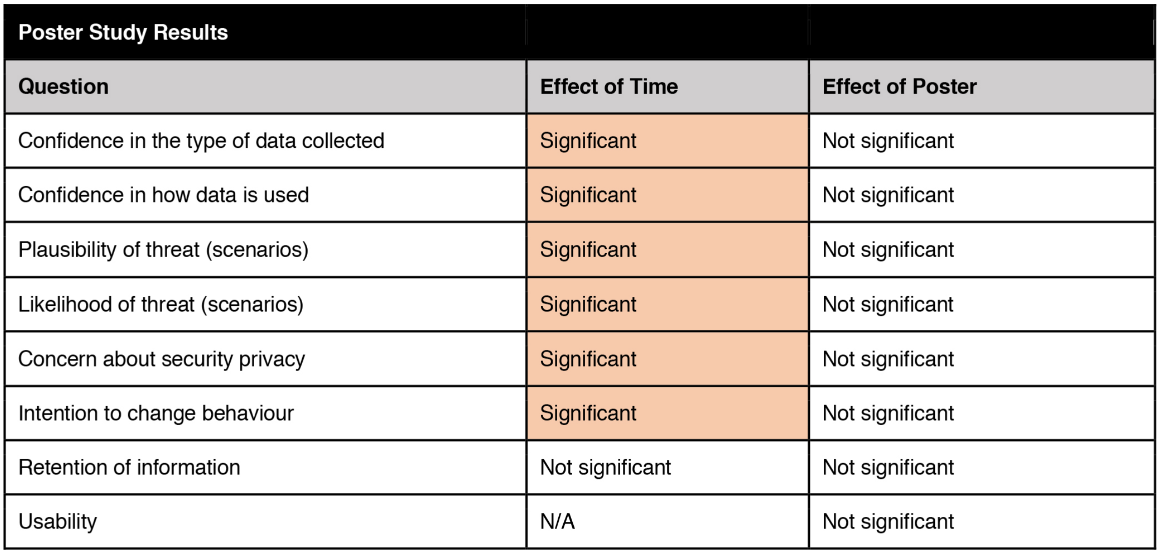


Figure 5.16: Usability scores out of 55 per poster type

Effect of Poster Type We used a Kruskal Wallis Rank Sum Test to compare scores for the four poster conditions. The test showed no significant effect on the usability score between the four poster conditions, $(\chi^2(2) = 1.1563, df = 3, p = 0.7635)$. We saw no difference in the reported usability scores between the different posters.

5.4 Discussion

Figure 5.17 summarizes the statistical results from our study. In this section, we discuss the results in relation to the research questions guiding this study.



Poster Study Results		
Question	**Effect of Time**	**Effect of Poster**
Confidence in the type of data collected	Significant	Not significant
Confidence in how data is used	Significant	Not significant
Plausibility of threat (scenarios)	Significant	Not significant
Likelihood of threat (scenarios)	Significant	Not significant
Concern about security privacy	Significant	Not significant
Intention to change behaviour	Significant	Not significant
Retention of information	Not significant	Not significant
Usability	N/A	Not significant

Figure 5.17: Summary of poster study results

RQ1 Effect of Presenting Information – *Does presenting information about fitness tracker security/privacy affect users' knowledge, attitude and behaviours?* We found evidence that presenting information about fitness tracker security/privacy did affect users' knowledge, attitude and behaviours, by making them more aware, making them more concerned, and leading them to take protective actions.

RQ2 Effect of Poster Type – *Does visual design and messaging affect users' knowledge, attitude and behaviours?* We found no statistically significant differences between the four types of posters presented in our study. The type of poster design and messaging did not affect users' knowledge, attitude and behaviours.

RQ3 Usability – *Which poster type do users deem most usable?* We found no statistically significant differences for usability between the four types of posters, therefore, we were unable to determine which poster type was most usable.

Given these results, most of our discussion focuses on how informing participants about privacy generally resulted in a change.

5.4.1 Effect of Presenting Information

Increased confidence in what they know: The literature indicates that users are unaware of the type of data collected by their fitness trackers and how it is used [42, 76]. In this second study, we found participants' *confidence* in both their knowledge of the type of data collected by their tracker and how this data is used increased significantly after they were presented with information about privacy. These results suggest that even presenting a brief and relatively high-level overview is enough to boost users' confidence and that the effect lasted for at least a week. This is important because Sawaya et al. [63] found that confidence in security knowledge affects user behaviour intentions more than their actual knowledge. The authors also noted that this has implications for how we educate users and suggest introducing approaches to increase user confidence in their ability to manage their security, for example, by providing timely and easy access to help for decision-making.

We must, however, be cautious to ensure users do not become overconfident. The *overconfidence heuristic* [37] explains how people tend to overestimate their skills and knowledge when they are overconfident. With fitness tracker data, over-confident users might unknowingly give up more personal information than they intend to. Given Sawaya et al.'s findings, we are hopeful that including strategies for confidence-building when educating users will serve to support rather than undermine their ability to manage their security and privacy. Further research is necessary to understand confidence/overconfidence and the effects it has on security and privacy behaviours.

An increase in understanding of threat scenarios: According to the *optimism bias*, users tend to think they are less likely to experience a privacy breach in comparison to others [15]. Aktypi et al. [1] found participants believed there is a low risk of anything happening to them, since none of their friends had experienced a negative incident. Because of this tendency towards optimism, we felt it important to gauge users' perceptions of the plausibility and likelihood of security and privacy threats.

We found, overall, participants thought scenarios were plausible but not as likely to occur. Participants' ratings of the plausibility and likelihood of threats increased after viewing the posters. Our results suggest presenting information has an immediate effect which diminished slightly over time.

Gold et al. [28] have found that people tend to exhibit more optimism with negatively framed events. Accordingly, this would have implications when educating users about security and privacy threats: presenting strategies for preventing threats rather than emphasizing negative aspects of threats could promote better protection practices. In our study, we used both negative and positive messages: we presented threat scenarios and followed up by suggesting a set of actions to mitigate risk. The intention was to inform users but at the same time, provide actionable solutions. Our results show an increase in participants' ratings for likelihood, and users took action to protect their data. This shows it is possible to use both types of messaging to prompt users to change their security and privacy behaviours. Further research would allow us to better understand the nuances of messaging types intended to incite behaviour change with fitness tracker users.

Of the top six scenarios rated most plausible and likely to occur, three were similar to instances of fitness tracker breaches recently reported in the media:

- Heart rate data combined with video footage at the scene helped identify a murder suspect [30];
- Running routes were tracked and mapped, providing an accurate picture of a user's movements [56]; and
- Insurance companies offered discounts based on an individual's health and fitness information [6].

Two were instances of similar use/misuse of data occurring with other digital platforms and had been reported in the media:

- Based on running data, an advertiser targeted ads for a specific brand of running shoes [48]; and
- Data collected by a fitness tracker left people open to identity theft [60], profiling [34] , stalking [44] and extortion [29].

The sixth scenario was an imagined threat based on the reporting of employer sponsored health and wellness programs, where employers supply employees with fitness trackers [25]:

- An employer fired an employee based on tracker data showing fitness activities during business hours

Similar to an example of the *availability bias* put forth by Gerber et al. [27], our participants rated some threats as more plausible and more likely to occur because they had these "available" in their memory through exposure to media. Fulton et al. [26] found users' beliefs about computer security are associated with fictional representations from film and television, even when the representations are inaccurate. To take advantage of this influence, they suggest collaborating with the entertainment industry to help them portray security realistically so users might make better security decisions. Similarly, we see potential with the popular news media. If used effectively, it can be a powerful tool to bring awareness of potential threats to users. Researchers could include novel ways of disseminating their findings, in an effort to reach a wider audience.

In the privacy risk literature [20], the level of risk is assessed based upon likelihood and severity of an event. As described by De et al. [20], a variety of both quantitative and qualitative methods are used to analyze the level of risk. For example, quantitative assessments can assign a single value of risk for a specific scenario by multiplying its likelihood by its severity. An example of a qualitative assessment describes mapping the dimensions "severity" and "likelihood", and categorizing them as either "low", "medium"or "high". These approaches, while beyond the scope of this study, might prove valuable to understand users' perceptions of risk and merit further investigation.

Increased concern about security and privacy: Users' concern increased after they were presented with the posters. This can be interpreted as a promising result. However, the result can also be explained as an effect of simply participating in the study. Previous research shows users may express privacy and security concerns but often display contradictory behaviour [52]). While this behaviour is frequently explained as the *privacy paradox*, current research suggests there are multiple factors associated with the dichotomy [27]. In some instances, users show concern but continue to use devices because of the benefits they gain (*i.e. privacy calculus*) [27]. Other researchers have found both high knowledge and high concern are predictors of good privacy and safety practices in the context of mobile devices [39], giving us hope that awareness campaigns or education may have a positive effect on users' behaviour.

An increase in taking steps to protect their security and privacy: Privacy intentions (what users say they will do) are not necessarily a good indication of privacy behaviour (what users actually do) [27, 37]. To understand if exposure to security and privacy information would affect participants' protection behaviours, we asked 5 questions about specific actions before exposure to the information posters, immediately after and again, one week later. This strategy allowed us to capture the baseline behaviour, intended behaviour, and reported behaviour. Responses showed participants intended to take protective steps after seeing the posters, and that some participants (although not all) reported a change in their behaviour one week later. The follow-up test totals were almost double those of the pretest.

For most questions, participants' "yes" responses were low for the baseline pretest, confirming results from previous research: fitness tracker users are not very active in protecting their fitness tracker data [1, 42]. On closer inspection, we can begin to see some of the specific areas awareness an education may be most helpful to users. The question showing the greatest increase related to reading the privacy policy. There were mixed results for changing default security and privacy settings and setting sharing preferences. For these two questions, most participants indicated a strong intention to take action but most follow-up responses remained at the pretest level. Based on these responses, we see a need to emphasize how data can be compromised depending on who it is shared with and the importance of attending to privacy and sharing settings.

Retention of information: There was no significant change from the post to follow-up tests in participant responses on the questions relating to the information from the posters, suggesting that participants retained the information they learned. Given the high scores, we can surmise that the information may have been salient enough to make it memorable. However, we are also cautious because the high scores (between 14 and 16 out of a possible 16) suggest a ceiling effect may have occurred. This may be due to the low difficulty of the questions or the high education level of the participants. For future work, it may be necessary to re-evaluate the questions to ensure they are difficult enough and/or test with participants who are more representative of the larger population.

5.4.2 Effect of Poster Type

We found no effect of poster type. In short, differences in our visual designs and messaging did not have a measurable effect on users' knowledge, attitude and behaviours.

We primarily attribute these results to the small sample sizes assigned to each condition (8 or 9 participants per condition). In some instances, visual inspection of the data suggested differences between poster conditions but none were statistically significant. However, we did observe interesting anomalies with the Narrative-Control, where it had higher scores on multiple questions.

The Narrative-Control poster was mainly black and white text and contained no images but relied heavily on guiding the user through the information with a prescribed story. We did not observe the same pattern of responses from viewing the Narrative poster, which additionally contained visuals. Thus, we cannot say with certainty that using a structured, storytelling approach heightens awareness. It is, however, worth examining how a Narrative approach (with and without visuals) affects users' knowledge, attitudes and behaviours. It could also be that undetermined characteristics of that particular participant group made them more sensitive to the presentation of the posters.

While the content (information) contained in the posters was the same for each, the visual and text treatment varied. It is evident from our results, that the content we used had a positive effect on participant responses. Given the results of our study, however, it is not yet evident which text and visuals are best suited to affect a change.

5.4.3 Limitations

Our sample may not be representative of the entire population of fitness tracker users. Participants ranged in age from 19 – 70 years, however, 62% were between the ages of 19 – 29 and thus, did not necessarily reflect the views of a wider range of users. Because of the limited number of participants (32, with either 8 or 9 for each condition), our results for effect of poster type are not reliable. We also note that our survey collects self-reported responses; these may not be completely objective and may not reflect actual behaviours. The artificial nature of viewing posters in a lab setting may yield different results than would occur in a naturalistic setting (for example, a poster campaign in a busy transit system frequented by users) because our study design does not take into consideration external influences that would be found in a realistic setting. We also acknowledge that the effects we found in this study could be due simply to raising general awareness about privacy concerns and not necessarily a result of viewing the information posters.

5.5 Summary

We compared the effectiveness of our four sets of posters for improving fitness tracker users' knowledge, behaviour, and attitudes towards privacy. We found that viewing the posters had a positive impact on participants. This effect lasted for at least a week after viewing and participants reported changes in their behaviour as a result. However, given our small sample size, we were unable to determine which of our poster designs was most effective.

Chapter 6

Discussion and Conclusion

The main objective for this thesis work was to enhance user awareness of the security and privacy risks related to the collection of their fitness data. In this section, we discuss how we fulfilled this objective by providing insights and recommendations, gleaned from our two studies.

6.1 Insights and Recommendations

6.1.1 A Method for Measuring Privacy Intentions and Behaviours

Our most important finding and the goal of the second half of this thesis was to prompt a change in fitness tracker users' security and privacy protection behaviour with the presentation of information posters.

In describing the literature on privacy attitudes and behaviour, Kokolakis [37] makes a distinction between privacy intention and privacy behaviour and notes that many of the papers under review confound intention and behaviour. We developed a series of questions and posed them at three different points in our study (pre, post and follow-up test):

- before viewing information posters (baseline behaviour);
- immediately after presentation (intention to act); and
- and one week later (long term behaviour.)

The questions were comprised of one general question and four specific protection behaviours. For the different test instances, we asked "Have you?", "Will you?", and "Did you?"

With this approach, we were able to determine whether the intervention is successful because we make the distinction between privacy intentions and reported behaviours, and we measure both. We found this methodological choice effective and would recommend it to others trying to evaluate the effectiveness of an educational intervention. As an extension, it would be plausible to add extra follow-up tests (e.g., after two weeks, after one month, or longer) to capture later behavioural changes.

6.1.2 Ensuring Follow Through of Protection Behaviours

In many cases, users indicated an intention to change and reported an actual change one week later. Two questions asked about actions that could directly improve their privacy (changing default security and privacy settings and setting sharing preferences). For these two questions, most participants indicated a strong intention to take action but most follow-up responses remained at the pretest level. There are many possible reasons for this lack of follow-through. We cannot determine from our data what happened, but we offer some possible explanations: 1) They viewed their current settings and found them to be satisfactory, so no changes were needed; 2) Participants simply forgot or were short for time; 3) The design of the interface was not usable and participants were unable to find, access, or otherwise change the privacy settings; 4) The interface provided limited sharing options and users could not change settings to match their preferences.

From our first study, we found that users had complex preferences relating to the types of data and the intended recipients. It is possible that the level of granularity for sharing specific types of data and specifying recipients is insufficient on current interfaces. For example, Fitbit provides only three options for sharing: private, friends only and public.

Within the context of user education, we suggest sending a reminder or prompt to users, shortly after an education session. Similarly, for studies where measuring behaviours is the goal, researchers could follow up with participants, as a reminder. Additionally, the post test questionnaire could include questions asking participants to elaborate on the reasons they did not act. This would help researchers develop appropriate strategies to address the basis for their inaction.

6.1.3 Supporting User Data Sharing Preferences

Our poster study shows that presenting information to users can raise awareness of the security and privacy risk associated to the collection of their data. Previous work [57]. found novice users' sharing preferences changed over time, but it is unclear whether their results hold for more experienced users. In another study [3], participants were not asked about specific recipients. Rather, these emerged through the interview process. Our survey study allowed us to quantify sharing preferences for individual recipient groups and for each type of data.

Our survey participants provided detailed information about what they are willing to disclose to the groups of recipients for specific data types. These results support previous research by Lowens et al. [42] that indicates users want granular control of their data, and extends the previous literature by detailing the specific preferences for the types of data depending on the recipient.

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 from a mobile app or website and not directly from the device, making them virtually invisible to users unless they 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 make them 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 period.

6.1.4 Targeting Complex Security and Privacy Behaviours

Privacy attitudes and behaviours are complex, often contradictory, and difficult to explain [27,37]. Our survey study demonstrates the inconsistencies in users' concerns about security privacy threats associated with the use of fitness tracker. Users were not very fearful of threats and believed them unlikely to occur. However, they believe consequences would be severe if breaches were to occur. They also exhibited little confidence that developers were ensuring their safety against threats. Furthermore, our poster study showed an immediate increase and partially sustained concern about security and privacy after viewing the information posters. These contradictions in concerns are troubling because research suggests that privacy concerns affect attitudes, which in turn impact privacy intentions, and finally, influence privacy behaviours [22].

Research on contradictory concerns and behaviours with technology is not definitive. There is support for the argument that high concern about security and privacy prompts an increase in protection behaviours [11, 43], but others have found that while users express concern, they do little to protect their data [1,42]. Kokolakis [37] explains security and privacy concerns are contextual and cautions us not to generalize the results from studies about privacy behaviours because they occur in different contexts and often provide contradictory evidence. If we extend this to privacy with fitness tracker use, we believe that it is important to focus on this specific context rather than generalizing findings from wearables or other types of technology.

While we cannot conclude that the visual design of our posters nor the individual components caused the change in users' reported behaviour, the structure and content of the posters was the same for each. By testing for the baseline behaviours (with no information), after presentation of posters, and after one week, we can say that providing information helped to prompt a change.

We offer the three-part framework that we used to inform users about privacy threats. The Fitness Tracker Privacy Risk Framework (FTPR Framework) shows the factors that contribute to privacy risks: tracker functions that are activated, the type of data required or generated by the tracker, and the data sharing practices. We designed information posters around this framework, using threat scenarios as examples, and provided privacy protection strategies. We encourage those interested in the research and development of educational materials to inform users about security and privacy to use our framework with familiar and relevant messaging. In our study, the scenarios believed to be most plausible and likely to occur were ones users may have encountered through media reports. In addition, customized messaging could be developed for users based on the type of activities they 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.

Some users are concerned about their privacy, but they are willing to give up personal information to have access to technology because of the benefits they receive [27]. Understanding these nuances and working towards educating users on their own terms with relevant, timely information could help minimize inconsistencies between concerns, attitudes, intent, and actual behaviours.

6.2 Contributions

To re-iterate, the main contributions of this thesis are as follows:

- Through our survey study, we extend previous literature by providing new insights on sharing preferences and behaviours of fitness tracker users. Users have distinct sharing preferences for specific types of data and for specific recipients, and they attribute different value to different types of data.

- We also provide fitness tracker-specific evidence of the complexities of privacy preferences and behaviours. Users exhibit contradictory behaviour: they are not very fearful of threats, believe they are unlikely to occur but know that they can cause substantial harm.

- Through our poster study, we demonstrate that it is possible to change fitness trackers' reported privacy behaviours by showing them information posters. We also demonstrate a method to evaluate whether privacy intentions translate to reported privacy behaviours.

6.3 Future Work

Moving forward, we want to further investigate how messaging and visuals can work to educate users about security and privacy, beginning designing a study that better allows us to differentiate the most effective characteristics of our information posters. In developing new informational materials, we would also consider other modes of delivery and data collection, such as through the user's mobile device. This would allow us to capture actual, rather than self-reported behaviours over time. Finally, we are interested in developing engaging, usable and relevant interventions to enhance user awareness. We believe these should be customized based on nuances in attitudes and personal preferences.

6.4 Conclusion

Personal data collected by fitness trackers can leave users open to security and privacy threats, often without their knowledge. We conducted two studies to explore whether enhancing user awareness of security and privacy risks might prompt users to take action to protect their personal information. For the first study, we conducted 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. The second study, conducted with 34 participants, was designed to determine whether the presentation of privacy information had the potential to affect a change in privacy behaviour. Participants completed a pre test questionnaire, viewed one of four prototypes, responded to a post test questionnaire and one week later, completed a follow-up questionnaire.

Users expressed specific preferences for data disclosure; they revealed the distinct types of data they are willing to share and with whom they are willing to share it. Our results show user attitudes can be complex and contradictory and good intentions and behaviours are not always aligned. Finally, we found evidence that presenting security and privacy information to fitness tracker users increased their intention to act and prompted them to take protective actions one week after our study.

Because of the popularity of fitness trackers and the many benefits they provide, it is important to inform users of the potential threats that can result with their use. We believe information design has the potential to make users aware of security and privacy risks and can encourage users to protect their personal data.

Bibliography

[1] Angeliki Aktypi, Jason RC Nurse, and Michael Goldsmith. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the 2017 International Workshop on Multimedia Privacy and Security*, pages 1–11. ACM, 2017.

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 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*, pages 787–796. ACM, 2015.

[3] Abdulmajeed Alqhatani and Heather Richter Lipford. "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)*, 2019.

[4] Annie I Antón, Julia B Earp, and Jessica D Young. How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, 8(1):21–27, 2010.

[5] Kim Baer and Jill Vacarra. *Information design workbook: Graphic approaches, solutions, and inspiration+ 30 case studies.* Rockport Publishers, 2008.

[6] Suzanne Barlyn. Strap on the fitbit: John hancock to sell only interactive life insurance, Sep 2018.

[7] Susanne Barth and Menno DT De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and Informatics*, 34(7):1038–1058, 2017.

[8] Scott Bateman, Regan L Mandryk, Carl Gutwin, Aaron Genest, David McDine, and Christopher Brooks. Useful junk?: the effects of visual embellishment on comprehension and memorability of charts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2573–2582. ACM, 2010.

[9] Jiang Bian, Kenji Yoshigoe, Amanda Hicks, Jiawei Yuan, Zhe He, Mengjun Xie, Yi Guo, Mattia Prosperi, Ramzi Salloum, and Francois Modave. Mining twitter to assess the public perception of the "internet of things". *PloS one*, 11(7):e0158450, 2016.

[10] Igor Bilogrevic and Martin Ortlieb. If you put all the pieces together...: Attitudes towards data combination and sharing across services and companies. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5215–5227. ACM, 2016.

[11] Grant Blank, Gillian Bolsover, and Elizabeth Dubois. A new privacy paradox: Young people and privacy on social network sites. In *Prepared for the Annual Meeting of the American Sociological Association*, volume 17, 2014.

[12] John Bowers. *Introduction to two-dimensional design: Understanding form and function*. John Wiley & Sons, 1999.

[13] John Bowers. *Introduction to graphic design methodologies and processes: understanding theory and application*. John Wiley & Sons, 2012.

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

[15] Hichang Cho, Jae-Shin Lee, and Siyoung Chung. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5):987–995, 2010.

[16] Michelle M Christovich. Why should we care what fitbit shares-a proposed statutory solution to protect sensitive personal fitness information. *Hastings Comm. & Ent. LJ*, 38:91–116, 2016.

[17] Fergus IM Craik and Robert S Lockhart. Levels of processing: A framework for memory research. *Journal of verbal learning and verbal behavior*, 11(6):671–684, 1972.

[18] Lorrie Faith Cranor, Joseph Reagle, and Mark S Ackerman. Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy*, pages 47–70, 2000.

[19] Carl Dair. University of toronto press, toronto, 1967. *Paperback reprint*, 1985.

[20] Sourya Joyee De and Daniel Le Métayer. Privacy risk analysis. *Synthesis Lectures on Information Security, Privacy, & Trust*, 8(3):1–133, 2016.

[21] Anandhi Vivek Dhukaram, Chris Baber, Lamia Elloumi, Bert-Jan van Beijnum, and Paolo De Stefanis. End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust. In *2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*, pages 478–484. IEEE, 2011.

[22] Tobias Dienlin and Sabine Trepte. Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, 45(3):285–297, 2015.

[23] Donis A Dondis. *A primer of visual literacy*. Mit Press, 1974.

[24] Casey Fiesler, Michaelanne Dye, Jessica L Feuston, Chaya Hiruncharoenvate, Clayton J Hutto, Shannon Morrison, Parisa Khanipour Roshan, Umashanthi Pavalanathan, Amy S Bruckman, Munmun De Choudhury, et al. What (or who) is public?: Privacy settings and social media content sharing. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 567–580. ACM, 2017.

[25] Fitbit Health Solutions. Support healthy behavior changes in your employees. *Fitbit website*, nd. `https://healthsolutions.fitbit.com/employers`.

[26] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

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

[28] Ron S Gold and Mark G Brown. Explaining the effect of event valence on unrealistic optimism. *Psychology, health & medicine*, 14(3):262–272, 2009.

[29] Austin Grabish. Porn extortion scam threatens to send webcam video of victims to their contact list — cbc news. *CBC news*, Jul 2018. `https://www.cbc.ca/news/canada/manitoba/porn-scam-manitoba-1.4762638`.

[30] Jason Hanna and Stella Chan. The murder suspect denies it. the victim's fitbit tells another story, police say. *Cable News Network*, 2018. `https://www.cnn.com/2018/10/04/us/california-fitbit-killing/index.html`.

[31] Christine Hauser. Police use fitbit data to charge 90-year-old man in stepdaughter's killing, Oct 2018.

[32] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel. Every step you fake: A comparative analysis of fitness tracker privacy and security. *Open Effect*, pages 1–76, Feb 2016. `https://openeffect.ca/reports/Every_Step_You_Fake.pdf`.

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

[34] Luisa Beck James McAuley. How free movement, a founding principle of the e.u., became less free. *The Washington Post*, Jul 2018. `https://www.washingtonpost.com/world/europe/how-free-movement-a-founding-principle-of-the-eu-became-less-free/2018/07/17/8e140c0c-7f04-11e8-a63f-7b5d2aba7ac5_story.html`.

[35] Carlos Jensen and Colin Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478. ACM, 2004.

[36] Carlos Jensen, Colin Potts, and Christian Jensen. Privacy practices of internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2):203–227, 2005.

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

[38] Hanna Krasnova, Elena Kolesnikova, and Oliver Guenther. " it won't happen to me!": self-disclosure in online social networks. In *Proceedings of the Fifteenth Americas Conference on Information Systems*, pages 1–9. AIS/ICIS, 2009.

[39] Lydia Kraus, Ina Wechsung, and Sebastian Möller. A comparison of privacy and security knowledge and privacy concern as influencing factors for mobile protection behavior. In *Workshop on Privacy Personas and Segmentation*, page 2014, 2014.

[40] Jason Lankow, Josh Ritchie, and Ross Crooks. *Infographics: The power of visual storytelling*. Taylor & Francis, 2012.

[41] Linda Lee, J Lee, Serge Egelman, and David Wagner. Information disclosure concerns in the age of wearable computing. In *Proceedings of the 2016 Workshop on Usable Security*. USEC, 2016.

[42] Byron Lowens, Vivian Genaro Motti, and Kelly Caine. Wearable privacy: Skeletons in the data closet. In *2017 IEEE International Conference on Healthcare Informatics (ICHI)*, pages 295–304. IEEE, 2017.

[43] Christoph Lutz and Pepe Strathoff. Privacy concerns and online behavior–not so paradoxical after all? viewing the privacy paradox through different theoretical lenses. *SSRN: https://ssrn.com/abstract=2425132 or http://dx.doi.org/10.2139/ssrn.2425132 (April 15, 2014)*, 2014.

[44] Kate Lyons. Stalkers using bugging devices and spyware to monitor victims. *The Guardian*, Feb 2018. `https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims`.

[45] Soultana Macridis and Nora Johnston. *2017 Alberta Survey on Physical Activity*. 2017.

[46] Clara Mancini, Keerthi Thomas, Yvonne Rogers, Blaine A Price, Lukazs Jedrzejczyk, Arosha K Bandara, Adam N Joinson, and Bashar Nuseibeh. From

spaces to places: emerging contexts in mobile privacy. In *Proceedings of the 11th international conference on Ubiquitous computing*, pages 1–10. ACM, 2009.

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

[48] Microsoft. Bing ads extreme scale using Azure SQL database. *Microsoft Customers Stories*, Jul 2007. `https://customers.microsoft.com/en-us/story/bing-ads-azure-sql-database-united-states`.

[49] Lorraine Mirabella. Under armour announces significant data breach of its myfitnesspal app, Mar 2018.

[50] Vivian Genaro Motti and Kelly Caine. Users privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*, pages 231–244. Springer, 2015.

[51] Josef Müller-Brockmann. *Grid systems in graphic design: a visual communication manual for graphic designers, typographers and three dimensional designers.* Arthur Niggli, 1996.

[52] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, 41(1):100–126, Summer 2007.

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

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

[55] Greig Paul and James Irvine. Privacy implications of wearable health devices. In *Proceedings of the 7th International Conference on Security of Information and Networks*, page 117. ACM, 2014.

[56] Richard Pérez-Peña and Matthew Rosenberg. Strava fitness app can reveal military sites, analysts say. `https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html`, Jan 2018.

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

[58] Emilee Rader and Janine Slaker. The importance of visibility for folk theories of sensor data. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 257–270. USENIX, 2017.

[59] Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 11–20. ACM, 2011.

[60] Matt Reynolds. Half a billion identities were stolen or exposed online in 2015. *WIRED*, Oct 2017. `https://www.wired.co.uk/article/identity-theft-symantec-security-2015-amount`.

[61] Marshall David Rice and Ekaterina Bogdanov. Privacy in doubt: An empirical investigation of canadians' knowledge of corporate data collection and usage practices. *Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration*, 2018.

[62] Christopher Rowland. With fitness trackers in the workplace, bosses can monitor your every step - and possibly more, Feb 2019.

[63] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214. ACM, 2017.

[64] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. Understanding the impact of information representation on willingness to share information. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 523. ACM, 2019.

[65] Edward Segel and Jeffrey Heer. Narrative visualization: Telling stories with data. *IEEE transactions on visualization and computer graphics*, 16(6):1139–1148, 2010.

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

[67] Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2347–2356. ACM, 2014.

[68] Annette Simmons. *The story factor: Inspiration, influence, and persuasion through the art of storytelling.* Basic books, 2006.

[69] Michael Warren Skirpan, Tom Yeh, and Casey Fiesler. What's at stake: Characterizing risk perceptions of emerging technologies. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 70. ACM, 2018.

[70] David Sless. What is information design. *Designing information for people*, pages 1–16, 1994.

[71] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. Facts and fears: Understanding perceived risk. In *Societal risk assessment*, pages 181–216. Springer, 1980.

[72] Erik Spiekermann. Foreword. In Alison Black, Paul Luna, Ole Lund, and Sue Walker, editors, *Information design: research and practice*, pages ix–x. Taylor & Francis, 2017.

[73] Paul Stiff. Some documents for a history of information design. In Alison Black, Paul Luna, Ole Lund, and Sue Walker, editors, *Information design: research and practice*, pages 147–159. Taylor & Francis, 2017.

[74] Walter R Thompson. Worldwide survey of fitness trends for 2019. *ACSM's Health & Fitness Journal*, 22(6):10–17, 2018.

[75] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5208–5220. ACM, 2017.

[76] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katherine Kritikos. Privacy attitudes and data valuation among fitness tracker users. In *International Conference on Information*, pages 229–239. Springer, 2018.

[77] Gary Wolf. The data-driven life. *The New York Times*, Apr 2010. `https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html`.

[78] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, 13:10–18, 2017.

[79] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. Engaging children about online privacy through storytelling in an interactive comic. In *Proceedings of the 31st British Computer Society Human Computer Interaction Conference*, page 45. BCS Learning & Development Ltd., 2017.

[80] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *2013 APWG eCrime Researchers Summit*, pages 1–11. IEEE, 2013.

[81] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, 2016.

[82] Michael Zimmer, Priya Kumar, Jessica Vitak, Yuting Liao, and Katie Chamberlain Kritikos. "there's nothing really they can do with this information": unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, pages 1–18, 2018.

Appendix A

Survey Study: Questionnaire

Please provide us with information about yourself.

Age: What is **your age?**

Gender: Which option below **describes you?**

○ Female
○ Male
○ Other
○ Prefer not to say

Education: What is **your highest level of education**?

Is this **completed** or **in progress?**

○ Completed ○ In progress

What is/was **your major**?
(Type N/A if this is not applicable to you).

Employment: Which of these describe **your employment status**?
(Check all that apply).

□ Full-time employed
□ Part-time employed
□ Not employed for pay
□ Caregiver (e.g., taking care of children, elderly individuals)
□ Homemaker
□ Full-time student
□ Part-time student
□ Retired
□ Other

What is/was **your occupation**?

(Type N/A if this is not applicable to you).

What is/was **your area of expertise**?

(Type N/A if this is not applicable to you).

Do you **use a fitness tracker, regularly**?

○ Yes
○ No

Which **brand of fitness tracker** are you **using, currently**?

○ Withings
○ Suunto
○ Garmin
○ Fitbit
○ Apple
○ Misfit
○ Huawei
○ Polar
○ Lenovo
○ Nokia
○ Samsung
○ Other

○ Do not use a fitness tracker

Please indicate on the scale, how confident you are that:

	Not at all confident 1	2	3	4	Extremely confident 5
You know what type of data is collected by your fitness tracker.	○	○	○	○	○
You know how your fitness tracker data is being used.	○	○	○	○	○

Please respond to the following questions, in relation to your fitness tracker:

	Yes	No	Don't remember
Have you ever read your fitness trackers's privacy policy?	○	○	○
Have you ever read your fitness trackers's terms and conditions?	○	○	○
Have you changed your fitness tracker's default security and privacy settings for your fitness tracker account?	○	○	○
Have you set the preferences for sharing your fitness tracker data?	○	○	○
Have you taken action/steps to ensure your fitness tracker data is secure and private.	○	○	○

*Aside from the examples above, i***ndicate any other actions/steps you've taken to ensure your fitness tracker data is secure and private:**

(Type N/A if this is not applicable to you).

Please indicate on the scale:

	Not at all interested 1	2	3	4	Extremely interested 5
Your degree of interest in seeking out more information about security and privacy in relation to your fitness tracker.	○	○	○	○	○

Please indicate on the scale, how comfortable you are with:

	Extremely uncomfortable 1	2	3	4	Extremely comfortable 5
Having your fitness data **collected and stored by a fitness tracker.**	○	○	○	○	○
Sharing your fitness tracker data **with a friend.**	○	○	○	○	○
Sharing your fitness tracker data **with work colleagues.**	○	○	○	○	○
Sharing your fitness tracker data **with your employer.**	○	○	○	○	○
Sharing your fitness tracker data **with the general public.**	○	○	○	○	○
Sharing your fitness tracker data **with an insurance company.**	○	○	○	○	○
Sharing your fitness tracker data **with advertisers.**	○	○	○	○	○

Please indicate the personal information on your fitness tracker that you would be comfortable sharing with each of the groups of people. **(Check all that apply).**

	Friends	Work Colleagues	Employers	Insurance Companies	The Public	Advertisers	Comfortable sharing with everyone	Not comfortable sharing with anyone
Pictures	□	□	□	□	□	□	□	□
Birthday	□	□	□	□	□	□	□	□
Gender	□	□	□	□	□	□	□	□
Height	□	□	□	□	□	□	□	□
Location	□	□	□	□	□	□	□	□
My Friends List	□	□	□	□	□	□	□	□

Please indicate the fitness tracker graph data you would be comfortable sharing with each of the groups of people. **(Check all that apply).**

	Friends	Work Colleagues	Employers	Insurance Companies	The Public	Advertisers	Comfortable sharing with everyone	Not comfortable sharing with anyone
Calories Intake and Burn Graph	□	□	□	□	□	□	□	□
Steps, Distance, Floors Graph	□	□	□	□	□	□	□	□
Time Active Graph	□	□	□	□	□	□	□	□
Sleep Graph	□	□	□	□	□	□	□	□
Weight Graph	□	□	□	□	□	□	□	□

Please indicate the fitness tracker statistical data you would be comfortable sharing with each of the groups of people. **Check all that apply).**

	Friends	Work Colleagues	Employers	Insurance Companies	The Public	Advertisers	Comfortable sharing with everyone	Not comfortable sharing with anyone
Milestones	□	□	□	□	□	□	□	□
Lifetime Steps, Distance, and Floors	□	□	□	□	□	□	□	□
Please Select the Last Box	□	□	□	□	□	□	□	□
Average Daily Step Count	□	□	□	□	□	□	□	□

Please indicate on the scale, how fearful you are that:

	Not at all fearful 1	2	3	4	Extremely fearful 5
Your fitness tracker data might be shared without your specific permission.	○	○	○	○	○
Your fitness tracker data will be tampered with or changed in some way.	○	○	○	○	○
Your fitness tracker account will be hijacked by a hacker and you will be locked out.	○	○	○	○	○
Your fitness tracker data will be used against you.	○	○	○	○	○
Please select the middle answer.	○	○	○	○	○
You are subjected to identity theft due to a breach of your fitness tracker account.	○	○	○	○	○

Please indicate on the scale, the likelihood that:

	Not at all likely 1	2	3	4	Extremely likely 5
Your fitness tracker data might be shared without your specific permission.	○	○	○	○	○
Your fitness tracker data will be tampered with or changed in some way.	○	○	○	○	○
Your fitness tracker account will be hijacked by a hacker and you will be locked out.	○	○	○	○	○
Your fitness tracker data will be used against you.	○	○	○	○	○
You are subjected to identity theft due to a breach of your fitness tracker account.	○	○	○	○	○

Please indicate on the scale, the severity of the consequences if:

	Not at all severe 1	2	3	4	Extremely severe 5
Your fitness tracker data was shared without your specific permission.	○	○	○	○	○
Your fitness tracker data was tampered with or changed in some way.	○	○	○	○	○
Your fitness tracker account was hijacked by a hacker and you are locked out.	○	○	○	○	○
Please, choose the fourth option.	○	○	○	○	○
Your fitness tracker data was used against you.	○	○	○	○	○
You are subjected to identity theft due to a breach of your fitness tracker account.	○	○	○	○	○

Please indicate on the scale, how confident you are that fitness tracker developers have ensured that:

	Not at all confident 1	2	3	4	Extremely confident 5
Your fitness tracker data cannot be shared without your specific permission.	○	○	○	○	○
Your fitness tracker data cannot be tampered with or changed in anyway.	○	○	○	○	○
Your fitness tracker account cannot be hijacked by a hacker who's intention it is to lock you out.	○	○	○	○	○
Your fitness tracker data cannot be used against you.	○	○	○	○	○

Given the following scenarios, please indicate if you think they:

- **could possibly occur**
- **would likely occur**

	Is this possible?			**Is this likely?**		
	Yes	No	Don't know	Yes	No	Don't know
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.	○	○	○	○	○	○
Life insurance companies created a "wellness score" from their client's fitness tracker data so they could cancel coverage of unhealthy people.	○	○	○	○	○	○
Assumptions were made about a fitness tracker user's sexual activity, based on the data showing changes in heart rate and intensity of movement.	○	○	○	○	○	○
An employer used fitness tracker data about a woman's health information (ovulation and menstrual cycles) for human resource planning.	○	○	○	○	○	○
A fitness tracker account was taken over by hackers, denying the user access to his own account until he paid a ransom.	○	○	○	○	○	○
Based on running data collected by a fitness tracker, an advertising agency was able to target advertising for brands of running shoes suited to a long distance runner.	○	○	○	○	○	○
Border control officers denied a man entry into the country based on fitness tracker GPS data showing the countries he visited in the past.	○	○	○	○	○	○
A hacker gained access to a user's fitness tracker account and could tell precisely where the user was located, and whether or not they were walking, cycling, swimming, etc.	○	○	○	○	○	○
Fitness tracker data was used in a murder investigation, where a victim's data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time-stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder.	○	○	○	○	○	○
Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user's home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.	○	○	○	○	○	○
Lack of sleep has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Fitness tracker sleep information could be used against someone who has been asked for access to their fitness tracker when applying for a job.	○	○	○	○	○	○
Camels raised in the wild have 2 legs.	○	○	○	○	○	○
Fitness data was intercepted by hackers when the data was transmitting from the fitness tracker device to the server.	○	○	○	○	○	○
Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual's health and fitness information.	○	○	○	○	○	○

Given the following scenarios, please indicate if you think they:

- **could possibly occur**
- **would likely occur**

	Is this possible?			**Is this likely?**		
	Yes	No	Don't know	Yes	No	Don't know
A fitness tracker user was identified simply by their gait (walking pattern) even when fitness tracker data was anonymized.	○	○	○	○	○	○
Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of a user's movements.	○	○	○	○	○	○
Based on the combined fitness tracker data of citizens showing they already maintain a high level of fitness, city council denied a request for a new fitness facility and running track.	○	○	○	○	○	○
An adoption agency prevented a couple from adopting children based on fitness tracker information that suggested they led an inactive lifestyle, did not exercise, and ate poorly.	○	○	○	○	○	○
Fitness tracker users were discriminated against because of their race, religion, and gender based on assumptions made from their tracker data and personal information.	○	○	○	○	○	○
Police officers used fitness tracker data as evidence to arrest someone for a crime.	○	○	○	○	○	○
Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.	○	○	○	○	○	○

Please indicate on the scale, **the likelihood that you will now:**

	Not at all likely 1	2	3	4	Extremely likely 5
Read your fitness tracker's privacy policy.	○	○	○	○	○
Read your fitness tracker's terms and conditions.	○	○	○	○	○
Change your fitness tracker's default security and privacy settings for your account.	○	○	○	○	○
Set the preferences for sharing your fitness tracker data.	○	○	○	○	○
Take action/steps to ensure your fitness tracker data is secure and private.	○	○	○	○	○

Aside from the examples above, indicate any other actions/steps you will now take to ensure your fitness tracker data is secure and private:

(Type N/A if this is not applicable to you).

	Not at all interested 1	2	3	4	Extremely interested 5
Your degree of interest in seeking out more information about security and privacy in relation to your fitness tracker.	○	○	○	○	○

Appendix B

Poster Study: Pre-test Questionnaire

SURVEY INSTRUCTION

Carleton
UNIVERSITY
Canada's Capital University

Educating Fitness Tracker Users – Pre-test

Please type **your ID number:**

Please re-type your **ID number:**

Please provide us with information about yourself.

Age: What is **your age?**

Gender: Which option below **describes you?**

○ Female
○ Male
○ Other
○ Prefer not to say

Education: What is **your highest level of education**?

Is this **completed** or **in progress?**

Completed	In progress
○	○

What is/was **your major**?

(Type N/A if this is not applicable to you).

Employment: Which of these describe **your employment status**?

(Check all that apply).

- □ Full-time employed
- □ Part-time employed
- □ Not employed for pay
- □ Caregiver (e.g., taking care of children, elderly individuals)
- □ Homemaker
- □ Full-time student
- □ Part-time student
- □ Retired
- □ Other

What is/was **your occupation**?

(Type N/A if this is not applicable to you).

What is/was **your area of expertise**?

(Type N/A if this is not applicable to you).

Do you **use a fitness tracker, regularly**?

- ○ Yes
- ○ No

Which **brand of fitness tracker** are you **using, currently**?

- ○ Withings
- ○ Suunto
- ○ Garmin
- ○ Fitbit
- ○ Apple
- ○ Misfit
- ○ Huawei
- ○ Polar
- ○ Lenovo
- ○ Nokia
- ○ Samsung
- ○ Other
- ○ Do not use a fitness tracker

List the **tracking functions** you use/view regularly (for example, counting steps, counting calories, etc.).

Please indicate on the scale, how confident you are that:

	Not at all confident 1	2	3	4	Extremely confident 5
You know what type of data is collected by your fitness tracker.	○	○	○	○	○
You know how your fitness tracker data is being used.	○	○	○	○	○

Please respond to the following questions, in relation to your fitness tracker:

	Yes	No	Don't remember
Have you ever read your fitness trackers's privacy policy?	○	○	○
Have you ever read your fitness trackers's terms and conditions?	○	○	○
Have you changed your fitness tracker's default security and privacy settings for your fitness tracker account?	○	○	○
Have you set the preferences for sharing your fitness tracker data?	○	○	○
Have you taken action/steps to ensure your fitness tracker data is secure and private.	○	○	○

Aside from the examples above, indicate any other actions/steps you've taken to ensure your fitness tracker data is secure and private:

(Type N/A if you have not taken other actions/steps).

Please indicate on the scale:

	Not at all concerned 1	2	3	4	Extremely concerned 5
Your degree of concern about the security and privacy of your fitness tracker data	○	○	○	○	○

Given the following scenarios, please indicate on the scale, the degree to which you think they:

- **could possibly occur**
- **would likely occur**

A hacker gained access to a user’s fitness tracker account and could tell precisely where the user was located, and whether or not they were walking, cycling, swimming, etc.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data was used in a murder investigation, where a victim's data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time-stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user's home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Lack of sleep has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Fitness tracker sleep information could be used against someone who has been asked for access to their fitness tracker when applying for a job.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 5 for both "Is this possible?" and "Is this likely?"

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness data was intercepted by hackers when the data was transmitting from the fitness tracker device to the server.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual's health and fitness information.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Given the following scenarios, please indicate on the scale, the degree to which you think they:

• could possibly occur

• would likely occur

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.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Life insurance companies created a “wellness score” from their client’s fitness tracker data so they could cancel coverage of unhealthy people.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for "Is this possible?" and number 1 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Assumptions were made about a fitness tracker user’s sexual activity, based on the data showing changes in heart rate and intensity of movement.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An employer used fitness tracker data about a woman’s health information (ovulation and menstrual cycles) for human resource planning.;

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker account was taken over by hackers, denying the user access to his own account until he paid a ransom.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on running data collected by a fitness tracker, an advertising agency was able to target advertising for brands of running shoes suited to a long distance runner.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Border control officers denied a man entry into the country based on fitness tracker GPS data showing the countries he visited in the past.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker user was identified simply by their gait (walking pattern) even when fitness tracker data was anonymized.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of a user’s movements.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on the combined fitness tracker data of citizens showing they already maintain a high level of fitness, city council denied a request for a new fitness facility and running track.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An adoption agency prevented a couple from adopting children based on fitness tracker information that suggested they led an inactive lifestyle, did not exercise, and ate poorly.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Police officers used fitness tracker data as evidence to arrest someone for a crime.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for "Is this possible?" and number 3 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker users were discriminated against because of their race, religion, and gender based on assumptions made from their tracker data and personal information.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Appendix C

Poster Study: Visual Conditions Post-test Questionnaire

SURVEY INSTRUCTION

Carleton
UNIVERSITY
Canada's Capital University

Educating fitness tracker users – Post Test

VIZ

Please type **your ID number:**

Please re-type your **ID number:**

Please indicate on the scale, how confident you are now that:

	Not at all confident 1	2	3	4	Extremely confident 5
You know what type of data is collected by your fitness tracker.	○	○	○	○	○
You know how your fitness tracker data is being used.	○	○	○	○	○

Indicate if the following statements are "True" or "False":

	True	False
To some extent, users can specify with whom they can share their fitness tracker data.	○	○
Fitness tracker manufacturers do not share user data.	○	○
Fitness tracker data can reveal a user's location.	○	○

Indicate if the following statements are "True" or "False":

Fitness tracker **data can be:**

	True	False
• shared without your knowledge	○	○
• used for purposes you are not aware of	○	○
• misinterpreted or taken out of context	○	○
• relied on to track activities with 100% accuracy	○	○
• accessed by hackers	○	○
• requested by legal authorities	○	○

Indicate if the following statements are “True” or “False”:

If your fitness tracker **data is compromised**, it **may result in:**

	True	False
• financial/property loss	○	○
• identity theft	○	○
• improved health	○	○
• surveillance	○	○
• profiling	○	○
• stalking	○	○
• extortion	○	○

For the following, indicate the degree to which you agree or disagree with the statements:

	Strongly Disagree 1	2	3	4	Strongly Agree 5
In reading the posters, I gained useful knowledge about privacy in relation to my fitness tracker.	○	○	○	○	○
The posters made the information pleasurable to read.	○	○	○	○	○
The posters were difficult to understand.	○	○	○	○	○
The posters improved my understanding of data collection associated with the use of fitness trackers.	○	○	○	○	○
The visuals used to portray the topic made it difficult to understand.	○	○	○	○	○
I think I would prefer to learn the information from a plain text-based poster.	○	○	○	○	○
I will most likely remember what I have learned, weeks later.	○	○	○	○	○
The posters have convinced me to change my privacy settings on my fitness account.	○	○	○	○	○
The posters have convinced me to be more mindful of the functions I choose to activate on my tracker.	○	○	○	○	○
The posters taught me something new regarding what could possibly happen to me with the use of my fitness tracker.	○	○	○	○	○
I would spend time reading these posters if I came across them elsewhere.	○	○	○	○	○
I would recommend these posters to other fitness tracker users.	○	○	○	○	○
I would share the information I learned with others.	○	○	○	○	○

Please give your feedback regarding the information provided on the posters (i.e. Was the information useful? Is there other additional information you would like to see?)

Please give your feedback regarding the visual aspects of the posters you viewed (i.e. Were they appealing? Were they appropriate for the topic? Did they help to enhance your understanding of the topic?)

How would you interact with the posters in a public setting, such as on a wall in a hallway or perhaps at a bus or train station? (i.e. Would you read them? How long might you spend time reading them?)

Given the following scenarios, please indicate on the scale, the degree to which you think they:

- **could possibly occur**
- **would likely occur**

A fitness tracker user was identified simply by their gait (walking pattern) even when fitness tracker data was anonymized.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of a user’s movements.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on the combined fitness tracker data of citizens showing they already maintain a high level of fitness, city council denied a request for a new fitness facility and running track.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 5 for "Is this possible?" and number 1 for "Is this likely."

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An adoption agency prevented a couple from adopting children based on fitness tracker information that suggested they led an inactive lifestyle, did not exercise, and ate poorly.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Police officers used fitness tracker data as evidence to arrest someone for a crime.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker users were discriminated against because of their race, religion, and gender based on assumptions made from their tracker data and personal information.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

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.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Life insurance companies created a “wellness score” from their client’s fitness tracker data so they could cancel coverage of unhealthy people.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 3 for "Is this possible?" and number 3 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Assumptions were made about a fitness tracker user’s sexual activity, based on the data showing changes in heart rate and intensity of movement.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An employer used fitness tracker data about a woman's health information (ovulation and menstrual cycles) for human resource planning.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker account was taken over by hackers, denying the user access to his own account until he paid a ransom.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on running data collected by a fitness tracker, an advertising agency was able to target advertising for brands of running shoes suited to a long distance runner.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Border control officers denied a man entry into the country based on fitness tracker GPS data showing the countries he visited in the past.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A hacker gained access to a user's fitness tracker account and could tell precisely where the user was located, and whether or not they were walking, cycling, swimming, etc.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data was used in a murder investigation, where a victim's data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time-stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user’s home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Lack of sleep has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Fitness tracker sleep information could be used against someone who has been asked for access to their fitness tracker when applying for a job.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for both "Is this possible?" and "Is this likely?"

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness data was intercepted by hackers when the data was transmitting from the fitness tracker device to the server.

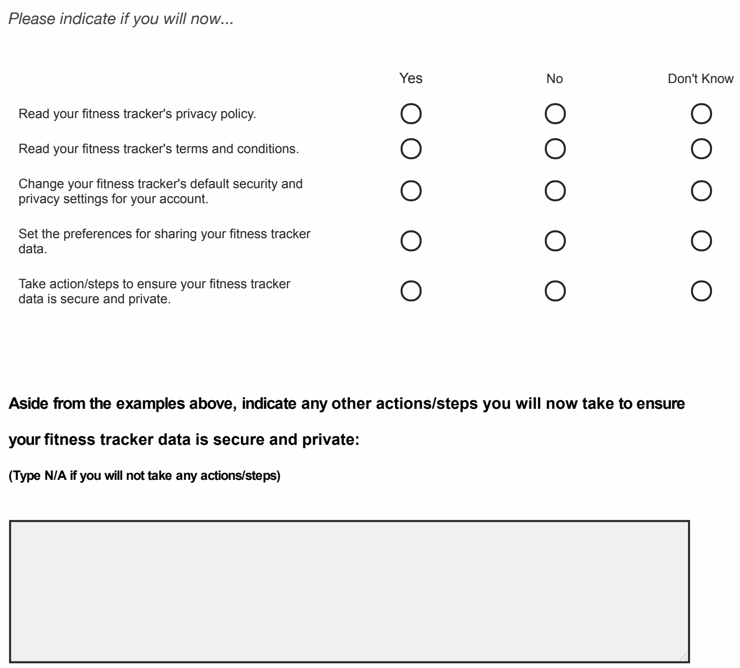
	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual’s health and fitness information.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Please indicate on the scale:

	Not at all concerned 1	2	3	4	Extremely concerned 5
Your degree of concern about the security and privacy of your fitness tracker data	○	○	○	○	○



Please indicate if you will now...

	Yes	No	Don't Know
Read your fitness tracker's privacy policy.	○	○	○
Read your fitness tracker's terms and conditions.	○	○	○
Change your fitness tracker's default security and privacy settings for your account.	○	○	○
Set the preferences for sharing your fitness tracker data.	○	○	○
Take action/steps to ensure your fitness tracker data is secure and private.	○	○	○

Aside from the examples above, indicate any other actions/steps you will now take to ensure your fitness tracker data is secure and private:

(Type N/A if you will not take any actions/steps)

Appendix D

Poster Study: Text Conditions Post-test Questionnaire

SURVEY INSTRUCTION

Carleton
UNIVERSITY
Canada's Capital University

Educating fitness tracker users – Post Test

TXT

Please type **your ID number:**

Please re-type your **ID number:**

Please indicate on the scale, how confident you are now that:

	Not at all confident 1	2	3	4	Extremely confident 5
You know what type of data is collected by your fitness tracker.	○	○	○	○	○
You know how your fitness tracker data is being used.	○	○	○	○	○

Indicate if the following statements are "True" or "False":

	True	False
To some extent, users can specify with whom they can share their fitness tracker data.	○	○
Fitness tracker manufacturers do not share user data.	○	○
Fitness tracker data can reveal a user's location.	○	○

Indicate if the following statements are "True" or "False":

Fitness tracker **data can be:**

	True	False
• shared without your knowledge	○	○
• used for purposes you are not aware of	○	○
• misinterpreted or taken out of context	○	○
• relied on to track activities with 100% accuracy	○	○
• accessed by hackers	○	○
• requested by legal authorities	○	○

Indicate if the following statements are “True” or “False”:

If your fitness tracker **data is compromised**, it **may result in:**

	True	False
• financial/property loss	○	○
• identity theft	○	○
• improved health	○	○
• surveillance	○	○
• profiling	○	○
• stalking	○	○
• extortion	○	○

For the following, indicate the degree to which you agree or disagree with the statements:

	Strongly Disagree 1	2	3	4	Strongly Agree 5
In reading the posters, I gained useful knowledge about privacy in relation to my fitness tracker.	○	○	○	○	○
The posters made the information pleasurable to read.	○	○	○	○	○
The posters were difficult to understand.	○	○	○	○	○
The posters improved my understanding of data collection associated with the use of fitness trackers.	○	○	○	○	○
The lack of visuals used to portray the topic made it difficult to understand.	○	○	○	○	○
I think I would prefer to learn the information from a poster with visuals.	○	○	○	○	○
I will most likely remember what I have learned, weeks later.	○	○	○	○	○
The posters have convinced me to change my privacy settings on my fitness account.	○	○	○	○	○
The posters have convinced me to be more mindful of the functions I choose to activate on my tracker.	○	○	○	○	○
The posters taught me something new regarding what could possibly happen to me with the use of my fitness tracker.	○	○	○	○	○
I would spend time reading these posters if I came across them elsewhere.	○	○	○	○	○
I would recommend these posters to other fitness tracker users.	○	○	○	○	○
I would share the information I learned with others.	○	○	○	○	○

Please give your feedback regarding the information provided on the posters (i.e. Was the information useful? Is there other additional information you would like to see?)

Please give your feedback regarding the visual aspects of the posters you viewed (i.e. Were they appealing? Were they appropriate for the topic? Did they help to enhance your understanding of the topic?)

How would you interact with the posters in a public setting, such as on a wall in a hallway or perhaps at a bus or train station? (i.e. Would you read them? How long might you spend time reading them?)

Given the following scenarios, please indicate on the scale, the degree to which you think they:

- **could possibly occur**
- **would likely occur**

A fitness tracker user was identified simply by their gait (walking pattern) even when fitness tracker data was anonymized.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of a user's movements.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on the combined fitness tracker data of citizens showing they already maintain a high level of fitness, city council denied a request for a new fitness facility and running track.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 5 for "Is this possible?" and number 1 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An adoption agency prevented a couple from adopting children based on fitness tracker information that suggested they led an inactive lifestyle, did not exercise, and ate poorly.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Police officers used fitness tracker data as evidence to arrest someone for a crime.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker users were discriminated against because of their race, religion, and gender based on assumptions made from their tracker data and personal information.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

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.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Life insurance companies created a “wellness score” from their client’s fitness tracker data so they could cancel coverage of unhealthy people.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 3 for "Is this possible?" and number 3 for "Is this likely."

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Assumptions were made about a fitness tracker user’s sexual activity, based on the data showing changes in heart rate and intensity of movement.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An employer used fitness tracker data about a woman’s health information (ovulation and menstrual cycles) for human resource planning.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker account was taken over by hackers, denying the user access to his own account until he paid a ransom.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on running data collected by a fitness tracker, an advertising agency was able to target advertising for brands of running shoes suited to a long distance runner.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Border control officers denied a man entry into the country based on fitness tracker GPS data showing the countries he visited in the past.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A hacker gained access to a user’s fitness tracker account and could tell precisely where the user was located, and whether or not they were walking, cycling, swimming, etc.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data was used in a murder investigation, where a victim’s data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time-stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user’s home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Lack of sleep has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Fitness tracker sleep information could be used against someone who has been asked for access to their fitness tracker when applying for a job.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for both "Is this possible?" and "Is this likely?"

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness data was intercepted by hackers when the data was transmitting from the fitness tracker device to the server.

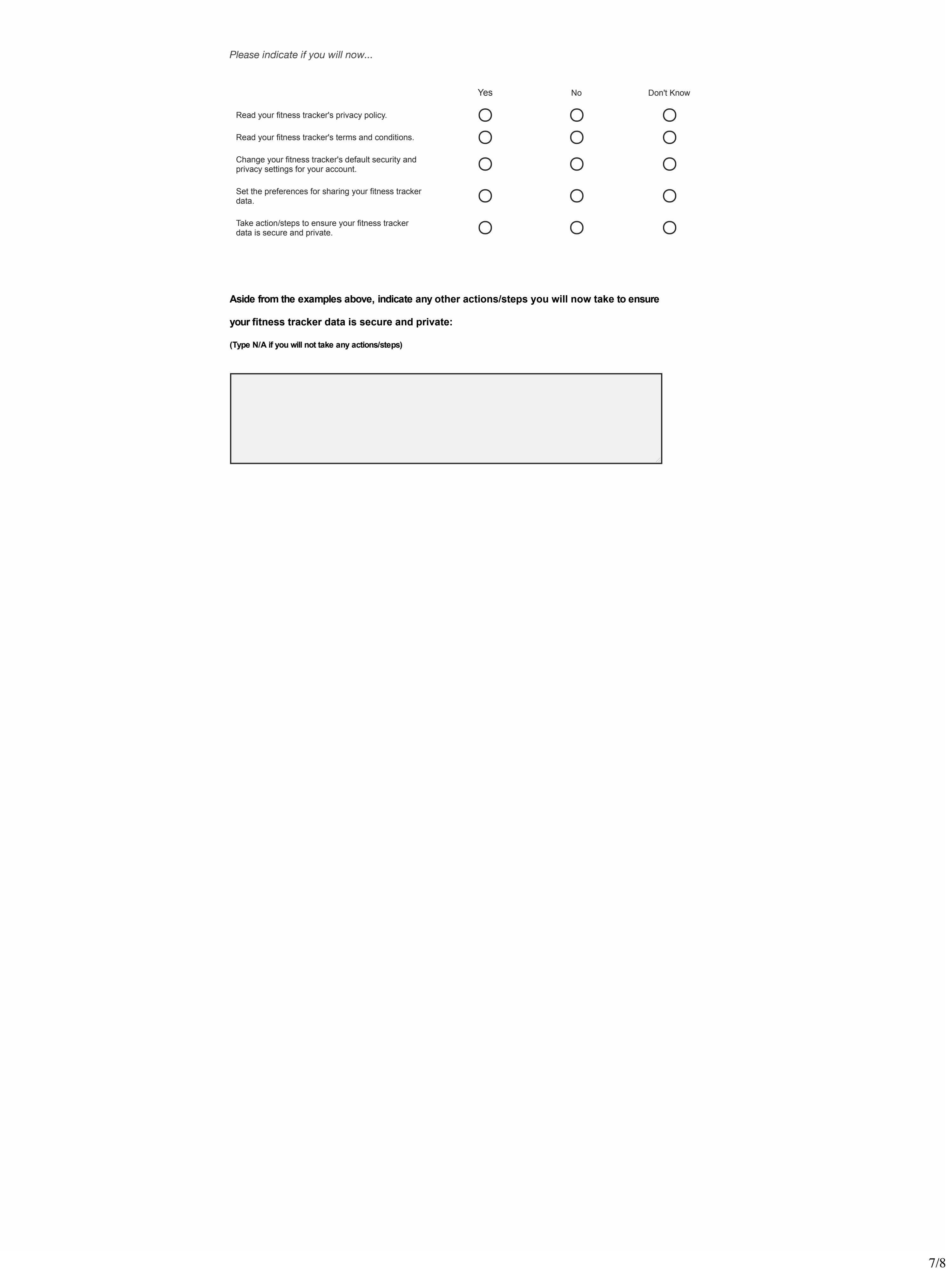
	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual’s health and fitness information.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Please indicate on the scale:

	Not at all concerned				Extremely concerned
	1	2	3	4	5
Your degree of concern about the security and privacy of your fitness tracker data	○	○	○	○	○



Please indicate if you will now...

	Yes	No	Don't Know
Read your fitness tracker's privacy policy.	○	○	○
Read your fitness tracker's terms and conditions.	○	○	○
Change your fitness tracker's default security and privacy settings for your account.	○	○	○
Set the preferences for sharing your fitness tracker data.	○	○	○
Take action/steps to ensure your fitness tracker data is secure and private.	○	○	○

Aside from the examples above, indicate any other actions/steps you will now take to ensure your fitness tracker data is secure and private:

(Type N/A if you will not take any actions/steps)

Appendix E

Poster Study: One-week Follow-up Questionnaire

SURVEY INSTRUCTION

Carleton
UNIVERSITY
Canada's Capital University

Fitness tracker users – Follow up

Please note that this survey will be best displayed on a laptop or desktop computer. Some features may be less compatible for use on a mobile device.

Informed Consent

Consent Form

Title:
Educating fitness tracker users about data practices

Ethics Clearance Number:
CUREB-B Clearance # 110890

Date of ethics clearance:
May 10, 2019

Ethics Clearance for the Collection of Data Expires:
May 30, 2020

Researcher:
Sandra Gabriele
School of Computer Science, Human-Computer Interaction
Carleton University, Ottawa, Canada
sandra.gabriele3@carleton.ca

Supervisor:
Dr. Sonia Chiasson
School of Computer Science
Carleton University, Ottawa, Canada
chiasson@scs.carleton.ca

This study is concerned with evaluating posters designed to help users become more aware of the vulnerabilities associated with the use of fitness trackers. To be eligible for this study you:
- are over 18 years of age;
- currently use a fitness tracker; and
- are comfortable interacting with prototypes and answering a survey in English.

Last week, you participated in a session with a pre-test questionnaire, a learning component, interacting with posters, a brief interview, and a post-test questionnaire;

Today, we will ask you to:
Complete an online follow-up questionnaire where you will provide your comments on the prototypes and your understanding and perceptions of privacy and security associated with your fitness data. This will take approximately 5-10 minutes. This questionnaire can be completed anywhere.

The risks associated with your participation in this study are no greater than the risks you take in your daily activities at work or at school. While this risk is expected to be minimal, we will take precautions to protect your identity. Your responses will be anonymized but might be disclosed in case of data breach or court order. Qualtrics servers are located in Toronto, Canada.

You will be paid $ 20.00 CAD for your participation if you complete the follow-up questionnaire. We will send you payment by bank transfer. If you withdraw from the study or do not complete the study, you will not be compensated.

During the follow-up questionnaire, you can simply close the browser window at any time to withdraw from the study and your follow-up questionnaire data will be destroyed. If you also want the data from the initial session destroyed, please contact the researcher, who will delete all your data. **Once you press "submit" at the end of the follow-up questionnaire, you can no longer withdraw your data.**

Once the study is complete, the questionnaire data will be downloaded and deleted from the Qualtrics server and platform identifiers will be removed. If you consent, the session will be audio-recorded for transcription to make it easier for the researcher to capture your feedback. Audio data will not be used for any other purposes. Trint, an online software will be used to transcribe data. Trint has servers in the United States, therefore, data is subject to US laws on data privacy.

Digital recordings and paper notes will be destroyed, once they have been transcribed. The anonymized data will then be stored on the researcher's password-protected computer and kept for possible comparison with later related studies. The data will be stored on the researchers' password protected computer and would only be shared with members of the research team. The data will never be made public. Personal identifiers (the link between email addresses and user IDs) will be deleted as soon as the study is complete. Data will be destroyed/deleted in 5 years .

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. Should you have any ethical concerns with the study, please contact Dr. Bernadette Campbell, Chair, Carleton University Research Ethics Board (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

Statement of Consent

Please indicate whether or not you agree to participate in the study.

○ I agree with the above and wish to participate
○ I do not wish to participate

Please type **your ID number:**

Please re-type **your ID number:**

Please indicate on the scale, how confident you are now that:

	Not at all confident 1	2	3	4	Extremely confident 5
You know what type of data is collected by your fitness tracker.	○	○	○	○	○
You know how your fitness tracker data is being used.	○	○	○	○	○

Please indicate if (in the last week) you have...

	Yes	No	Don't Know
Read your fitness tracker's privacy policy.	○	○	○
Read your fitness tracker's terms and conditions.	○	○	○
Changed your fitness tracker's default security and privacy settings for your account.	○	○	○
Set the preferences for sharing your fitness tracker data.	○	○	○
Taken action/steps to ensure your fitness tracker data is secure and private.	○	○	○

Aside from the examples above, indicate any other actions/steps you have taken to ensure your fitness tracker data is secure and private:
(Type N/A if you have not taken other actions/steps).

Indicate if the following statements are “True” or “False”**:**

	True	False
To some extent, users can specify with whom they can share their fitness tracker data.	○	○
Fitness tracker manufacturers do not share user data.	○	○
Fitness tracker data can reveal a user’s location.	○	○

Indicate if the following statements are “True” or “False”:

Fitness tracker **data can be:**

	True	False
• shared without your knowledge	○	○
• used for purposes you are not aware of	○	○
• misinterpreted or taken out of context	○	○
• relied on to track activities with 100% accuracy	○	○
• accessed by hackers	○	○
• requested by legal authorities	○	○

2_Knowledge3

Indicate if the following statements are “True” or “False”:

If your fitness tracker **data is compromised,** it **may result in**:

	True	False
• financial/property loss	○	○
• identity theft	○	○
• improved health	○	○
• surveillance	○	○
• profiling	○	○
• stalking	○	○
• extortion	○	○

2_Knowledge Multiple Choice

Please give your **feedback** regarding the information provided at the in-person session (i.e. **Was the information useful?** Is there other **additional information** you would like to see?)

Given the following scenarios, please indicate on the scale, the degree to which you think they:

- **could possibly occur**
- **would likely occur**

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.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Life insurance companies created a “wellness score” from their client’s fitness tracker data so they could cancel coverage of unhealthy people.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for "Is this possible?" and number 3 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Assumptions were made about a fitness tracker user’s sexual activity, based on the data showing changes in heart rate and intensity of movement.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An employer used fitness tracker data about a woman’s health information (ovulation and menstrual cycles) for human resource planning.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker account was taken over by hackers, denying the user access to his own account until he paid a ransom.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on running data collected by a fitness tracker, an advertising agency was able to target advertising for brands of running shoes suited to a long distance runner.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Border control officers denied a man entry into the country based on fitness tracker GPS data showing the countries he visited in the past.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A hacker gained access to a user's fitness tracker account and could tell precisely where the user was located, and whether or not they were walking, cycling, swimming, etc.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data was used in a murder investigation, where a victim's data showed the precise time and changes in her heart rate (a spike and then a sudden stop in heart rate). This information was linked to time-stamped video footage of a car parked in the driveway. The owner of the car was named a suspect in the murder.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker data (stairs climbed, location, sleep information, etc.) provided a burglar with information about a fitness tracker user's home and habits. He could see the precise location and the number of floors in the house and when the user was likely to be home.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Lack of sleep has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Fitness tracker sleep information could be used against someone who has been asked for access to their fitness tracker when applying for a job.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 5 for both "Is this possible?" and "Is this likely?"

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness data was intercepted by hackers when the data was transmitting from the fitness tracker device to the server.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Insurance companies collected data from fitness trackers and used this information to offer discounts based on an individual's health and fitness information.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

A fitness tracker user was identified simply by their gait (walking pattern) even when fitness tracker data was anonymized.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker GPS and exercise data showing running routes were tracked and mapped, providing an accurate picture of a user's movements.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Based on the combined fitness tracker data of citizens showing they already maintain a high level of fitness, city council denied a request for a new fitness facility and running track.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

An adoption agency prevented a couple from adopting children based on fitness tracker information that suggested they led an inactive lifestyle, did not exercise, and ate poorly.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Police officers used fitness tracker data as evidence to arrest someone for a crime.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Data collected by a fitness tracker left people open to identity theft, profiling, stalking and extortion.

	Not at all				Extremely
	1	2	3	4	5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Select number 1 for "Is this possible?" and number 3 for "Is this likely."

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Fitness tracker users were discriminated against because of their race, religion, and gender based on assumptions made from their tracker data and personal information.

	Not at all 1	2	3	4	Extremely 5
Is this possible?	○	○	○	○	○
Is this likely?	○	○	○	○	○

Please indicate on the scale:

	Not at all concerned 1	2	3	4	Extremely concerned 5
Your degree of concern about the security and privacy of your fitness tracker data	○	○	○	○	○

Appendix F

Poster Study: Narrative Posters

How did this happen?

data files

Investigating the privacy risks with fitness tracker use

Privacy Risks

Your fitness tracker data can be...
- shared without your knowledge
- used for purposes you are not aware of
- misinterpreted or taken out of context
- accessed by hackers
- requested by legal authorities.

If your fitness tracker data is compromised, it may result in...
- financial/property loss
- identity theft
- surveillance
- profiling
- stalking
- extortion.

Using a fitness tracker can leave you open to privacy risks. We present *data files,* a set of posters that demonstrate possible risks.

For each case you're shown "the evidence" describing the circumstances that contribute to the risk (the tracker functions, the type of data used, the data sharing practices) and privacy implications. Next, *data files* suggests actions to minimize risks.

Tracker Functions:

Every fitness tracker has core functions and functions selected by the user.

Type of Data:

The fitness tracker uses and collects data that is: input by the user*; gathered by sensors; or is generated by the operating system. This data can be combined with data from other sources, posing further risks.

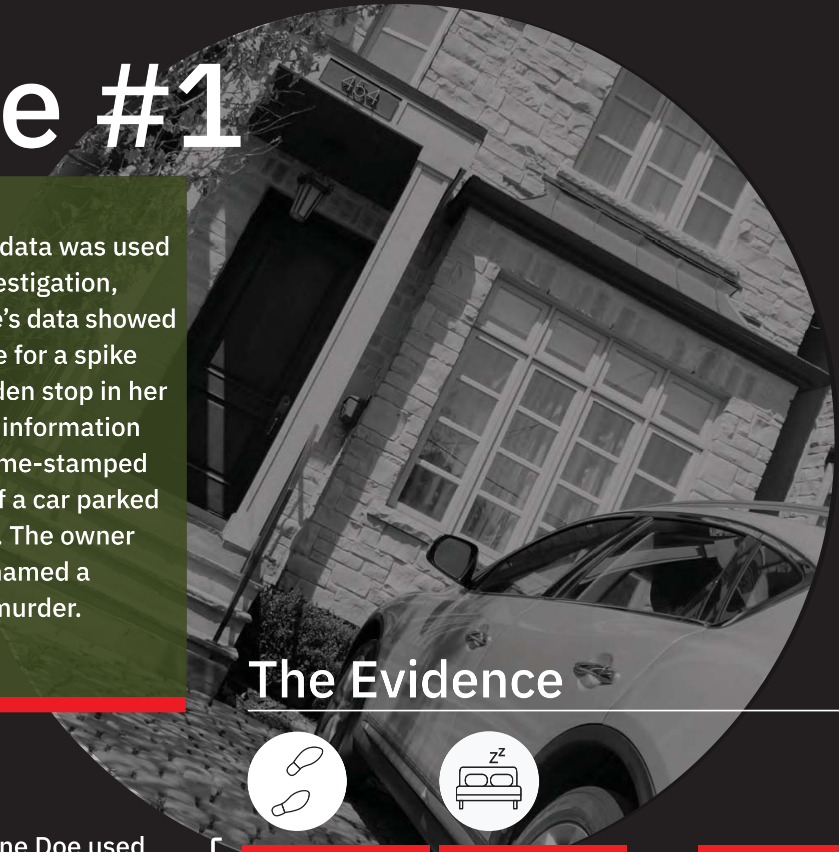
Sharing Practices:

Users can specify with whom they share their data, but others can have access too. 1) Fitness tracker companies share your data with "partners", 2) legal authorities can request access to your data, and 3) your data can be hacked.

* The tracker requires user provided personal data to function (name, email, password, gender, birthday, height, weight, time zone). Users may also provide other details (profile photo, biography, country information, and community username).

Investigating privacy risks with fitness tracker use

Case #1



The Scenario

Fitness tracker data was used in a murder investigation, where Jane Doe's data showed the precise time for a spike and then a sudden stop in her heart rate. This information was linked to time-stamped video footage of a car parked in her driveway. The owner of the car was named a suspect in her murder.

The Evidence

Jane Doe used her tracker for:	**Steps**	**Sleep**		**Other Data**
Jane Doe's tracker collected:	**User Provided Data** Stride length (walking) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	+	Video surveillance footage

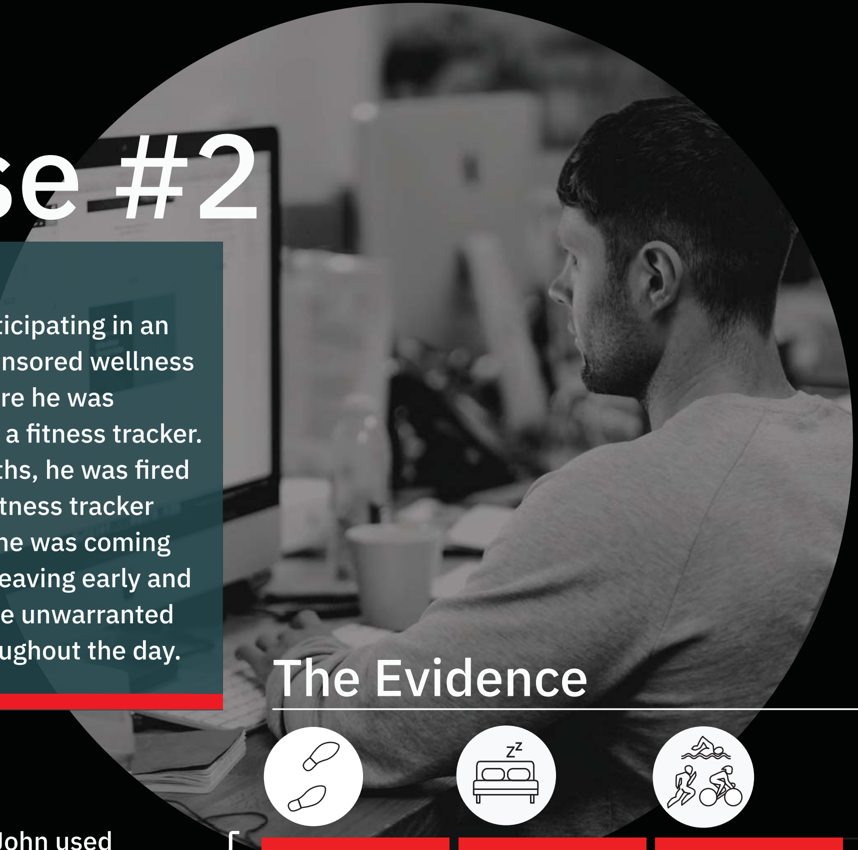
Jane Doe's data was shared with: The Police

Privacy Implications

By court order, legal authorities can gain access to your fitness tracker. While this may be useful for solving crimes, this type of access could be misused. For example, data may be taken out of context or misinterpreted. Data collected by these devices is not 100% reliable and could pose a risk if the data is misused.

Investigating privacy risks with fitness tracker use

datafiles



Case #2

The Threat

John was participating in an employer-sponsored wellness program, where he was provided with a fitness tracker. After six months, he was fired because his fitness tracker data showed he was coming to work late, leaving early and taking multiple unwarranted "breaks" throughout the day.

The Evidence

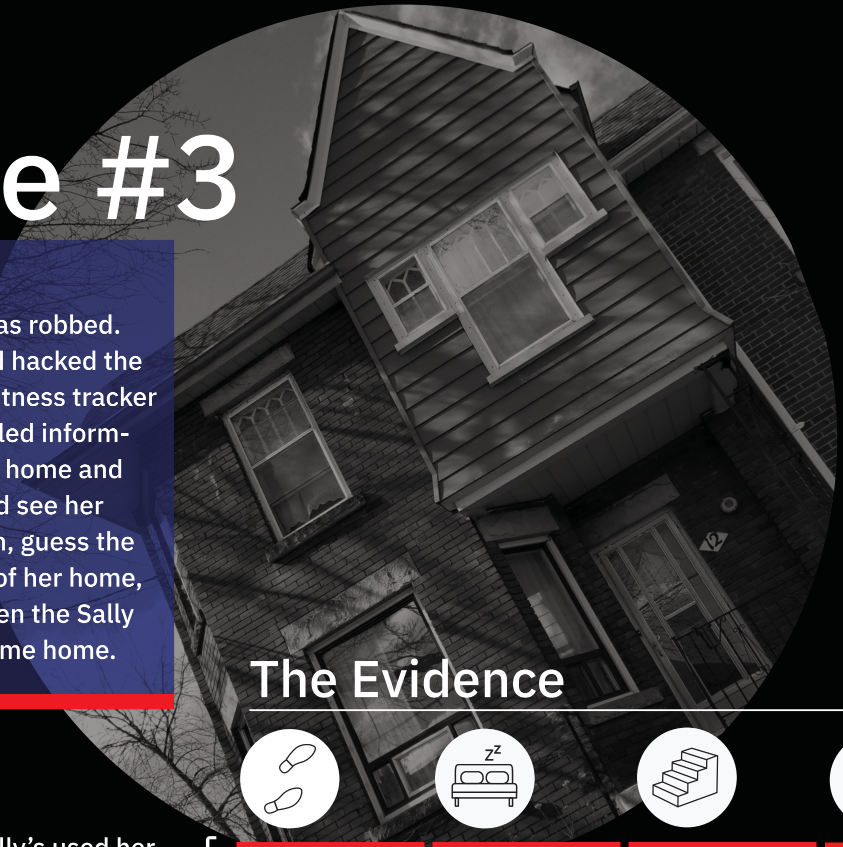
John used his tracker for:	Steps	Sleep	Workouts
John's tracker collected:	**User Provided Data** Stride length (walking) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	**User Provided Data** Stride length (running) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate Pace Distance Location (GPS) **System Data** Time Date
John's data was shared with:	His Employer		

Privacy Implications

While useful in helping you to improve your fitness and health, an employer-sponsored health monitoring program may leave you open to situations where your personal data can be used against you. If you allow an employer access to your fitness tracker data, you may be giving permission to monitor you continuously. Data revealing your location, heart rate, movements, etc. provides an indication of your activities and your health.

Investigating privacy risks with fitness tracker use

datafiles



Case #3

The Scenario

Sally’s home was robbed. The burglar had hacked the homeowner’s fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the Sally was likely to come home.

The Evidence

Sally’s used her tracker for:	**Steps**	**Sleep**	**Floors**	**Routes**
Sally’s tracker collected:	**User Provided Data** Stride length (walking) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Elevation gains **System Data** Time Date	**Data Collected by Sensors** Location (GPS) **System Data** Time Date

Sally's data was shared with: A Hacker

Privacy Implications

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user’s habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Investigating privacy risks with fitness tracker use

Protecting Yourself

Your fitness tracker is a networked computing device. By using it, you are vulnerable to many of the same security and privacy risks as you are with any other computer you use. Practice basic safety hygiene by making sure your device is secure and private.

Actions you can take to minimize risks:

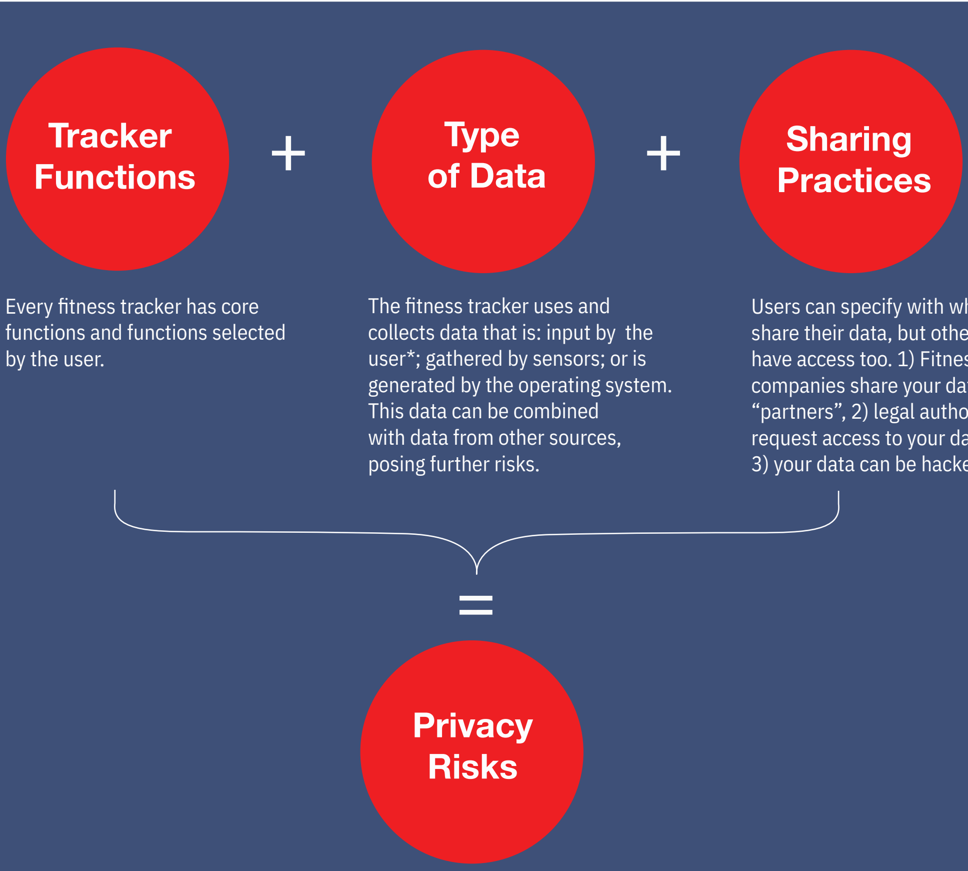
- Weigh the pros and risks of using a fitness tracker before committing to using it
- Decide your own comfort level with collecting and sharing your data
- Understand your fitness tracker's privacy policies and terms and conditions.
- Find out what data is being collected and its implications
- Customize the fitness tracker's default security and privacy settings for your fitness tracker account.
- Set the preferences for sharing your fitness tracker data.
- Check your account settings to ensure no devices other than your own are linked to your account.
- Create a secure, unique password and change it periodically.
- Keep your device firmware and app updated to ensure you receive the latest security updates.
- Turn off the features you don’t use.
- Report any relevant suspicious emails or suspicious activity to the tracker company.

Appendix G

Poster Study: Explorative Posters

Privacy risks with fitness tracker use

Using a fitness tracker can leave you open to privacy risks. We present a set of posters that demonstrate possible risks. For each case, you're shown the circumstances that contribute to the risk (the tracker functions, the type of data used, the data sharing practices) and the privacy implications. Next, we suggest actions to minimize risks.



Every fitness tracker has core functions and functions selected by the user.

The fitness tracker uses and collects data that is: input by the user*; gathered by sensors; or is generated by the operating system. This data can be combined with data from other sources, posing further risks.

Users can specify with whom they share their data, but others can have access too. 1) Fitness tracker companies share your data with "partners", 2) legal authorities can request access to your data, and 3) your data can be hacked.

Your fitness tracker data can be...

- shared without your knowledge
- used for purposes you are not aware of
- misinterpreted or taken out of context
- accessed by hackers
- requested by legal authorities.

If your fitness tracker data is compromised, it may result in...

- financial/property loss
- identity theft
- surveillance
- profiling
- stalking
- extortion.

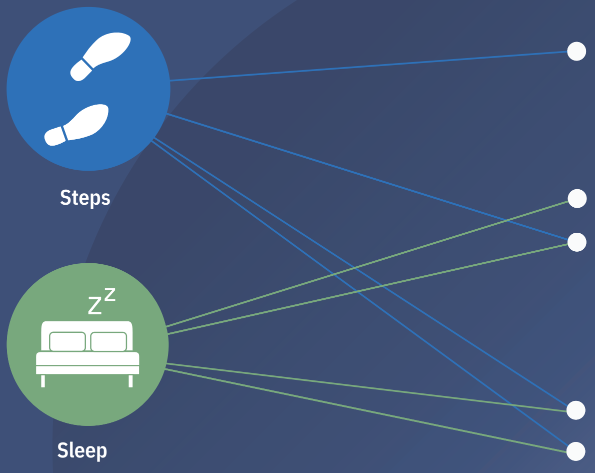
* The tracker requires user provided personal data to function (name, email, password, gender, birthday, height, weight, time zone). Users may also provide other details (profile photo, biography, country information, and community username).

Privacy risks with fitness tracker use

The Scenario

Fitness tracker data was used in a murder investigation, where a victim's data showed the precise time for a spike and then a sudden stop in her heart rate. This information was linked to time-stamped video footage of a car parked in her driveway. The owner of the car was named a suspect in the murder.

Tracker Function



Type of Data

User Provided Data

stride length (walking)

Data Collected by Sensors

heart rate

movement (frequency, duration, intensity & pattern)

System Data

time

date

+

Data From Other Sources

video surveillance footage

Sharing Practices

shared with police

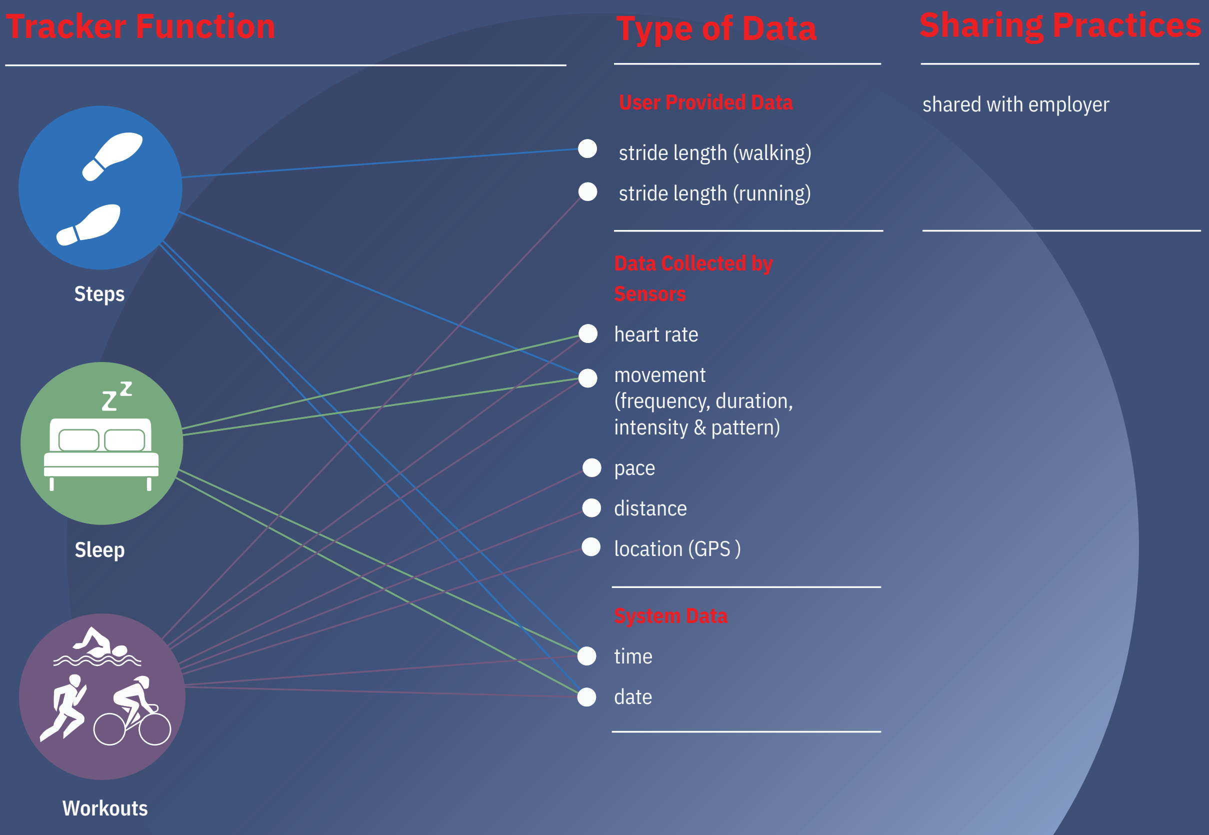
Privacy Implications

By court order, legal authorities can gain access to your fitness tracker. While this may be useful for solving crimes, this type of access could be misused. For example, data may be taken out of context or misinterpreted. Data collected by these devices is not 100% reliable and could pose a risk if the data is misused.

Privacy risks with fitness tracker use

The Scenario

A man participated in an employer-sponsored wellness program. He was given a fitness tracker monitored by his employer. After six months, he was fired because his fitness tracker data showed he came to work late, left early, and took too many “breaks” throughout the day.



Tracker Function

Steps

Sleep

Workouts

Type of Data

User Provided Data

- stride length (walking)
- stride length (running)

Data Collected by Sensors

- heart rate
- movement (frequency, duration, intensity & pattern)
- pace
- distance
- location (GPS)

System Data

- time
- date

Sharing Practices

shared with employer

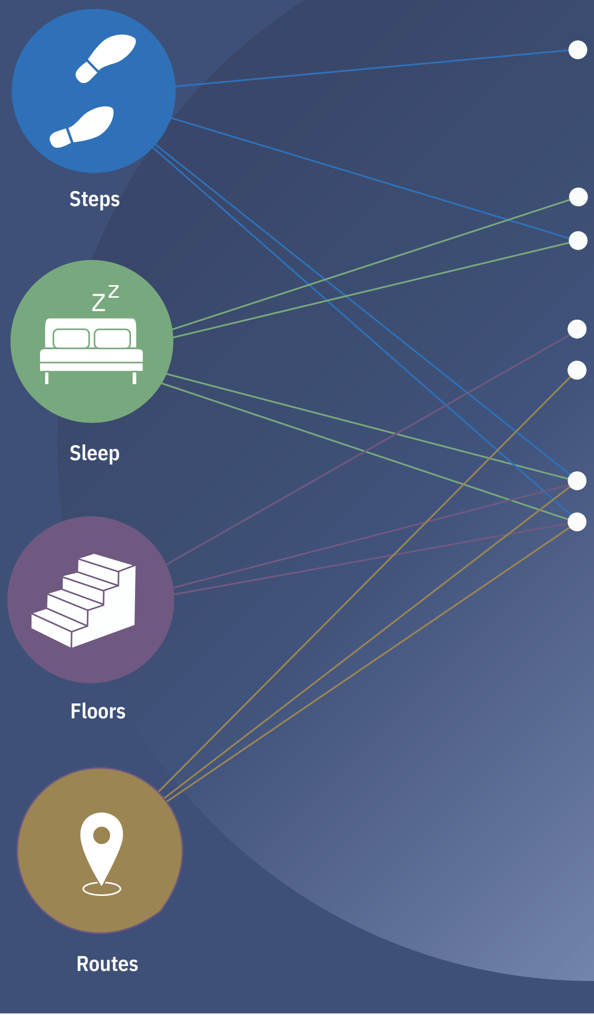
Privacy Implications

While useful in helping you to improve your fitness and health, an employer-sponsored health monitoring program may leave you open to situations where your personal data can be used against you. If you allow an employer access to your fitness tracker data, you may be giving permission to monitor you continuously. Data revealing your location, heart rate, movements, etc. provides an indication of your activities and your health.

Privacy risks with fitness tracker use

The Scenario

A home was robbed. The burglar had hacked the homeowner's fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the owner was likely to come home.



Tracker Function

Steps

Sleep

Floors

Routes

Type of Data

User Provided Data

- stride length (walking)

Data Collected by Sensors

- heart rate
- movement (frequency, duration, intensity & pattern)
- elevation gains
- location (GPS)

System Data

- time
- date

Sharing Practices

accessed by a hacker

Privacy Implications

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user's habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Privacy risks with fitness tracker use

Your fitness tracker is a networked computing device. By using it, you are vulnerable to many of the same security and privacy risks as you are with any other computer you use. Practice basic safety hygiene by making sure your device is secure and private.

Protecting yourself

Actions you can take to minimize risks:

- Weigh the pros and risks of using a fitness tracker before committing to using it
- Decide your own comfort level with collecting and sharing your data
- Understand your fitness tracker's privacy policies and terms and conditions.
- Find out what data is being collected and its implications
- Customize the fitness tracker's default security and privacy settings for your fitness tracker account.
- Set the preferences for sharing your fitness tracker data.
- Check your account settings to ensure no devices other than your own are linked to your account.
- Create a secure, unique password and change it periodically.
- Keep your device firmware and app updated to ensure you receive the latest security updates.
- Turn off the features you don't use.
- Report any relevant suspicious emails or suspicious activity to the tracker company.

Appendix H

Poster Study: Narrative Control Posters

How did this happen?

Data Files

Investigating privacy risks with fitness tracker use

Security and Privacy Threats

Your fitness tracker data can be...
- shared without your knowledge
- used for purposes you are not aware of
- can be misinterpreted or taken out of context
- accessed by hackers
- requested by legal authorities.

If your fitness tracker data is compromised, it may result in...
- financial/property loss
- identity theft
- surveillance
- profiling
- stalking
- extortion.

Using a fitness tracker can leave you open to privacy risks. We present *data files,* a set of posters that demonstrate possible risks.

For each case you're shown "the evidence" describing the circumstances that contribute to the risk (the tracker functions, the type of data used, the data sharing practices) and privacy implications. Next, *data files* suggests actions to minimize risks.

Tracker Functions:

Every fitness tracker has core functions and functions selected by the user.

Type of Data:

The fitness tracker uses and collects data that is: input by the user*; gathered by sensors; or is generated by the operating system. This data can be combined with data from other sources, posing further risks.

Sharing Practices:

Users can specify with whom they share their data, but others can have access too. 1) Fitness tracker companies share your data with "partners", 2) legal authorities can request access to your data, and 3) your data can be hacked.

* The tracker requires user provided personal data to function (name, email, password, gender, birthday, height, weight, time zone). Users may also provide other details (profile photo, biography, country information, and community username).

Case #1

The Scenario

Fitness tracker data was used in a murder investigation, where Jane Doe's data showed the precise time for a spike and then a sudden stop in her heart rate. This information was linked to time-stamped video footage of a car parked in her driveway. The owner of the car was named a suspect in her murder.

The Evidence

Jane Doe used her tracker for:	**Steps**	**Sleep**	**Other Data**
Jane Doe's tracker collected:	**User Provided Data** Stride length (running) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	+ Video surveillance footage
Jane Doe's data was shared with:	The Police		

Privacy Implications

By court order, legal authorities can gain access to your fitness tracker. While this may be useful for solving crimes, this type of access could be misused. For example, data may be taken out of context or misinterpreted. Data collected by these devices is not 100% reliable and could pose a risk if the data is misused.

Investigating privacy risks with fitness tracker use

Data Files

Case #2

The Scenario

John participated in an employer-sponsored wellness program. He was given a fitness tracker monitored by his employer. After six months, he was fired because his fitness tracker data showed he came to work late, left early, and took too many “breaks” throughout the day.

The Evidence

John used his tracker for:	Steps	Sleep	Workouts
John’s tracker collected:	**User Provided Data** Stride length (walking) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	**User Provided Data** Stride length (running) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate Pace Distance Location (GPS) **System Data** Time Date

John’s data was shared with:	His Employer

Privacy Implications

While useful in helping you to improve your fitness and health, an employer-sponsored health monitoring program may leave you open to situations where your personal data can be used against you. If you allow an employer access to your fitness tracker data, you may be giving permission to monitor you continuously. Data revealing your location, heart rate, movements, etc. provides an indication of your activities and your health.

Case #3

The Scenario

Sally’s home was robbed. The burglar had hacked the homeowner’s fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the Sally was likely to come home.

The Evidence

Sally’s used her tracker for:	Steps	Sleep	Floors	Routes
Sally’s tracker collected:	**User Provided Data** Stride length (walking) **Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Heart rate **System Data** Time Date	**Data Collected by Sensors** Movements (frequency, duration, intensity & patterns) Elevation gains **System Data** Time Date	**Data Collected by Sensors** Location (GPS) **System Data** Time Date
Sally data was accessed by:	A Hacker			

Privacy Implications

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user’s habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Protecting Yourself

Your fitness tracker is a networked computing device. By using it, you are vulnerable to many of the same security and privacy risks as you are with any other computer you use. Practice basic safety hygiene by making sure your device is secure and private.

Actions you can take to minimize risks:

- Weigh the pros and risks of using a fitness tracker before committing to using it
- Decide your own comfort level with collecting and sharing your data
- Understand your fitness tracker's privacy policies and terms and conditions.
- Find out what data is being collected and its implications
- Customize the fitness tracker's default security and privacy settings for your fitness tracker account.
- Set the preferences for sharing your fitness tracker data.
- Check your account settings to ensure no devices other than your own are linked to your account.
- Create a secure, unique password and change it periodically.
- Keep your device firmware and app updated to ensure you receive the latest security updates.
- Turn off the features you don’t use.
- Report any relevant suspicious emails or suspicious activity to the tracker company.

Appendix I

Poster Study: Explorative Control Posters

Privacy risks with fitness tracker use

Using a fitness tracker can leave you open to privacy risks. We present a set of posters that demonstrate possible risks. For each case, you're shown the circumstances that contribute to the risk (the tracker functions, the the type of data used, the data sharing practices) and the privacy implications. Next, we suggest actions to minimize risks.

Tracker Functions

Every fitness tracker has core functions and functions selected by the user.

+

Type of Data

The fitness tracker uses and collects data that is: input by the user*; gathered by sensors; or is generated by the operating system. This data can be combined with data from other sources, posing further risks.

+

Sharing Practices

Users can specify with whom they share their data, but others can have access too. 1) Fitness tracker companies share your data with "partners", 2) legal authorities can request access to your data, and 3) your data can be hacked.

=

Privacy Risks

Your fitness tracker data can be...

- shared without your knowledge
- used for purposes you are not aware of
- misinterpreted or taken out of context
- accessed by hackers
- requested by legal authorities.

If your fitness tracker data is compromised, it may result in...

- financial/property loss
- identity theft
- surveillance
- profiling
- stalking
- extortion.

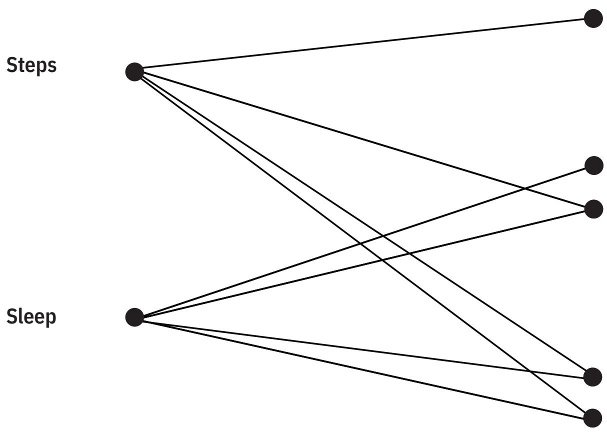
* The tracker requires user provided personal data to function (name, email, password, gender, birthday, height, weight, time zone). Users may also provide other details (profile photo, biography, country information, and community username).

Privacy risks with fitness tracker use

The Scenario

Fitness tracker data was used in a murder investigation, where a victim’s data showed the precise time for a spike and then a sudden stop in her heart rate. This information was linked to time-stamped video footage of a car parked in her driveway. The owner of the car was named a suspect in the murder.

Tracker Function



Steps

Sleep

Type of Data

User Provided Data

stride length (walking)

Data Collected by Sensors

heart rate

movement (frequency, duration, intensity & pattern)

System Data

time

date

+

Data From Other Sources

video surveillance footage

Sharing Practices

shared with police

Privacy Implications

By court order, legal authorities can gain access to your fitness tracker. While this may be useful for solving crimes, this type of access could be misused. For example, data may be taken out of context or misinterpreted. Data collected by these devices is not 100% reliable and could pose a risk if the data is misused.

Privacy risks with fitness tracker use

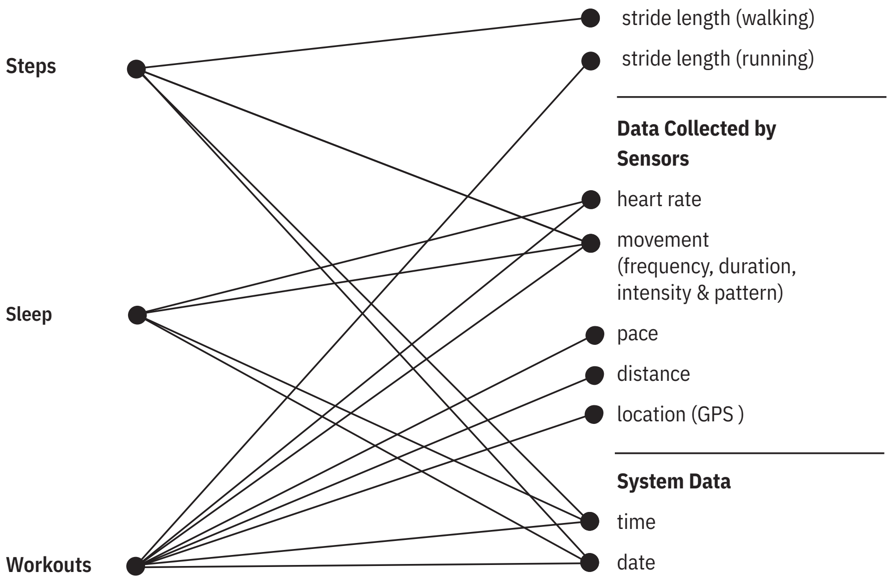
The Scenario

A man participated in an employer-sponsored wellness program. He was given a fitness tracker monitored by his employer. After six months, he was fired because his fitness tracker data showed he came to work late, left early, and took too many “breaks” throughout the day.

Tracker Function

Type of Data

Sharing Practices



Steps

Sleep

Workouts

User Provided Data

stride length (walking)

stride length (running)

Data Collected by Sensors

heart rate

movement (frequency, duration, intensity & pattern)

pace

distance

location (GPS)

System Data

time

date

shared with employer

Privacy Implications

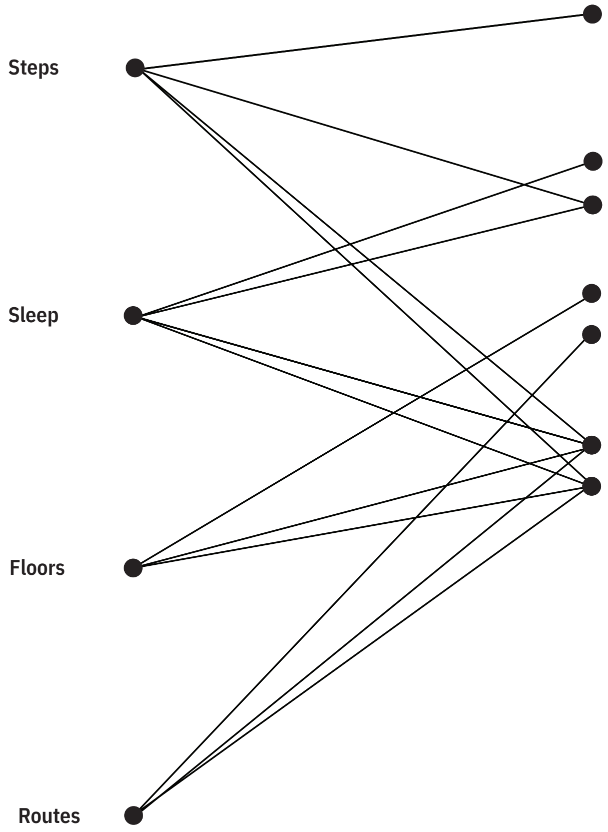
While useful in helping you to improve your fitness and health, an employer-sponsored health monitoring program may leave you open to situations where your personal data can be used against you. If you allow an employer access to your fitness tracker data, you may be giving permission to monitor you continuously. Data revealing your location, heart rate, movements, etc. provides an indication of your activities and your health.

Privacy risks with fitness tracker use

The Scenario

A home was robbed. The burglar had hacked the homeowner’s fitness tracker data that revealed information about her home and habits. He could see her precise location, guess the general layout of her home, and predict when the owner was likely to come home.

Tracker Function



Type of Data

User Provided Data

stride length (walking)

Data Collected by Sensors

heart rate

movement (frequency, duration, intensity & pattern)

elevation gains

location (GPS)

System Data

time

date

Sharing Practices

accessed by a hacker

Privacy Implications

While helpful for improving fitness and health, using a fitness tracker may provide a hacker with personal information that reveals a user’s habits. Fitness tracker data gives clues about when a user would be away from home, and the location and general layout of the house. This leaves users vulnerable to hackers who could plan and commit a robbery.

Privacy risks with fitness tracker use

Your fitness tracker is a networked computing device. By using it, you are vulnerable to many of the same security and privacy risks as you are with any other computer you use. Practice basic safety hygiene by making sure your device is secure and private.

Protecting yourself

Actions you can take to minimize risks:

- Weigh the pros and risks of using a fitness tracker before committing to using it
- Decide your own comfort level with collecting and sharing your data
- Understand your fitness tracker's privacy policies and terms and conditions.
- Find out what data is being collected and its implications
- Customize the fitness tracker's default security and privacy settings for your fitness tracker account.
- Set the preferences for sharing your fitness tracker data.
- Check your account settings to ensure no devices other than your own are linked to your account.
- Create a secure, unique password and change it periodically.
- Keep your device firmware and app updated to ensure you receive the latest security updates.
- Turn off the features you don’t use.
- Report any relevant suspicious emails or suspicious activity to the tracker company