# UNDERSTANDING AND DESIGNING FOR SHARING AND PRIVACY IN WEARABLE FITNESS PLATFORMS

by

Abdulmajeed Alqhatani

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2021

Approved by:

_____
Dr. Heather Lipford

_____
Dr. Mohamed Shehab

_____
Dr. Weichao Wang

_____
Dr. Tricia Turner

# ABSTRACT

ABDULMAJEED ALQHATANI. Understanding and Designing for Sharing and Privacy in Wearable Fitness Platforms. (Under the direction of DR. HEATHER LIPFORD)

Commercial wearable devices that collect health and fitness data are widely used. These devices sense and collect a variety of personal data, which can be shared by users with other people and with third parties. Yet, the collection of personal data by these sensor devices and the sharing of it poses several risks, including stalking, secondary use, aggregation, and inferences. In this dissertation, I present a detailed understanding of fitness tracker users' sharing practices, concerns, awareness, and needs. The main goal is to design controls and features that empower users over the sharing and privacy of their information. My research utilized different approaches, including semi- structured interview, survey, and participatory design studies. Overall, the findings uncover several sharing patterns by fitness tracker users, with practices in each pattern based on the intended audiences. While users do not consider much of the data collected by their devices sensitive, they have concerns about the possibility of abusing their data. However, users have limited awareness about the potential to infer personal information from the primary data collected by activity trackers. My research provides several factors that might impact users' perceptions and attitudes towards inferences in the context of IoT wearable devices. Lastly, my research presents a set of taxonomies for sharing and privacy controls and mechanisms in fitness tracker platforms and contributes several design guidelines.

# ACKNOWLEDGEMENTS

First, I would like to thank my beloved family: my parents for instilling in me the love of learning since I was a child; my wife who has always supported me during my Ph.D. journey; my brothers and sisters for their encouragement; and my beautiful daughter, Layan, for bringing happiness and joy to my life.

Special thanks to my advisor, Dr. Heather Lipford. She guided me step by step throughout my research and has always been ready to help. Dr. Lipford is more than a mere mentor; she is supportive and encouraging, and she has become an integral member of my support system. I'm lucky to have had the opportunity to learn from her incredible knowledge and expertise, which will certainly influence me in my career.

I am also grateful to my dissertation committee members, Dr. Mohamed Shehab, Dr. Weichao Wang, and Dr. Tricia Turner, for their valuable feedback and suggestions. Also, I thank my friends and members of the Human-Computer Interaction lab who helped me in my doctoral studies. My thanks extend to the faculty and staff members of the Department of Software and Information Systems for their support and to the University of North Carolina at Charlotte for this exceptional education experience.

Finally, I would like to express my appreciation to Najran University and to my country, the Kingdom of Saudi Arabia, for providing me the opportunity to pursue my education in the United States.

TABLE OF CONTENTS

LIST OF FIGURES xi

LIST OF TABLES xii

CHAPTER 1: INTRODUCTION 1

1.1 Problem Statement 4

1.2 Research Outline & Questions 5

1.3 Contributions 9

CHAPTER 2: BACKGROUND 10

2.1 Wearable Fitness Devices 10

2.2 Wearable Fitness Data Sharing 12

2.3 Privacy Concerns 14

2.3.1 Data Control & Ownership 14

2.3.2 Perceived Sensitivity 15

2.3.3 Inferences 16

2.3.3.1 Potential inferences 17

2.3.3.2 Awareness 18

2.3.3.3 Attitudes 20

2.4 Sharing Controls and Awareness mechanisms 22

CHAPTER 3: “THERE IS NOTHING THAT I NEED TO KEEP SECRET”: SHARING PRACTICES AND CONCERNS OF WEARABLE FITNESS DATA 25

3.1 Motivations 25

3.2 Methodology 27

3.2.1 Interview Study 27

3.2.2 Participants 28

3.2.3 Data Analysis 28

3.2.4 IRB Approval 29

3.2.5 Limitations 30

3.3 Results 30

3.3.1 Use: Motivations & Contexts 31

3.3.2 Patterns of Goals & Audiences 33

3.3.2.1 Friends 34

3.3.2.2 Family 36

3.3.2.3 Strangers 37

3.3.2.4 Physicians 38

3.3.2.5 Financial incentive programs 39

3.3.2.6 Co-workers 40

3.3.3 Sharing Impact 41

3.3.4 Privacy Concerns 43

3.4 Discussion & Implications 46

3.5 Summary 50

CHAPTER 4: USERS' PERCEPTIONS AND ATTITUDES TOWARDS INFERENCES IN WEARABLE FITNESS TRACKERS 51

4.1 Motivations 51

4.2 Methodology 53

4.2.1 Semi-Structured Interviews 53

4.2.2 Online Survey 55

4.3 Results 56

4.3.1 Interview Results 57

4.3.1.1 Participant profiles 57

4.3.1.2 Primary data 58

4.3.1.3 Inference Perceptions and Attitudes 60

4.3.1.4 Emerging Factors 64

4.3.1.5 Mitigation and Potential Solutions 67

4.3.1.6 Summary 68

4.3.2 Survey Results 69

4.3.2.1 Participants 69

4.3.2.2 Knowledge of Data Practices 70

4.3.2.3 Sharing Comfort with Recipients 71

4.4 Limitations 75

4.5 Discussion and Implications 75

4.5.1 Reasons for lack of awareness 76

4.5.2 Comfort with inferences 77

4.5.3 Implications 79

4.6 Summary 83

CHAPTER 5: EXPLORING THE DESIGN SPACE OF SHARING AND PRIVACY MECHANISMS IN WEARABLE FITNESS PLATFORMS 84

5.1 Motivations 84

5.2 Design Space Exploration 84

5.3 Findings 85

5.3.1 Sharing Mechanisms 86

5.3.2 Data Collection Awareness Mechanisms 96

5.4 Discussion 98

5.4.1 Sharing Patterns 98

5.4.2 Data Collection Awareness 101

5.5 Summary 102

CHAPTER 6: CO-DESIGN FOR SHARING AND PRIVACY IN WEARABLE FITNESS TRACKERS 104

6.1 Motivation 104

6.2 Methodology 105

6.3 Findings 109

6.3.1 Sharing, Privacy Concerns and Management 109

6.3.2 Co-design Sessions 112

6.3.2.1 Privacy 113

6.3.2.2 Social Interaction 117

6.3.2.3 Considerations of Different Health & Fitness Goals 119

6.3.2.4 Clarity and Consistency 122

6.4 Summary and Discussion 124

CHAPTER 7: DISCUSSION, DESIGN GUIDELINES, AND CONCLUSION 128

7.1 Design Guidelines 132

7.2 Future Research 133

7.3 Conclusion 134

REFERENCES 136

APPENDIX A: CHAPTER 3 INTERVIEW SCREENING SURVEY 147

APPENDIX B: CHAPTER 3 INTERVIEW QUESTIONS 148

APPENDIX C: CHAPTER 4 INTERVIEW SCREENING SURVEY 150

APPENDIX D: CHAPTER 4 INTERVIEW QUESTIONS 151

APPENDIX E: CHAPTER 4 ONLINE SURVEY QUESTIONS 153

APPENDIX F: CHAPTER 4 ADDITIONAL SURVEY RESULTS 165

APPENDIX G: CHAPTER 6 EMAIL RECRUITMENT 166

APPENDIX H: CHAPTER 6 SOCIAL MEDIA POST FOR RECRUITMENT 167

APPENDIX I: CHAPTER 6 SCREENING SURVEY 168

APPENDIX J: CHAPTER 6 PARTICIPATORY DESIGN 170

# LIST OF FIGURES

Figure 1: Classification of Wearable Fitness Devices 11

Figure 2: Participants' Knowledge Regarding Data Practices 70

Figure 3:Users' Comfort with Sharing Primary Data vs. Derived Information 72

Figure 4: Likelihood That Each of The Six Scenarios Can Occur. 74

Figure 5: Importance of Specific Factors Based on Inferred Information 74

Figure 6: Sharing Fitness Tracker Data on Facebook (Samsung Health) 91

Figure 7: Family Feature within Fitbit 93

Figure 8: Two Data Access Representation by Fitbit for Two Third Party apps 95

Figure 9: Customization 114

Figure 10: Marks Made by Participants about Privacy of Comments 116

Figure 11: Features for Competitions 117

Figure 12: Feature Designed by a Group for Tracking and Analyzing Activity Trends 118

Figure 13: Interface for Sharing with Doctors 120

Figure 14: Feature with Different Options for Supporting Goals 121

Figure 15: Feature for Comparing an Exercise Level Against Friends and Groups 122

# LIST OF TABLES

Table 1: Summary of Participants' Information 29

Table 2: Participants' Goals & Practices Based on Audience 34

Table 3: Interview Participants Information 58

Table 4:Scenarios on Inferences 62

Table 5: Devices Used by Survey Participants 70

Table 6: Stat. Dif. of Primary Data Vs. Inferred Information (Sig. p-values are bolded) 73

Table 7: Taxonomy of the Sharing Patterns in Five Wearable Device Platforms 86

Table 8: Taxonomy of Boundary Controls in Wearable Fitness Platforms 88

Table 9: Visibility Controls of Activity Information 89

Table 10: Visibility Controls of Groups 94

Table 11: Participants' Information (Participatory Design) 107

Table 12: Sharing Audiences of Participatory Design Participants 111

Table 13: Summary of Features 113

# CHAPTER 1: INTRODUCTION

Internet of Things (IoT) devices have been integrated into many aspects of our lives, ranging from smart wearables that track individuals' activities, to home automation with a variety of connected appliances, and to smart cities that can reduce power consumption. These internet-connected devices are laden with a variety of sensors (e.g., accelerometers, gyroscopes, GPS) to capture data about the surrounding environment, which can be communicated between these devices and their users as well. Utilizing such devices has facilitated human's tasks in different domains, increased productivity, and improved quality of life.

Among those IoT applications that have a widespread adoption are wearable fitness devices. This is evidenced by the increasing sales of this category of wearables over the past years [32]. Researchers estimate that wearable device shipments will be doubled in 2022 compared to 2018, reaching 233 million units sold with a value of $27 billion [69]. More than 75% of those devices are personal fitness trackers, including smartwatches with fitness tracking capabilities. The increasing demand for wearable fitness devices suggests that they have the potential to provide numerous benefits to consumers.

Available in different shapes and with numerous sensors, commercial wearables continually collect personal data, such as location, steps taken, distance traveled, calories consumed, sleep quality, and many others. Through these metrics, users can monitor different aspects of their health and fitness. For example, people who are overweight can take advantage of features, such as step count and food intake, to improve their health practices. In addition, individuals with chronic disease, including diabetes and hypertension, can utilize these personal trackers to monitor their vital signs regarding any

abnormal health conditions. Some devices, such as Fitbit, not only keep track of one's fitness data but also remind users to increase their physical activity. Wearable fitness devices are now part of the so-called "quantified-self," monitoring and analyzing aspects of one's body and life using digital technologies [46].

Many wearable fitness devices today enable users to share their fitness data with different individuals and parties. For example, some devices have embedded social features that allow users to share activity information with friends and family. The social element can be encouraging to stay accountable toward fitness goals. As an alternative, some devices allow users to broadcast their data to popular social media networks, such as Facebook and Twitter, in order to reach further audiences. Users can also connect their trackers with different external apps, such as pharmacies and health-related apps.

Researchers have investigated why individuals disclose personal fitness data, prior to the wide adoption of personal fitness trackers. Users share this data socially for accountability and emotional support regarding specific health goals (e.g., weight loss), especially with individuals who have similar interests or who went through similar experiences [19, 53, 76]. Sharing personal information with such people can motivate users to achieve their health goals. Self-presentation is another common goal for sharing fitness information by many users [19, 53]. Thus, social media platforms are good venues to communicate positive healthy behaviors. In addition, users share their fitness data with different organizations for several benefits, such as financial discounts on health insurance. With the introduction of wearable fitness devices that sense a variety of data and provide interaction capabilities, sharing fitness information has become more convenient and easier.

However, collecting personal data continuously and sharing it impose several privacy concerns. For example, sharing data of an exercise route can be used by criminals to pinpoint a user's home address and sensitive locations [72]. Even if the information is shared only with known people, users sometimes may not feel comfortable sharing fitness information with certain connections, such as workmates. In addition, there is a concern that organizational actors (e.g., marketers and insurers) might access users' data without users' permission. If users are skeptical about how their information is used, they may forgo their privacy, or alternatively, stop using the service. This calls for solutions that empower users to manage their privacy and help to inform their privacy decisions before disclosing their personal data.

Privacy controls are common mechanisms that can be used to restrict access to personal information. However, there has been limited research that looked into how effective the existing controls of wearable fitness platforms are in supporting users in managing their privacy. Privacy notices are another mechanism that can inform users about companies' data practices. Nevertheless, the usability of many of the existing notices remains a problem, especially in the case of wearable devices that typically have limited screen size. Even if users are aware of a device company's data practices, third parties have their own policies that users need to learn about.

Several regulations exist to protect the privacy of consumers' health information. For example, in the U.S., the Health Insurance Portability and Accountability Act (HIPAA) seeks to protect consumers' health information [4]. However, HIPPA does not cover information that is not identifiable, such as what is collected by wearable fitness devices. Data is stored anonymously in the manufacturers' databases, but it is still prone to

inferences and even re-identification. The embedded sensors can capture numerous personal data, which can be used independently or in combination with data from other sources (e.g., public records and social media) to reveal undisclosed personal information. For example, the GPS feature reveals certain places users visit (e.g., coffee shop, sport center, religious places). Location is one common type of data that users consider sensitive, but there are generally other concerning sensors' data that can be exploited to infer highly private information. For instance, heart rate data can reveal sexual activity, emotions, and mood such as stress. Yet, it remains unclear how aware users are of these potential inferences, and whether users' awareness influences their privacy and sharing decisions. It is also not fully understood how the settings of the current devices and their platforms support users to control their privacy.

## 1.1 Problem Statement

Privacy in wearable devices has been a major concern. Prior research has examined the sharing of health and fitness data collected by these devices as an important aspect of privacy. A great deal of that research has focused on examining users' goals and practices of the sharing of this data, primarily on social media or within workplaces [17, 19, 25, 28, 57, 74, 76]. Other research has investigated people's perceptions of the sensitivity of this information and their awareness about companies' data practices [42, 80]. Despite the existing research on the sharing of information collected by fitness trackers, we lack a holistic view of all forms of sharing patterns, which can help us to gain better insight into users' behaviors.

One of the major concerns associated with devices that collect health-related data is the ability to infer private information about users (e.g., health status). Thus, a number of studies have investigated users' awareness and behaviors regarding this issue [7, 65, 70].

Those studies showed that people have limited knowledge about privacy problems resulting from the collection and sharing of sensor data. Yet, users' understanding about privacy issues in the context of these devices, and how this could relate to their sharing decisions with different audiences, have not been examined.

Privacy concerns can be mitigated if users are empowered to control the collection and sharing of their information. As in other contexts, users of wearable fitness trackers have sharing considerations— what information to share, with whom, and how. This suggests that fitness tracker users need effective mechanisms that satisfy their sharing preferences and help them in protecting their information. Unfortunately, there is little research that contributes actual design solutions to privacy problems in wearable fitness devices and their platforms. Past research on the sharing of this type of information has mainly focused on understanding users' behaviors through interviews, focus groups and surveys.

Taking these research limitations together, I aim to present design guidelines that address users' need for sharing and privacy and improve their awareness about potential privacy risks associated with the collection and sharing of their information by these kinds of sensor devices. In doing so, I need to first understand all forms of users' sharing practices, as well as their perceptions and behaviors regarding privacy issues in these technologies.

## 1.2 Research Outline & Questions

My research provides an in-depth examination of wearable fitness data sharing as an important aspect of privacy. The primary goal is to present design guidelines that can help users to control the sharing of their information and enhance their privacy. I investigate the following research questions:

1) What are users' practices and privacy-related behaviors when sharing health and fitness data recorded by wearable sensing devices?
2) What are users' perceptions about potential inferences based on sensor data, and how do those perceptions relate to users' sharing and privacy decisions?
3) What controls and mechanisms do current devices have for sharing and privacy management?
4) What new mechanisms are needed to better match users' desired sharing practices and privacy behaviors?
5) How can new mechanisms be designed to help users manage the sharing and privacy of their information?

The first question was addressed through semi-structured interviews (chapter 3) I conducted with existing users of different fitness trackers [9]. My original goals were to examine how the design of the devices and sharing platforms, the sensitivity of certain kinds of data, and the availability of controls influence users' disclosure behaviors. However, I found that users' sharing behaviors and decisions had less to do with the design of controls and the sensitivity of data. Rather, users' behaviors are primarily impacted by a set of common sharing patterns, relating goals, audiences, and specific practices. The overwhelming perception among the study participants is that most wearable fitness data, in particular step count, is not sensitive. While the participants did realize that potential private information could be inferred from their tracker data, they did not provide concrete examples of how such inferences could be done.

Thus, the purpose of the study of chapter 4 is to address the second research question by investigating people's perceptions of the personal information that can be inferred from

data collected by fitness tackers by other individuals, device manufacturers, and external parties, and whether such inferences influence users' privacy behaviors and decisions. The study utilizes semi-structured interviews and an online survey with both sharers and non-sharers of fitness tracker information. During the interviews, participants were asked to list all the personal information they think can be predicted about themselves from the sensor data collected by their devices. The study participants were presented with several privacy scenarios, focusing on data that are generally considered less sensitive, such as step count and heart rate. In the interviews, I asked the participants how comfortable they would be if certain personal information is inferred about them, and what they think are the possible risks of these inferences. My interview findings suggest that users may lack awareness that additional information could be derived from the data collected by fitness trackers and shared by users. The interview participants' attitudes toward inferences are impacted by several considerations that include the likelihood that inferences can occur, the accuracy of data that can be inferred, perceived value, notice and consent, and anonymization. Thus, the online survey aims to examine my findings from a larger sample of users. The survey also explores users' comfort with sharing different types of primary data and inferred information with different recipients. The survey results showed additional evidence that users lack awareness about inferences from primary sensor data. My survey participants were less comfortable sharing derived information than primary data across all recipients.

In chapter 5, I combined the findings from the first two studies to explore wearable fitness tracker's platforms regarding sharing and privacy control mechanisms. The main goal is to identify unexplored design opportunities around these mechanisms. For example, I investigated whether a device platform enables users connect with friends on social media

channels, and what interface features these platforms have for privacy awareness. I analyzed and compared five popular device platforms for tracking fitness and formalize several taxonomies. I found similar privacy features among those platforms, such as the features for creating fitness groups and for pushing data to social media apps. However, the investigated platforms lack privacy nudges, such as those that actively inform users about third party use of their data.

Previous research has focused on understanding fitness tracker users' sharing practices and privacy behaviors through qualitative and quantitative research methods [19, 42, 44, 70]. However, there are few studies that provide design solutions to the sharing and privacy issues in the context of wearable fitness devices. Thus, in the last stage of my dissertation I conducted participatory design sessions with pairs of Fitbit users. Fitbit is among the top selling wearable fitness trackers on the market [62]. My main goal was to understand privacy needs and to elicit design ideas from end users. Prior to each design session, I interviewed each participant pair and asked them how they share their information and what type of privacy controls they would like the Fitbit to have. I then asked them to co-design together new features that could improve the sharing and privacy of users' information over the app. Many of the proposed designs by users intersect with the findings in the previous studies, such as the need for granular sharing in terms of data and recipients.

Chapter 7 concludes this dissertation with a discussion of the main findings and contributions and presents design guidelines for enhancing privacy in wearable fitness devices.

Finally, I would note that portions of this dissertation have been published in the Symposium on Usable Privacy and Security [9]. Chapter 5 of this dissertation has also been accepted for publication in the Workshop on Usable Security and Privacy [10].

## 1.3 Contributions

My dissertation contributes to existing research by expanding the knowledge on sharing and privacy of information collected by wearable fitness trackers. It provides insights into people's perceptions, practices, and concerns regarding their information. The main contribution is a set of design guidelines for sharing and privacy in wearable fitness devices. In summary, this dissertation has the following contributions:

- It enriches existing literature regarding sharing aspects of data collected by these novel technologies by providing a holistic view of all forms of users' sharing goals and related practices.
- The mixed methods provide better insights into users' privacy behavior regarding sensor devices that collect health data, and how this behavior relates to sharing decisions.
- It presents taxonomies of controls and mechanisms in fitness device platforms and identifies design opportunities for enhancing privacy and supporting sharing goals and preferences.
- Co-designed features by end-users that indicate their sharing and privacy needs
- A set of design guidelines proposed based on the findings from several user studies that can help in developing sharing and privacy controls and features.

# CHAPTER 2: BACKGROUND

Collecting and sharing sensed fitness data imposes privacy concerns. In this chapter, I will first present a brief overview of wearable devices that can track health and fitness data. Next, I will discuss the related work on the sharing and privacy of information in these devices from both social and data privacy lenses. This chapter will conclude by reviewing the sharing and privacy mechanisms within wearable fitness devices, as well as the existing solutions for privacy issues associated with these devices.

## 2.1 Wearable Fitness Devices

Technology has evolved, becoming more powerful and smaller in size. Today, a variety of wearable IoT devices that track health and fitness are widely adopted. Many of these devices have sensors that collect various data, such as movement and vital signs. Data collected by these devices can be synchronized with mobile apps through Bluetooth Low Energy (BLE), connected to the internet via Wi-Fi, and stored in the cloud [29]. Wearable fitness trackers commonly have their own platform that enables users to analyze their self-tracking data. In this research, I define wearable fitness trackers as any small digital device with embedded sensors, and possibly internet connection capability, that can be worn on the body to continually collect and generate data in order to support personal health and fitness tracking.

It is important to distinguish between commercial fitness wearables and another type of health wearables known as Wireless Body Area Networks (WBANs). Although there is an overlap between research on these two topics, the latter is much wider as it integrates a large number of sensors and employs implanted tools to detect and monitor different health conditions [71]. The focus of this research is on commercial wearables, which are simpler

and more personal in nature. Fitbit is one popular example of commercial health and fitness wearables, which enable users to track daily and weekly movement, calories consumed, sleep pattern and several other metrics. In addition, Fitbit and other similar devices offer other features to support users with their fitness goals, such as virtual coaching and social interaction. Commercial wearables for tracking health and fitness are among the top selling IoT devices on the market [39, 69].

There is a lack of research that provides a comprehensive classification of wearable fitness devices, possibly due to the tremendous number of products in the market. Overall, wearable fitness trackers can be classified into accessories or textiles (Figure 1). The first category can be further classified into Wrist-Worn Devices (e.g., Fitbit), Head-Worn Devices (e.g., Samsung Gear IconX), and others, which include smart jewelry (e.g., Motiv ring) and straps (e.g., Polar H10 HR sensor) [71]. The second main category is E-textiles, such as smart shoes. These devices can vary with their sensors and features, but all are capable of tracking personal health and fitness.

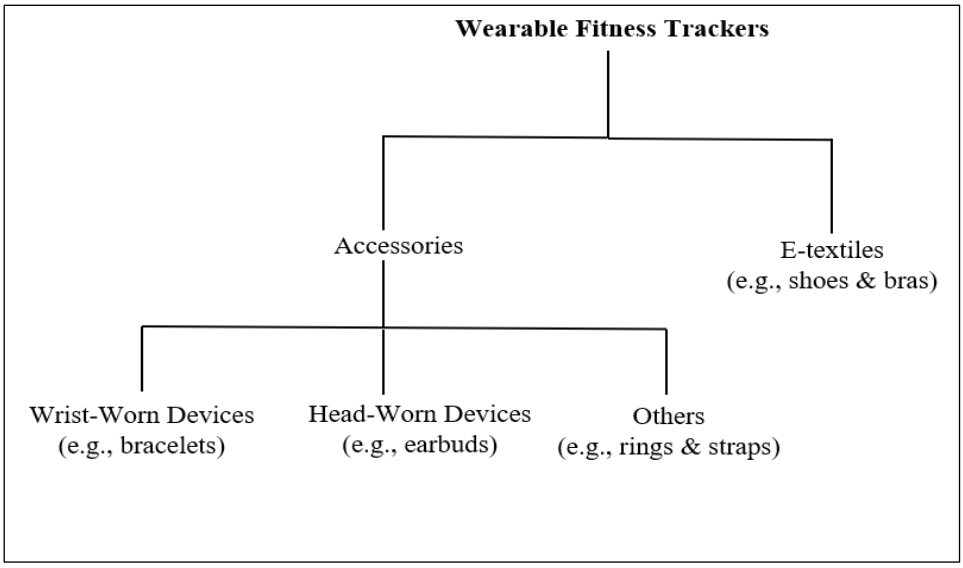



Figure 1: Classification of Wearable Fitness Devices

## 2.2 Wearable Fitness Data Sharing

A number of studies have examined technologies for tracking and sharing fitness data, prior to the widespread adoption of wearable sensing devices. These studies indicate that users find value in sharing activity data (e.g., for accountability, advice, and emotional support), and doing so encouraged them to pursue a healthy lifestyle [55, 76]. However, users sometimes have trouble determining what to share and with whom [51, 53]. In addition, users struggle to find desired sharing features on various platforms [51].

The introduction of wearable fitness trackers has contributed to widespread tracking and sharing of fitness information. Today, many wearable fitness device's platforms have embedded features that allow users to share their data with other users, as well as features to integrate with different external platforms, such as social media applications. Sharing fitness information through these platforms has become an important part of many users' practices toward achieving their health and fitness goals [9]. One study found that half of their participants utilized the features within the devices to support their fitness activities [22].

Thus, a number of studies have examined users' motivations and behaviors of sharing fitness tracker data on different platforms and within different domains [26, 28, 35, 57, 74, 84]. For example, researchers have explored the opportunities of sharing wearable fitness data with people online, primarily on social media sites [28, 36, 57, 74, 84]. Users' motivations for sharing include increasing motivation through accountability, finding social support, and competing with others, all in support of users' health or fitness goals [19, 36]. Indeed, social sharing and competing have been linked with an increased intention to exercise [84]. Some users were also motivated to share in order to help and connect with

others with similar goals; however, finding the right community in terms of what to share and with whom can be challenging [22].

For example, Gui et al. conducted a qualitative study on a fitness plugin for the Chinese social networking service WeChat [28]. Participants preferred utilizing their existing network of social contacts and sharing fitness data as part of their regular social networking practices. Users found increased opportunities for interaction with others who also shared their fitness information. Participants also reflected on the impressions that can be inferred by others as a result of such sharing. However, sharing using such social features may lack emotional support, or can be less effective when sharing with unknown contacts [28].

A similar study by Dong et al., focused on the Chinese site Weibo [19], found that users shared data from the wearable sensing device Mi Band primarily to record their life and motivate themselves. In comparing users' motivations for posting on Weibo versus WeChat, their findings also provide evidence that people have several motivations for sharing on different social network sites based on the different audiences found on different sites [28]. As a result, people may integrate different social platforms into their communication practices in order to reach a broader audience to meet their intended goals [83].

Finally, several researchers have investigated sharing data from activity sensing devices with different companies and organizations, such as employers and insurance companies [17, 25, 26, 60]. Users generally do not feel that step count is sensitive data and are willing to share with their employers and other companies to also receive financial rewards or discounts. However, perceptions can change over time as people gain an understanding of how details of their personal lives and activities are reflected in just a step count [25]. Thus,

the next section investigates privacy issues of sharing personal data collected by fitness trackers.

## 2.3 Privacy Concerns

Altman defined privacy as “the selective control of access to the self” [11]. Given the ability of wearable trackers to continually collect various personal data, several privacy concerns can arise when this data is shared with other individuals or parties. This section reviews the common privacy issues related to the collection and sharing of data collected by fitness trackers. Specifically, it examines the aspects of data control and ownership, perceived sensitivity of data, and inferences.

### 2.3.1 Data Control & Ownership

Researchers have examined privacy concerns on the collection and sharing of sensed fitness information [5, 16, 44, 92]. Users are primarily concerned with the unintended use and lack of control over their personal tracking data [44]. For instance, users are concerned that a health insurance company could access their fitness data without users’ awareness and adjust their coverage’s rate accordingly. People are also concerned that undesirable decisions (e.g., job promotions) can be made based on the wearable fitness data they share [16]. Users of IoT devices are likely to consent to the collection of their data if there are perceived benefits [41], but they also want the ability to opt out at any time [52].

Thus, users strongly desire to retain full control and ownership over their self-tracking data [44]. Users always want to be assured that their data are not kept by device manufacturers after they stopped using the service. However, users’ data may not completely be deleted as companies might store the data in several locations to optimize their services [27]. The desire to control data by users is not limited to the data provided to

organizations, but also when the data is shared socially with different people [92]. Paul and Irvine [58] analyzed the privacy policies of four popular wearable fitness companies. They noted that three of these policies did not provide clear statements about the ownership of data. Users also can be unaware about wearable device company data practices, such as who owns the data, how it can be used, and with whom it can be shared. For example, Vitak et al., found that users of fitness trackers have limited knowledge of the data practices of device manufacturers [80]. Thus, users favored being reminded on a regular basis (e.g., monthly) and in a usable manner to help them make informed decision about the sharing of their personal information [52].

In many countries, regulations protect the collection, storage, and sharing of health-related information. Yet, it is unclear how much data from wearable devices is covered by those regulations [5]. The problem is more complicated with the advancement of interconnected devices, such as IoT devices. Paul and Irvine [58] found that some fitness tracker companies did not comply with existing privacy regulations regarding informing users about the use of health-related data and any updates in the privacy policy.

### 2.3.2 Perceived Sensitivity

Users' concerns about their information obviously depend greatly on the type of information, the recipient, and the reason and benefits for sharing [52, 60]. Several studies have found that users of wearable sensing devices do not find movement data, such as step count, as sensitive [35, 49], and thus people are willing to share such information with many different audiences. However, weight and sleep data are considered more sensitive, depending on the audience [42, 60]. The primary privacy concern is with locational

information captured by devices with GPS. Users are worried that location data shared online can be used by strangers, or even criminals, to know where they live [35, 49].

Researchers have also reported other potential factors that might influence people's perception towards the sensitivity of wearable device data. For instance, the study by Vitak et al., [80] examined users' demographics and their valuation of the personal data collected by fitness trackers. The study shows that users' age and privacy concerns are positively correlated with users' valuation of their wearable fitness data. Becker [13] also noted that users treat self-tracking data differently based on a device focus— data collected by wearable devices with a health focus is considered more sensitive than data collected by those with a fitness focus.

Users do not expect much value to be gained by others from devices that do not store sensitive information, such as financial information [7]. However, the personal health metrics can be lucrative for several parties, such as marketers and data brokers [7, 13]. There is also a possibility to infer private information about users and to even reidentify them from stored anonymized data by combining information together from multiple sources, which I will discuss next.

### 2.3.3 Inferences

Prior studies examined users' concerns regarding the accumulation of personal information on a wide range of online services [14, 18, 79], including exploration of inferences [18, 64]. However, inferences in the context of wearable fitness devices have not been fully explored, particularly from an end-user's perspective. Concerns toward inferences in wearable fitness devices can be linked to users' knowledge and privacy attitudes regarding fitness trackers [7, 9, 23, 49, 65, 70, 80]. I first discuss the potential

inferences that can occur with wearable fitness devices before turning to research on users' awareness and attitudes.

#### 2.3.3.1 Potential inferences

Previous research on inferences has focused on studying individuals' behaviors towards online targeting and advertising, also called Online Behavioral Advertising (OBA). In that domain, researchers define inferences as any information that can algorithmically be derived about users from online and offline sources [30]. The proliferation of IoT devices has led to the potential for unexpected inferences about users' personalities, habits, and physical health. Wearable fitness trackers are one common category of IoT devices that has a number of embedded sensors, such as accelerometers, altimeters, temperature sensors and others that collect and report a range of data to their users. I refer to this data as primary data, which includes things such as step count, heart rate, miles covered, and sleep patterns. In addition to sensed data, users also typically provide personal information, such as gender, weight, and age, to a device's mobile or online platform to take advantage of certain tracking or application features, such as reporting calories consumed.

Researchers have demonstrated that such primary data can be used to infer other information with high accuracy, such as eating moments [77], moods [38], places [48, 86], and sexual activity [45]. In addition, there is wide concern that data generated by fitness trackers might be used in the future for undesirable decisions, such as to disqualify users for employment, insurance, or loans [59]. Studies have noted that current regulations do not protect personal data collected by wearable devices, or that such regulations are outdated and cannot cope up with the increasing legal challenges created by such IoT devices [7, 59]. For example, unlike common sensors, such as cameras and GPS on mobile

phones, fitness tracker sensors do not always require permission to access users' data, and can collect data automatically and continually [37, 38]. The greatest concern is that data collected by IoT fitness trackers might be associated with a user's real identity [7]. The accumulation of data provided by a user (e.g., birth date), along with activity data (e.g., exercise route), contextual data (e.g., timestamps), and online data has been demonstrated to accurately predict users' real identities [7, 23]. As a result, Aktypi et al. [7] stated that their study participants underestimated the risks associated with the usage of their fitness trackers. Users may not be aware of the information that can be inferred from sensor devices [70]. However, what contributes to users' lack of awareness, or otherwise their apathy, towards inferences in the context of wearable fitness devices has not been explored.

Finally, while much of the research on inferences is concerned with information that can be derived algorithmically, users may also be concerned with what people would infer about them based on information shared socially. For example, users who do not have much time to exercise may choose to not share fitness tracker data on social media so friends would not think they were lazy. Thus, in Chapter 4, I also examine perceptions regarding a variety of audiences and kinds of inferences, including those made by other people.

#### 2.3.3.2 Awareness

Apart from IoT devices, researchers have examined peoples' awareness regarding inferences in a wide range of online services [18, 63]. In general, users are aware that their data is processed and stored by service providers [14]. Users can also be aware of online tracking [87], but they may not know that their data could be aggregated and even shared with third parties [14]. Individuals who have greater awareness of data aggregation have

greater likelihood of concerns towards undesirable inferences [63]. Awareness increases when users link inferences to their own past actions [64], and this also influences users to take protective actions [87]. Nevertheless, users sometimes have misconceptions about inferences, and their beliefs about how companies use their data differ from reality [86].

In terms of wearable devices, researchers have examined users' understanding about the information that can be inferred from data collected by these devices [7, 65, 70]. For example, Rader and Slaker [65] investigated the impact of folk theories on users' reasoning about data collected by fitness trackers. The findings reveal that users' conceptions helped them reason about dependencies among data types but did not support users in understanding what additional information can be derived from their data. For example, users who indicated that distance is calculated based on GPS did not mention that home location might also be inferred. In the study of chapter 3, I found that the participants believed that potential private information can be inferred from their tracker data, but they did not provide concrete examples of how such inferences could be done.

There is considerably less work on how awareness of inferences can impact users' behaviors. In an online survey, Schneegass et al. [70] examined how information collection representation in fitness trackers could impact users' willingness to disclose information. More specifically, when data is requested at the sensor level (e.g., accelerometer) versus when it is requested at the information level (e.g., step count). The authors reported that users have inconsistent preferences between these representation levels– participants showed higher willingness to share derived information in certain contexts than sensor data and vice versa. In the study of chapter 4, I investigate potential inconsistencies between primary information, such as step count, and inferred information. As people become more

aware of potential inferences over time, this may discourage them from sharing their personal fitness tracking data. One study from Gorm and Shklovski [25] showed evidence of this, where participants in a workplace campaign discovered how shared step count can reveal additional personal information, and as a result they renegotiated their personal disclosure boundaries with colleagues.

Researchers indicated that users are widely unaware about inferences collected by IoT sensor devices [7, 59, 91]. Yet, little research investigated the factors that contribute to that awareness. Gabriele and Chiasson [23] found that users may not believe that certain inferences are possible, leading them to discount the threats. Other studies have attributed the lack of awareness about inferences by users to the absence of interface cues that help users to speculate about possible inferences [65, 85]. These studies suggest redesigning existing interfaces to enhance users' reasoning about inferences, with a few examples that explore practical approaches to increase awareness. For example, Aktypi et al. [7] present an interactive tool to teach people how their identity and other private information can be revealed by combining data from activity trackers and online social media sites. Other researchers have focused on enhancing awareness through games, as in the work by Williams et al. [88] that presents a serious game to encourage protective behaviors of smart watch users. In chapter 4, I extend this prior work by examining in depth how users perceive various inference scenarios.

#### 2.3.3.3 Attitudes

A number of researchers have investigated users' attitudes about the collection and sharing of fitness tracker data. Attitudes towards this data have been shown to be dependent on data sensitivity [9, 25, 49], risk perception [7], trust [7, 92] and comfort with recipients

[23]. However, we have seen little research examining attitudes towards inferences in this domain. Users' reactions to inferences have been studied in online tracking and advertising [14, 18, 79, 87]. These studies reported that users have mixed feelings about such inferences, considering them "useful", and "creepy" [18, 79]. For example, inferences that are relevant to users' interests are perceived as useful [18, 79], but users can be uncomfortable that they are being monitored [18]. Inferences related to certain data, such as gender, financial and online behavior information are regarded as sensitive [13, 14], but people's comfort was found to be correlated with the accuracy of inferences regardless of sensitivity [14].

The personal nature of fitness tracker data may also result in inferences that users would consider sensitive, such as mood, health status, or location. Yet, researchers report that users do not consider much of the fitness tracker data as sensitive [92], and are generally willing to widely disclose information, such as step count and heart rate. People do not consider information collected and stored by fitness trackers sensitive compared to other information, such as banking information [9]. The primary concern users have is with location data [49]. Studies have also reported that fitness tracker users trust the companies who collect their data and feel that the risk of disclosing their information is low [7, 92]. Finally, users' concerns about the disclosure of their personal data are greatly dependent on who receives the data. Several studies have indicated that users are generally comfortable disclosing their fitness tracker data to friends and family members but are less comfortable providing it to strangers and advertisers [23]. I extend these prior studies by examining similar attitudes and perceptions regarding information that can be inferred from data collected by fitness trackers by different audiences in chapter 4.

## 2.4 Sharing Controls and Awareness mechanisms

Users can utilize different platform mechanisms to control access into their information by other users and organizational actors. These mechanisms should be flexible in order to meet users' varying levels of privacy preferences (what, how, when, and with whom). Unfortunately, there has been little research that examines privacy settings in the context of IoT devices, especially fitness trackers. The focus of previous research has been on improving privacy settings of popular social media platforms. However, studies indicate that users of wearable fitness devices strongly demand granular control over their information [44]. We also lack a study that collectively examines multiple platforms regarding their mechanisms for privacy management, and what new mechanisms are needed to better match users' preferences.

Those few studies that examined platforms of commercial IoT devices aimed to gain insights into their structure, and design similarities and differences. For example, Mare et al. [47] examined several smart home systems to explore their design choices with respect to access control, privacy, and automation. In terms of fitness trackers, Witte et al. [90] analyzed and categorized ten popular wearable device platforms to understand their ecosystem as a whole. They found similar mechanisms among these platforms, such as the features to integrate with social media applications. Epstein et al., [21] developed a framework that aims to guide the design of social sharing in personal fitness informatics. The authors evaluated their framework by analyzing posts made by Runkeeper app users on Twitter. The researchers found that tweets with user-generated text receive more responses than tweets with system generated text, and thus the authors encouraged supporting the manual sharing of fitness information in broader social networks. Other

research focused on managing the complexity of data access and sharing settings in IoT platforms by recommending privacy settings that can match users' preferences [12, 78]. For example, the work by Torre et al. [78] implemented a data-driven method to design a set of customizable recommendations for fitness tracker privacy settings.

Privacy concerns can be mitigated if users are made aware of what information can be collected about them and what risks are associated with such collection. Although studies reported that fitness tracker users seemed to be unconcerned about the privacy of this type of data [49, 80], effective awareness mechanisms may encourage users to reconsider their sharing decisions. Thus, the Human-Computer Interaction (HCI) researchers and interface designers have proposed solutions to help users in making informed decisions about the collection and sharing of their personal data by IoT devices. For example, Wagner et al. [85] proposed a privacy awareness framework named I-AM (Inform- Alert- Mitigate) for e-health technologies, such as fitness trackers. The authors analyzed privacy concerns arising from data collected by these technologies and demonstrated how the framework can be implemented in health technology's interfaces in order to communicate privacy issues and mitigation actions. In another study, Bosua et al. [15] built an intelligent warning system to nudge users about any violation that occurs with their data, such as insecure storage of users' sensitive data in the cloud.

Privacy notices are the primary method to inform user about data practices. Yet, these notices are often unusable and may not effectively communicate to users the mass amount of personal information that can be collected by IoT devices. Egelman et al. [20] designed and evaluated several privacy icons that aim to help users understand privacy notices in ubiquitous sensing platforms. Although many of the proposed icons were able to

communicate what data was being collected, participants had less understanding about other contextual details. Railean and Reinhardt [67] designed “privacy facts” label for IoT devices that aims to help non-expert users prior to buying a device understand how IoT devices collects, processes, and stores data. The results suggest that the privacy label can help users in making informed privacy decisions. In another study, Gluck et al. [24] addresses poor usability of privacy notices in mobile and wearable devices. They used a Fitbit privacy policy to examine if a shortened form of privacy notices can improve users’ awareness. The results show that the short form of a privacy policy did improve users’ awareness about the company’s practices, but only those practices that users are familiar with.

In chapter 5, I explore the design opportunities of five popular wearable fitness device’s platforms based on their sharing and data collection awareness mechanisms. I compare and present several taxonomies of these mechanisms. I believe that these mechanisms are important because they deal with how people can manage their privacy when disclosing personal data with different entities, including individuals, device manufacturers, and third parties.

# CHAPTER 3: "THERE IS NOTHING THAT I NEED TO KEEP SECRET": SHARING PRACTICES AND CONCERNS OF WEARABLE FITNESS DATA

This chapter explores users' intentions for sharing sensed fitness data, how and with whom they share it, and the actions they take to control their privacy. My goals are to understand more about the privacy-related decisions and practices of long-term users of wearable activity devices, and how those decisions are related to users' motivations for disclosing personal information. Based on the findings, I identified several implications to help improve existing platforms regarding sharing fitness information. This chapter has been published in the Fifteenth Symposium on Usable Privacy and Security [9].

## 3.1 Motivations

Sharing health and fitness information has become an important part of many users' practices towards achieving their health and fitness goals. Thus, most wearable devices today have also social features that allow users to share their information and interact with different people and organizations. Some devices like Fitbit have built-in social circles where users can talk about their exercises, goals, and progress. Alternatively, users can broadcast their wearable fitness data on external health and fitness apps (e.g., Strava & RunKeeper), via common communication applications (e.g., WhatsApp), or over popular social media applications (e.g., Facebook & Twitter). In addition, users may share data with insurers or through workplace campaigns to receive rewards to further incentive healthy behaviors. Individuals may utilize several different platforms, and more than one communication channel, and switch between them to share their information online [83].

Researchers have primarily examined fitness data sharing on social media platforms [53, 57, 74, 76] and in the workplace [17, 25, 26], revealing a range of common reasons

and outcomes for sharing. Others have investigated privacy implications and concerns, including the sensitivity of various information and the lack of understanding of fitness trackers' data practices [58, 80]. I expand upon this work by investigating users' practices across the range of sharing that they perform. I examine both aspects of social privacy– how users disclose and interact with other people around their shared data, as well as data privacy issues that arise when they provide their data to additional organizations. As Contextual Integrity theory posits, information sharing is governed by the norms and expectations of the context, and privacy problems occur when those expectations are violated [54]. I aim to examine these considerations in order to gain insights into users' sharing behaviors and needs.

More specifically, contextual integrity suggests that sharing preferences of people may vary based on the receiver, the information type, and transmission principle. Thus, my original goals were to examine how the design of the devices and sharing platforms, the sensitivity of certain kinds of data, and the availability of controls influence users' disclosure behaviors and privacy concerns. However, I found that participants' behaviors had less to do with such factors than with their sharing goals and the associated audiences related to those goals. Therefore, this study contributes a set of common sharing patterns, relating goals, audiences, and specific practices of participants as part of understanding users' privacy decision making and behaviors.

Specifically, my study reports on a qualitative study with 30 existing users of wearable fitness trackers, who have shared their information with different audiences, in order to understand their sharing practices and behaviors. The results indicate that users' concerns about disclosing wearable fitness information are about self-presentation goals and

acceptable behaviors of sharing with people on different platforms, rather than concerns over the sensitivity of data.

This study has the following contributions:

- It enhances the understanding of the sharing of wearable fitness data across the range of platforms and audiences of users.
- It provides a set of common patterns of sharing goals, audiences, and practices.
- It provides insights into users' perceptions regarding their disclosure decisions and privacy considerations and presents implications for researchers and designers to help users share their information as desired.

## 3.2 Methodology

### 3.2.1 Interview Study

I conducted 30 semi-structured interviews with wearable fitness users (15 males and 15 females) to examine their sharing and privacy preferences. As the focus of the study is on the sharing of fitness information, participation was restricted to people who have a wearable fitness device for at least three months and who have shared their information recorded by the device with other people or organizations. Participants were first prompted to fill out an online screening survey. I then contacted the people who met the participation criteria to schedule an interview. All the interviews except one were conducted remotely on the phone, over Skype, or Google Hangout. Interviews lasted on average 25 minutes and ranged from 14 to 43 minutes. Study participants were all compensated with a $10 Amazon gift card for their time after completing each interview.

The interview questions were structured into three parts. The first part discussed the general usage of the wearable fitness devices by participants. I asked the participants how

frequently they use their devices, and how and when they check their sensed data. In the second part, I focused on the users' practices and behaviors with respect to the sharing of their data. For example, participants were asked how they share their information, what information they share and with whom, and what platforms they utilize. Some participants were uncertain about their profiles, so they were requested to go through their accounts to answer the previous questions. This was followed by questions about the participants' sharing practices, and the impact of sharing on their behaviors and use of their devices. In the last part, I asked the interviewees about their privacy concerns and how they manage their privacy. Participants mentioned different scenarios regarding how their information could be misused and expressed several sharing and privacy needs. The full interview is listed in appendix B.

### 3.2.2 Participants

Interview participants were recruited between April and June 2018. Participants were recruited through flyers posted at fitness centers near the university campus, and by advertising on relevant Reddit forums. The methods of recruitment in this study allows to have participants from diverse age groups and professions. The average age of participants was 32 years old, ranging from 20 to 51. Educational backgrounds of the interviewees ranged from high school to doctorate. Table 1 reports the demographics of participants along with the devices they have.

### 3.2.3 Data Analysis

All interviews were audio-recorded and transcribed. I utilized open coding and a qualitative data analysis tool to identify patterns from the participants' responses. Initially, three interview transcripts were analyzed to develop a codebook. Coding saturation was

met after coding these three transcripts, after which no more codes were added. The developed codebook consists of 26 codes. Each code was conceptually assigned to one of three categories: usage, sharing, or privacy. Then, I and another coder independently coded the remaining 27 transcripts using that codebook. We kept track of our disagreements and the calculated inter-rater agreement was 80%. The remaining disagreements were discussed and resolved.

### 3.2.4 IRB Approval

To ensure the protection of human subjects, prior to the start of this study, the university Institutional Review Board (IRB) approved this study as an exempt protocol.

Table 1: Summary of Participants' Information

| | **Gender** | **Age** | **Occupation** | **Device(s)** |
|---|---|---|---|---|
| P1 | M | 38 | Software developer | Nokia |
| P2 | M | 29 | Physician | Apple Watch |
| P3 | M | 34 | Software Engineer | Garmin |
| P4 | M | 39 | Designer | Apple Watch |
| P5 | M | 44 | Self-Employed | Apple Watch |
| P6 | M | 47 | Risk Manager | Apple Watch |
| P7 | F | 29 | Food Services | Apple Watch |
| P8 | F | 28 | Designer | OMbra |
| P9 | M | 38 | Fire Fighter | Garmin |
| P10 | M | 51 | Computer Engineer | Garmin; Fitbit |
| P11 | F | 25 | Gerontology Researcher | Apple Watch |
| P12 | F | 27 | Event Rentals | Jawbone |
| P13 | M | 47 | Finance | Apple Watch |
| P14 | F | 31 | Marketing | Jawbone |
| P15 | M | 32 | Product Manager | Fitbit |
| P16 | F | 35 | Student | Fitbit |
| P17 | F | 35 | GIS Manager | Fitbit |
| P18 | M | 35 | Self-Employed | Apple Watch |
| P19 | F | 22 | Student | Fitbit |
| P20 | F | 26 | HR Manager | Fitbit |
| P21 | F | 27 | Student | Fitbit |
| P22 | F | 26 | Student | Fitbit |
| P23 | F | 32 | Teacher | Fitbit |
| P24 | F | 25 | IT | Apple Watch |
| P25 | M | 27 | Sales | Apple Watch |
| P26 | F | 20 | Student | Polar M600; Polar H10 |
| P27 | M | 27 | Software Administrator | Garmin |
| P28 | M | 48 | Journalist | Jawbone |
| P29 | M | 25 | Student | Nokia |
| P30 | F | 25 | IT project Manager | Motiv Ring |

### 3.2.5 Limitations

This study has limitations similar to many qualitative interview studies: a convenience sample of limited size that may not be generalizable to the broader population of users. The inclusion criteria for participation in this study required at least three months of device usage, which may not be enough to assess the sharing behaviors of the participants. Also, while I attempted to recruit users from diverse ages and professions and balanced participants with respect to gender, I did not consider their cultural backgrounds which may influence participants' views on sharing and privacy. Finally, in focusing on the broad range of participants' self-reported behaviors, interviewees may have neglected to report detailed or accurate sharing behaviors.

## 3.3 Results

Any numbers reported in the results are not meant as quantitative analysis, but merely to indicate prevalence of themes in this sample of participants.

Participants utilize a variety of wearable health and fitness devices that have different sensors to track movements and vital signs (Table 1). The devices used in the study come in different form factors that include smart watch, chest strap, smart bra, and smart ring. Apple Watch is the most common device used by participants, followed by Fitbit. These two are the top-selling brands in the last two years [62]. A few participants have shared information from more than one wearable fitness device, but I excluded devices that have been used for less than three months. It is also noteworthy that Jawbone had gone out of business a few days before the interviews were completed. I begin with a general discussion related to participants' use and perspectives regarding their devices, before moving into more detail about sharing and privacy aspects.

### 3.3.1 Use: Motivations & Contexts

Participants reported several goals for using wearable health and fitness devices. Tracking physical activity, mainly step count, as well as being aware of general health were the primary reasons for use by all participants. Many of the interviewees have sedentary jobs, and they used the devices as a reminder to move. In addition, people make use of wearable fitness trackers to motivate themselves to exercise and to stay accountable. Aside from fitness tracking, a considerable number of participants reported using the devices for medical reasons, such as for recovery after surgery:

> *"I had back surgery in October, so I use it as a tool to make sure that I am maintaining my recovery from my surgery"* [P11].

For many participants, the impact of using a device is measured by whether or not goals are attained, or behaviors have changed. For example, four interviewees who wanted to lose body weight expressed positive attitudes toward the device because it supports them by tracking how many calories they consume and how many pounds they lose every week. Other participants used a wearable tracker to monitor vital signs, such as heart rate, or to track sleep quality. For instance, P22 has sleep apnea and she uses a Fitbit to assist her in detecting the problem. Unlike human beings, a wearable device provides unemotional facts about one's health status. P10 stated:

> *"The device is sort of truth because humanly you can say I have an active day, I have a busy day. In actual fact you were busy on your desk, whereas the fitness device is unemotional. It's unaware of how you're feeling. It's only aware of your physical movement."*

In contrast, two participants did not find their wearable trackers to be helpful in achieving their fitness goals. For example, P6 believed that the device did not change his behavior, and he did not find features like badges and rewards within the device to be encouraging. Another participant indicated that the device was motivating when he first

bought it, but that impact has diminished over time, especially after his best friend who he used to exercise and share information with moved away. In general, the majority of participants were pleased about their wearable trackers and they stated several benefits that they received from their use.

I asked participants why they decided to use the device they have rather than a different device. As expected, Apple Watch was preferred due to its variety of metrics as well as its capability to integrate fitness tracking with other features, such as sending text messages and taking phone calls. Two participants who had Jawbone liked its design that encourages users to keep active by achieving scores. Other devices were chosen for other goals, such as heart rate monitoring. I also found that a single device may not fulfill some users' needs; as a result, they incorporate more than one device into their practice. For example, P26 reported using a smart watch to track her runs and to map routes during soccer games, as well as a chest strap to track heart rate. Similarly, P10 uses one device for running analytics and another one for general health data monitoring. While the wearable devices used by participants have different measurements, all have sensors to capture steps taken.

Participants also expressed different contexts for use. Most of the participants mentioned that they use their wearable tracker at all times even while sleeping. Five interviewees indicated that they use their devices at certain times, mostly when they are exercising or during an activity such as biking. Users reported reviewing regularly, either after a particular activity or in the morning or night to check regular nightly or daily statistics.

### 3.3.2 Patterns of Goals & Audiences

Participants' goals for sharing wearable fitness information are similar to those reported in other studies, such as competing with peers, mutual support, and boasting [19, 36]. However, my study expands on previous research by describing a set of common sharing goals, audiences, and practices. Overall, I found that users make decisions about their audiences based on their goals, which also drive their choices regarding the way they communicate their wearable fitness data. Table 2 summarizes the common goals I found in this study.

Participants' goals were related to their choices of audience to help them with those goals. The analysis revealed six categories of audiences: friends, family, strangers, physicians, financial incentive programs, and co-workers.

Participants shared their information with friends (25/30), family (17/30), or both (13/30). Eleven participants indicated that they shared with strangers, mainly through different health and fitness forums. Sharing wearable fitness data with physicians for medical tracking was mentioned by seven participants; while five interviewees have their devices connected with third party applications, such as insurance companies and pharmacists in order to receive financial discounts or rewards. Finally, four participants identified co-workers with whom they share data. Participants disclose more or less information depending on the recipients and their goals, with practices specific to those goals and audiences. Again, Table 2 summarizes these practices and I now discuss the details of those patterns.

Table 2: Participants' Goals & Practices Based on Audience

| **Goals** | **Targeted Audience** | **Practices** |
|---|---|---|
| Accountability<br><br>Competition<br><br>Boasting a positive self-image | Friends | • Share common sensed data only (e.g. step count).<br>• Sharing mostly done on social media channels.<br>• Share after good physical performance. |
| Support family maintaining a healthy lifestyle<br><br>Mutual & emotional encouragement | Family | • Disclose more information to family than to friends.<br>• Simple ways to communicate wearable data outside of platform |
| Feedback from experienced individuals<br><br>Accountability | Unknown people (strangers) | • Share using device built-in social communities, or on social media communities<br>• Share variety of non-identifiable information related to fitness goals |
| Vital signs monitoring<br><br>Tracking medical conditions (e.g., sleep apnea) | Physicians | • Disclose everything accurately<br>• Compile data manually, or show doctors data in the app. |
| Receive financial discounts/rewards | Insurance companies; Pharmacist; Employers | • Wear the device continuously to maximize the metrics<br>• Provide permission to incentive programs to access data directly on the device, or make sure to update data regularly. |
| Competition in the workplace | Co-workers | • Share step count only.<br>• Set regular step goals and interact with others to achieve. |

3.3.2.1 Friends

The majority of participants shared fitness data collected by wearable trackers with friends, often on social network sites. Accountability was mentioned as a strong motivation for sharing with friends. Participants also indicated that being able to see friends' activity progress and receive notifications about others' achievements encouraged them to pursue

their fitness goals. Sharing can sometimes turn into competition and the desire to outperform each other by being the most active person in the day. Moreover, individuals may feel embarrassed if they failed to meet their fitness goals:

> *"It's kind of partially just a motivational thing but also partially… I guess you can say it's kind of shame like that you know they see if you haven't set or hit your goals."* [P15].

Another goal that emerged from interviewees' responses for sharing wearable fitness data with friends was the intention to boast and communicate a positive image about one's fitness and health. For a few people, accountability can only be met if other users acknowledge good physical performance.

However, sharing with peers for accountability may also impose challenges. A few participants, especially those who may not always have the time to exercise, expressed fears about friends' judgements of their lack of activity. Two participants also did not like to share fitness information with friends on social media because it might be perceived as bragging. Another participant decided to stop sharing with Facebook friends, and instead limited the sharing to a few friends with similar interests on the device's platform:

> *"I kind of started feeling a lot of pressure when I was sharing it because I thought like, oh well if I share on Facebook and I don't share anything for a while, what everybody will think, or they gonna think that I stopped working out. And I think that for me this is on the perfect balance that I can share with my friends on the app and my friends on the app who are active can share with me"* [P22].

Others faced concerns over the broad audience on social media platforms and limited the data they shared accordingly. For example, P12 sometimes found sharing wearable fitness data inappropriate; she stated: *"Facebook friends include co-workers or professional contacts, and it just seemed weird to share my fitness activity with people that I work with or people that I have a contact with them for professional reasons."* Several

other participants chose to not share with friends on social media channels because of perceived lack of interest of their friends on those platforms.

All participants who shared with friends reported sharing basic sensed data, such as step count and distance covered. None of those participants disclosed more personal information with friends, such as body weight, and the majority of the interviewees were unwilling to share their eating habits. In addition, other detailed health data, such as heart rate or blood pressure, were not shared because such data was considered less interesting to friends.

Participants mostly utilized the features within their devices' apps to hook up their data in the trackers with their social media accounts. However, participants are selective on when and what to share in order to maintain a positive self-image. For example, instead of sharing on a regular or automated basis, they only shared data after positive physical performance.

#### 3.3.2.2 Family

Another audience that many participants mentioned sharing with is those they are closest to, primarily family members (e.g., spouse) and occasionally very close friends. In this case, sharing was more about mutual and emotional encouragement. Participants expressed feeling responsible to share their information or any experience they had, whether good or bad, to motivate their loved ones towards a healthy lifestyle:

> *"We did have bad habits when it comes to food, and so I show them look at what happened when I was going through depression in October. Look at how I was eating and look at my heart rate, and look at it right now. You know I share with them to show them, it is like you are family, you are just like I am"* [P5].

P13 commented that he does not usually workout with his wife, but he liked the challenges and notification features generated by the device, which makes it feel as if they

are exercising together. However, only three participants utilized features within devices to share data with family members or a few close contacts. The majority reported using simple techniques to communicate their sensed data. For example, they simply talk about their activity goals and progress or show family members steps count in their trackers. It could be because family members may not have the same device to connect directly with the user.

Family members are typically aware of each other's health conditions; thus, it is not surprising that participants disclose more information to family than to friends. They reported feeling comfortable sharing personal information, such as weight or fitness goals, with family:

> *"If I share it with more people, I would have chosen which specific pieces of information, but I will still share everything with my wife"* [P13].

#### 3.3.2.3 Strangers

More than one third of the participants shared wearable fitness data with unknown people, mainly on fitness forums. Some used the communities on the device's platform, others found forums and groups on various social media sites, such as Reddit and Facebook. By sharing on these fitness forums, participants seek to receive help and feedback from experienced people (e.g., coaches) regarding specific fitness goals, such as weight loss. Holding oneself accountable was also a primary motivation, through interacting with other people with similar interests and goals.

For example, P12 described herself as *"conservative"* with respect to sharing personal information. She used to share her fitness information with her friends on Facebook, but later felt uncomfortable because of a mismatch between her and her friends' interests. This participant then joined a women's fitness group on Facebook and restricted sharing to that

group of strangers with similar interests. P22 also found a fitness group on Facebook and stated such sharing can be an opportunity to build relationships with others with similar goals. Another participant even reported that she is looking for a new device with better support for fitness communities, in order to connect with others with similar interests.

Unlike with friends, participants did report sharing body weight, calories consumed, and the type of food and exercise, in addition to step count. Participants expressed willingness to share because they saw little harm that could come to them:

> *"I guess I share more even when I don't reach my goals because I want to… I don't know, because they are also on the same journey so I feel like it is for accountability and they are not going to use that information in a way that would negatively affect me."* [P12].

However, interviewees were unwilling to disclose data they saw as personal, such as location information, with unknown people due to safety concerns. A few also reported putting fake information in their accounts to protect their identities. In addition, they were less interested in sharing any sensed data that were considered irrelevant to their health or fitness goals.

#### 3.3.2.4 Physicians

It was surprising how many participants also shared their data with doctors or other caregivers. Participants' intentions were to share vital signs with doctors, often due to medical conditions. For example, P22 had been working with her doctor to lose weight by sharing steps taken. In addition, she takes medicine that affects her heart rate functions and uses the device to monitor any heart rate abnormality. She also has sleep apnea and used the sleep logs feature to show her doctor her sleep quality. Another participant (P11) had back surgery and shared her data with physicians to keep track of her walking progress afterwards.

Participants indicated they were comfortable disclosing their data openly with doctors because it would be helpful to manage their health with accurate information. For instance, P18 stated: *"Generally, it made me more diligent in my recordings. I want to get things right if I am showing my doctor the information; it is accurate, and it is not misleading to my professionals."*

Participants expressed frustration with the methods they utilize to communicate their wearable fitness data to physicians. All those participants, except one, reported that they manually record or copy data from the device's website into files, take a screenshot of data, or show their doctors the data in the app. They expressed desire for a centralized control where wearable device data can be integrated with other health information systems such as Electronic Health Records (EHRs) to allow medical providers to directly access their data and interact with them more easily.

> *"I can't just share the data directly with my doctor. I have to compile the data and then present a report to my doctor, and that can be frustrating and time consuming."* [P18].

3.3.2.5 Financial incentive programs

The results of this study reflect those reported in other studies (e.g., [17]) that users of wearable fitness devices may disclose their sensed data in order to receive financial discounts or rewards. Interviewees found financial incentive programs to be a great motive to increase physical activity. Participants reported different recipients of their data for this goal, including insurance companies, employers, and pharmacists. Incentives can be received as prizes offered by an employer, or discounts on purchases and insurance rates. Participants update the data, mainly step count, on a regular basis through an employer's portal. Others provided permissions to incentives programs to pull the pedometer data

automatically from their devices. In order to receive financial incentives, participants make sure to have their trackers on all the time to collect the data.

Two participants admitted that their primary goal for sharing was to receive financial incentives. P28 indicated that he connected his Jawbone to a pharmacy app in order to collect points based on the number of steps taken, which then can be redeemed as discounts on purchases. Similar to most of the participants, this user had no concern about sharing this type of data: *"The sharing with the pharmacy, there has been a very motivating financial affect, maybe 20 dollars every few months. It is free money, but I never been giving away something confidential. I was giving away the number of steps or my weight. There is nothing that I need to keep secret."* He repeatedly described the sharing experience on the device as a *"game"* where one tries to achieve high scores.

Another participant, P15, linked his Fitbit account to his employer health insurance portal. He considered himself healthy right now but was worried about the possibility of increasing his premium based on his fitness condition in the future.

Two other participants did not share their information for any financial incentives, but expressed a desire to share if they were offered this option:

> *"If it is something that gives me a discount, I will definitely share information with them. I probably will be more inclined to. It gives me another reason to be active to save money on my health insurance."* [P25].

#### 3.3.2.6 Co-workers

Finally, a few people identified co-workers with whom they disclosed wearable fitness information as part of participating in workplace health campaigns. Some organizations offer employees the option to link their trackers' data to the employer's website. For many of those participants, sharing with co-workers is a *"friendly competition,"* although prizes can sometimes be offered to further motivate participants. P3 stated: *"When I originally*

*started wearing it's because of the competition. You don't wanna be at the bottom of the list of your co-workers so you wanna be more active."*

However, participants find sharing fitness data with workmates as an opportunity to increase physical activity, especially because some of these participants have jobs that restrict their physical movements during the day. It can also be an opportunity to reinforce behavior change, so moving and exercising become habits rather than merely competition. Participants set daily step goals and send cheers to other co-workers who hit their step goals. To compare data with other co-workers, participants synchronize their daily step count to the employer's system. Although some of the workmates may not personally be known, sharing the number of steps walked every day was not something they were concerned about.

### 3.3.3 Sharing Impact

I asked participants about their perspectives regarding sharing and how it impacts their behaviors. Most of the participants (19/30) said that sharing their self-tracking fitness data has impacted them in a positive way. It helped participants to become more aware about their health and fitness status and encouraged them to stay competitive and accountable. Similar to Prasad et al.[60], I found that users' sharing behaviors may change over time, especially with respect to the level of information shared. For example, one participant realized that she became willing to share more data in order to motivate herself to exercise:

> *"I would like to share more because I noticed that the more that I'm sharing with people that I feel comfortable with I guess or with people that are having the same goal, the more I feel I exercise more"* [P12].

In contrast, another participant decided to share less information with the public, mainly because of privacy concerns:

> *"I actually think I share publicly a lot less than I used to because I become more concerned with privacy, but I have been sharing more information with some of my private connections"* [P18].

Five interviewees were uncertain about the impact of sharing. These participants indicated that sharing wearable fitness data has provided some benefits, such as the desire to exercise, but it did not help them to achieve desired goals. In addition, participants with mixed feelings indicated that the impact depends on the audience's reaction and feedback.

Another six participants stated that sharing did not impact their behaviors. Some of these interviewees commented that they are self-motivated, but they shared their wearable fitness data to help others and for enjoyment:

> *"I just enjoy sharing the information and posting the challenge to my followers to keep up"* [P10].

Finally, much of the recent research focused on sharing wearable fitness data on popular social networking platforms. I asked participants about the impact of this sharing on their behaviors and goals. The findings contradict those reported by Chung et al. that sharing wearable fitness information on popular social media can encourage physical movements [17]. In my study, the majority of the participants (9/14) who shared their sensed fitness data on common social network sites indicated that this sharing was not all that helpful, and some are no longer sharing on such platforms. Our participants reported several reasons that include lack of interest over time, lack of interest by audience to see this type of information, unclear impact on behaviors and goals, and privacy concerns regarding third party access to their data, especially if the data is shared on Facebook:

> *"I don't think it's impacted me that much on Facebook because it is just kind of a general, you know people post things on there and it doesn't have much of impact on me I think"* [P14].

However, the Chung et al. study was based on an existing built-in feature within a Chinese social network for sharing fitness activities. Cultural norms and expectations may explain the difference between their findings and mine. Unfortunately, I did not have the data to examine these factors.

### 3.3.4 Privacy Concerns

Finally, I explored users' concerns and perspectives regarding privacy of sharing personal and sensed data related to fitness. The overwhelming perception is that most wearable fitness information, and in particular step count, is not sensitive. Thus, few had concerns over sharing this information with any audience:

> *"I wouldn't really care if someone knew how many steps I have taken"* [P3].

> *"This is not really confidential private information. I mean in some sense it is, but it is not at the level of confidence or privacy that would make think oh I better not to share this"* [P28].

Some of the participants indicated that they would probably be concerned if the disclosed data contains identifiable information, or if the device stores financial information:

> *"If it was something from... I don't know, you have to register your ring with your address, and you have to have the credit card number in file, so something like that have my personal details that's not fitness related, then I would be concerned."* [P30].

Rather, participants' biggest concerns centered around the ability to manage their self-image and to comply with social norms of sharing. Norms complicate users' decisions to share wearable fitness information in different ways. For example, participants struggled to reconcile the desire to share with their contacts on different platforms (e.g., Facebook) and to conform to what is considered normal to share on those platforms. For instance, P18 commented about sharing his sensed data on Facebook: *"I'm not going to share my blood*

*oxygenation level with friends or in public. That would be ridiculous."* In addition, participants avoid posting too much or too detailed information in order to not bore others:

> *"My family and friends will kind of get annoyed if I keep sharing constantly"* [P5].

Other participants felt uncomfortable sharing fitness information with the different kinds of contacts they may have on social media platforms, such as professional colleagues. Others worried that friends may perceive sharing fitness achievements as a way of showing off. These concerns led participants to share less on social network sites and find other platforms for sharing with people with similar goals.

Therefore, maintaining a good self-image was important for interviewees and drove sharing decisions. Users wanted to communicate a positive image regarding their fitness life to other people. Thus, they reported being selective about the information they share, sharing positive achievements for example, rather than sharing generally and automatically. Participants also chose to not disclose information related to eating and sleeping because they think it might potentially impact how they are perceived by others.

Some participants (9/30) did express minor concerns over unintended use of their data. This concern was also reported in several prior studies of wearable tracking devices [44, 49]. For example, interviewees were concerned that their health insurance company could get access to their data in the trackers and tie their insurance premiums to their fitness status. Others were concerned that the devices' companies could pass their data to third parties (e.g., sport or drug companies) without their awareness. A few participants also identified that people or organizations could infer personal facts based upon the data shared, and were thus careful about what identifiable information was shared with strangers or organizations.

Finally, there were some concerns related to information security and physical safety. For example, four participants discussed a security breach as a potential risk, resulting in their data being used outside of their intentions. In addition, the GPS feature was a concern reported by four people, indicating that it can be exploited by stalkers:

> *"It's pretty much just the location data that bothers me the most. I don't want people knowing where I am in case there is patterns."* [P26].

I asked participants what they do to protect the privacy of their wearable health and fitness data. They reported spending little or no effort on privacy protection, beyond their choices on what and when to share information. Many of the participants were unaware of their privacy settings; and those few people who were aware about their settings had not changed them since they started to use the service. I asked the participants to go over their profiles and settings if possible, and some discovered that their platform profile was indeed viewable by the public. The remaining participants stated that they changed their controls only once, and that was when they set up the device. Despite this, many participants complained about the lack of options available in the settings to adjust the desired level of privacy.

A few participants reported other ways they protected their information. Two interviewees indicated that they disclose only basic information on their profiles– as little as possible. Another user stated that he put in fake information when he created the account. Six other participants discussed using standard security mechanisms, such as authentication. For example, P3 said: *"I have a username and a password, and I just use that in the Garmin to protect my data."*

## 3.4 Discussion & Implications

My study reveals a set of common patterns related to users' sharing goals, their chosen audience, and the resulting choices participants make to disclose and manage their sensed information. My results confirm previous findings of sharing on social media [19, 36], that users are motivated by accountability, advice, and competition when sharing sensed fitness information with other people, in pursuit of their individual fitness and health goals. Participants also reported helping and providing motivation and emotional support to others. An additional goal we have not previously seen is to track and improve health by sharing with physicians. Users expressed a willingness to share if that sharing was helping them meet their health and fitness goals, and reduced sharing if it was found to not help their goals. In other words, participants were consciously making the trade-off to share information for personal health or financial benefits.

The results also provide useful insights into users' privacy concerns and behaviors. I found that users' practices have little to do with concerns over the sensitivity of the data. Rather, my study suggests that norms and self-presentation are the two key concerns of users. Although research suggests that sharing fitness data on popular social network sites is promising to encourage physical activity (e.g., [28]), I argue that site norms can be a barrier and drive users to find other platforms. For example, users sometimes limit the information shared with their friends in order to manage the impressions of the many different contacts they have on social network sites. Many of the participants wanted to communicate a positive image about themselves by sharing only positive fitness achievements. Thus, those who were doing well with their fitness goals found social network sites as a valuable platform to share these achievements with a broad range of

friends, but those who struggled with their goals found more support on platforms where they could connect either to friends or strangers with similar goals.

Examining participants' perspectives regarding sensitivity of wearable fitness data reveals that, for the most part, this data is not perceived as sensitive. Users have a common fallacy that there is *"nothing that I need to keep secret."* This perspective toward sensed fitness data has influenced many users to pay little attention to protect their data, even leaving their device platform profiles with default or public privacy settings. Even though some of the participants gave scenarios of how their information could be misused, they felt that the risk was far-fetched. Additionally, the fact that a device company has been in the market for many years has made users trust that their data is safe. However, incidents have shown how data collected by fitness trackers is valuable to criminals [6]. Research has also demonstrated that very sensitive information can be inferred from seemingly innocuous fitness sensor data [37]. While most of the participants in my study did understand that some information could be inferred from their data, they did not express concrete examples of such sensitive information, or feel that they were very susceptible to negative consequences as a result of such inferences.

My results also suggest that financial incentives are a powerful motive for sharing, and the availability of various wearable fitness devices today has made sharing with different incentive programs (e.g., insurance companies, employers, pharmacies) much easier. This is evidenced by the considerable number of people in our study who disclosed their information to receive discounts or rewards. For a few, the incentive was the primary driver for sharing with such organizations, rather than being in support of a health or fitness goal. However, the findings suggest that concerns over secondary use of data may discourage

users from sharing with such programs long term, or as their health or fitness levels decline. Many participants commented that health insurance companies could potentially utilize fitness trackers to adjust coverage plans, although this had not happened yet.

In the light of these findings, I offer several implications for designing wearable trackers that promote sharing and privacy of fitness-related information:

**Design controls and sharing features around common goals and patterns.** As I noted, users' goals for sharing fitness information vary, and this may require sharing different levels of personal information in different ways. Yet there are a number of common practices depending on those goals, and the associated platforms used. Thus, device platforms could ease this sharing by providing designs centered around these goals and practices. For example, sharing settings could be designed to allow users to have sharing profiles with different audiences. These settings could reflect common data sharing norms, while still allowing for customization of content depending on the goals. In addition, designers should provide visualization mechanisms to help sharers focus on their goals. For example, if a user's sharing goal is to lose weight, a summary of data for this goal such as calories consumed, and distance traveled could be visualized in the interface for the intended audience.

**Methods for sharing with physicians.** Individuals who share their wearable fitness data with physicians expressed a strong desire to directly connect their self-tracking data with health providers in some way. Thus, there is currently an unmet need in how to provide full access to, and useful views of information for health providers. For example, sharing settings could be designed to enable users to provide permission to their personal medical provider to access their data using doctors email address, for example. Such support would

reduce the burden of this important sharing, facilitate conversation prior to clinical visits, and encourage long term use and tracking of sensed data in support of health goals.

**Awareness of sharing policies.** Generally speaking, users do not consider most of their wearable fitness data to be harmful to them. Yet, they also do not appear to be very aware of device manufacturer's data practices, and how they share their information [80]. Device manufacturers should present their data policies to users on a regular basis (e.g., semiannually), remind users about their choices, and even explain the possible risks to enhance users' awareness. Wearable fitness companies can share users' data with different external parties, such as drug and sport companies. Yet few of my study participants expressed concerns over this potential and how data may be shared without their explicit interaction. And while some users acknowledged the possibility of data inference, few expressed any concerns beyond the use of locational data. Additional research is needed to determine what organizational data practices most concern users, and how to increase the awareness over such practices.

**Privacy Nudges.** Many of my study participants discussed how their sharing and perceptions had changed over time, as other studies have also pointed out [25, 60]. Thus, designers should seek solutions that are easy to modify over time. Users should be provided with opportunities to reflect on the audiences for their sharing, and how their sharing has changed. For example, as with other forms of social media sharing, nudges could prompt users to reflect on their audience as they share [81]. Nudges could also be designed to remind users of how their information is being shared, and revisit controls over time.

## 3.5 Summary

In this chapter, I conducted qualitative interviews, investigating the sharing goals, practices, and privacy behaviors of 30 users of wearable fitness devices. The findings reveal that decisions to disclose information to other people and organizations are primarily influenced by the goals people have when sharing with different audiences, and how well different device and sharing platforms can support those goals. My results highlight the need for more privacy and sharing features centered around these patterns and the sharing norms on various platforms, to support users in their ultimate goals of improving and maintaining their health and fitness.

# CHAPTER 4: USERS' PERCEPTIONS AND ATTITUDES TOWARDS INFERENCES IN WEARABLE FITNESS TRACKERS

The findings in chapter 3 highlighted a common concern many participants have, which is the possibility of inferring private information from the data collected by their wearable fitness devices. Therefore, this chapter examines people's perceptions and attitudes regarding the information that can be derived from the data collected by a device or shared by users, and how these perceptions and attitudes might influence users' decisions to share their information with different recipients.

## 4.1 Motivations

Depending on the sensors available, a variety of data can be collected by wearable sensor devices, such as step count, sleep quality, average heart rate, location data, etc. The pervasive and often invisible collection of data by these sensor devices and the sharing of it impose privacy concerns. One of these concerns is the possibility of inferring information from the primary data collected by devices or that shared by users. For example, in January 2018, reports revealed that fitness tracker data shared by users on Strava, a social fitness service, showed accurate locations of U.S. military sites [31]. In another example, a person sought help from a Reddit community regarding an abnormal elevated heart rate showed by his wife's Fitbit [33]. He assumed that the device was not functioning properly but discovered from people's comments that his wife could be pregnant, and she actually was.

So far, research has investigated people's awareness and attitudes regarding the information that can be inferred from fitness tracker data [7, 65, 70]. Users seemed unconcerned about the risks associated with the use of fitness trackers [7]. However, studies have shown that primary data collected by wearable sensor devices can be used to

infer highly private information, such as frequently visited places [48], stress level [38], and sexual activity [45]. Users can be unaware of the potential inferences resulting from the collection and sharing of fitness tracker data, as there are limited application features that can inform users' mental models [65].

A less explored issue, however, is how users' understanding about inferences in the context of fitness trackers influences their sharing decisions. In this chapter, I aim to expand upon prior work by investigating the perspective of both sharers and non-sharers of wearable fitness data regarding the information that can be derived by other individuals, device manufacturers, and third parties. I conducted semi-structured interviews and an online survey with users of wearable fitness devices. In both studies, I presented participants with several concrete inference scenarios to examine their perceptions and comfort with a range of derived information and uses of that information. I also explored users' comfort with sharing different types of data collected and inferred by fitness trackers with a number of different recipients. My main findings include:

- Additional evidence that users of fitness trackers lack awareness that personal information can be derived from the primary data their devices capture and share. Users are not considering the potential for inferences in disclosing fitness tracker data.
- Users are less comfortable sharing derived information than primary information with all kinds of recipients.
- Identification of factors related to users' perceptions of inferences, including notice and consent, likelihood and trade-offs of risk, accuracy and anonymity of data, and trust.

The findings demonstrate the need for additional awareness mechanisms to enable users to understand what other information could be derived from their data, and thus to help them in protecting their information.

## 4.2 Methodology

I utilized mixed methods (interviews and an online survey) to examine users' perceptions and comfort regarding inferences. Each method is described in detail below. I chose to recruit current and former users of wearable fitness trackers, as well as those who both do and do not share their data with others, in order to understand if inferences influence their use and sharing decisions. The interview participants were recruited in August and September 2019. I recruited the survey participants in February 2020 using Amazon Mechanical Turk (MTurk), and the survey was hosted on Qualtrics. In total, the study has 23 interview participants and 159 survey respondents. The study methods and materials were approved by our UNC Charlotte IRB.

### 4.2.1 Semi-Structured Interviews

I interviewed a total of 23 users of various wearable devices that collect fitness data (Table 3). I recruited the interview participants by advertising the study in relevant Reddit communities. I contacted the participants through email to schedule a phone interview. This method of recruitment allowed me to access English-speaking participants from diverse geographical locations. The interview participants live in the United States (17), the United Kingdom (2), Argentina (1), Australia (1), Belgium (1), and Canada (1). The interview duration lasted between 17 and 40 minutes. Each participant received a $10 gift card after completing the interview.

The interview began by asking the participants behavioral questions, such as what data participants think is collected by their devices, who can access it, and what concerns they have about their information. The main part of the interview focused on the information that can be inferred about the participants based on their fitness tracker data. I then provided the participants with seven brief hypothetical scenarios to examine their comfort sharing their information if inferences could be made about them by the device companies or other individuals and parties. I asked the participants what information they think can be inferred about them in each scenario, and how comfortable they would be if that information was inferred. This was followed by questions that prompted participants to think about the risk, and how the information can be inferred in each given scenario. In the last part of each interview, I asked the participants how they protect their information against possible inferences, and what features they would like their devices to have in order to help them in managing their privacy. The full set of interview questions is included in appendix D.

I utilized scenarios to elicit users' comfort and attitudes, similar to other studies about privacy preferences and data collection awareness, such as for online services [14] and IoT [20, 65]. I designed the scenarios based on potential inferences described in previous related work [59]. Users' sharing comfort is dependent on who receives the data [9, 23], and so I assume that this might also be true for inferred information. Thus, I designed the study scenarios to investigate users' comfort regarding sharing primary data with different individual and parties if potential inferences can be made from such data (see Table 4).

I audio recorded and then transcribed all the interviews. Two coders analyzed the transcripts using qualitative data analysis software and an inductive coding approach. First, the two coders independently and iteratively coded three transcripts to identify common

themes. The coders then compared and merged their themes into a master codebook. The resulting master codebook consisted of 32 codes that were conceptually grouped into three categories: use and sharing, inferences, and recipients. The remaining interview transcripts were coded by the two coders using the master codebook. The coders kept track of their disagreements and the calculated inter-rater agreement was 81.25%. The coders then discussed and resolved their disagreements.

### 4.2.2 Online Survey

I recruited people who are English speakers, aged 18 or older, current or former users of wearable fitness trackers, and had at least a 98% HIT approval rate on MTurk. I first conducted a pilot test of our survey questions with 5 users to ensure the appropriateness of wording and to estimate the duration to complete the survey. The final survey consisted of 45 questions (the complete survey questions are provided in appendix E). Of the 206 participants who answered a pre-screening question, 159 (104 M & 55 F) met the participation criteria. The participants spent, on average, 10 minutes to complete the survey and received $1.50 USD.

The first part of the survey collected information about fitness tracker use and sharing by our participants. I first asked the participants to select all the wearable fitness trackers they used, to identify if they shared their information with other individuals or parties, and to indicate their goals for sharing fitness tracker information. I also asked the respondents about their knowledge of device manufacturer data practices by asking them to rate their confidence in their knowledge on a scale from 1 to 5. To examine the participants' attitudes about inferences, I first provided them a list of ten recipients and asked about their comfort with sharing different types of primary data (e.g., step count and heart rate), which is

collected by common wearable devices. The recipients included both other people, such as friends and acquaintances, as well as organizations, such as insurance companies and workplaces. I then presented our respondents with six short statements where personal information might be inferred or predicted from the primary data that was already provided (e.g., stress level, as suggested by heart rate data) and asked them to specify their sharing preferences with the same group of recipients. This allowed me to also explore users' sharing preferences of different fitness tracker data with different audiences. I further examined participants' attitudes about inferences by asking them to choose "likely", "unlikely", or "not sure" that a given scenario would happen. At the end of the survey, the participants responded to demographic questions (age, gender, major education level, technical skills, and ethnic group).

With respect to the quantitative analysis, the results are mainly descriptive statistics and graphical representations of the responses, which I used to draw a conclusion about the participants' knowledge and comfort regarding inferences. However, I performed an inferential statistic using McNemar's and Cocheran's Q tests (the latter for a comparison involving three types of information) to compare participants' comfort with sharing primary data and inferred information with multiple groups of recipients. I found many statistically significant results in participants' comfort levels based on the type of recipient and inferred information.

## 4.3 Results

I first report the results of the interview study, discussing participants' perceptions towards inferences. I then describe the survey results which detail the sharing preferences for both primary and inferred information. Note that any numbers reported in the interview

results are merely to reflect prevalence of themes in our sample. I use the following words in characterizing the results: a few (2-4), some (5-10), many (11-18), and most (19-22).

### 4.3.1 Interview Results

#### 4.3.1.1 Participant profiles

I interviewed 23 users of wearable fitness devices (13 M & 10 F) with an average age of 33 years old (ranging from 18 to 52 years old). The participants are well educated; all the participants except two attended a university and have a degree. The interviewees utilized a wide range of devices for tracking health and fitness, most commonly the Apple Watch, followed by Fitbit (Table 3). Many of these devices enable users to track a variety of sensor-based data, including movement data, vital signs, and location. Most of the devices used by our participants are also paired with that device's mobile app or web service that provides users with a variety of tracking features and allows them to share their data with others. Eight participants reported using more than one device currently or in the past in order to take advantage of desired or new features. For example, P3 uses a Garmin and an Apple Watch and switches between them in order to access the running analytics offered by the Garmin and the smart options of the Apple Watch.

The participants mentioned several goals for using fitness trackers, such as tracking exercise, losing weight, and optimizing health. Many participants also reported connecting their device data to external platforms, such as Strava, mainly to access metrics or features not offered by their devices. In addition, a few participants utilized fitness trackers for other reasons that include tracking sleep and monitoring medical conditions.

Table 3: Interview: Participants Information

| ID | Gender | Age | Device(s) | Shared with |
|---|---|---|---|---|
| P1 | F | 30 | Apple Watch | Friends |
| P2 | F | 20 | Fitbit | |
| P3 | M | 51 | Garmin; Apple Watch | Friends; Strava |
| P4 | F | 37 | Fitbit | |
| P5 | M | 18 | Apple Watch; Fitbit | Family members |
| P6 | F | 35 | Fitbit | Friends |
| P7 | M | 23 | Apple Watch; Android Smart Watch | |
| P8 | M | 24 | Apple Watch | Friends |
| P9 | M | 29 | Apple Watch; Fitbit; Samsung Watch | Friends; significant other; online fitness communities; |
| P10 | M | 40 | Garmin | Friends; Acquaintances; Strava; MyFitnessPal |
| P11 | M | 40 | Apple Watch | |
| P12 | M | 29 | Xiaomi Mi Band | Friends; significant other |
| P13 | M | 50 | Apple Watch; Fitbit; Garmin | MyFitnessPal |
| P14 | F | 48 | Fitbit | Significant other; Weight Watchers |
| P15 | F | 36 | Apple Watch | Significant other; MyFitnessPal |
| P16 | M | 23 | Polar Watch; Oura Ring | |
| P17 | M | 19 | Apple Watch | Close friends; health provider |
| P18 | M | 52 | Polar Watch | Friends; Strava |
| P19 | F | 34 | Samsung Galaxy Watch; Fitbit | Weight Watchers; MyFitnessPal; Strava; MapMyRun; Pharmacy |
| P20 | M | 27 | Apple Watch | Friends; Family members; Reddit fitness communities |
| P21 | F | 35 | Polar Watch | |
| P22 | F | 31 | Apple Watch; Garmin; Fitbit | Family members; Strava |
| P23 | F | 29 | Apple Watch | Strava; Nike Run Club |

#### 4.3.1.2 Primary data

In order to gain insight into our participants' perceptions and attitudes about inferences, I first prompted them to think about the information their fitness trackers are collecting. The participants described a wide variety of data that is collected by their trackers, which indicates that they seemed to have a good understanding about the data collection capabilities of their devices.

I also asked the interview participants if they ever shared their fitness tracker data, why they shared it, and with whom. The majority (n= 17) of the participants said that they shared their fitness tracker data. Friends were the most common reported audience, where goals include competition, motivation, and fun. Seven people indicated that they shared with

significant others or family members for mutual encouragement towards health and fitness goals. Understandably, those participants reported sharing information openly with family members and loved ones. The participants also disclosed their data on external health and wellness platforms, such as Strava and MyFitnessPal, where they mostly connect with strangers. Other recipients that were mentioned are healthcare providers (for continuous tracking of abnormal changes in vital signs) and a pharmacy (to earn points based on activity level for a discount).

Six participants did not share their fitness tracker data with any individuals or companies (beyond the device manufacturer). One participant considered this information personal, and thus did not want to disclose it to others. The remaining ones indicated that sharing their data was either not valuable or did not occur to them.

I also asked interviewees about their concerns with sharing primary data, particularly step count, sleep patterns, and heart rate. Similar to prior studies [9], more than half of the interview participants were not concerned about fitness tracker data because they did not consider it risky. For instance, one participant said: *"It doesn't bother me because I'm not a professional athlete, but if I was a professional athlete, it maybe devoting more information to my competitors."* [P10].

In contrast, five participants did express discomfort, indicating that while their information is not identifiable, it is personal, and no one has the right to access it. Thus, they only shared with people known to them in real-life. Four people were concerned about adjusting insurance premiums; one of them mentioned that heart rate specifically can reveal potential information about a person's health. A few participants said they were primarily concerned about location information, mainly because it may compromise their physical

safety. For example, P17 indicated that he is worried about sharing fitness data that also shows location information: *"I would be fine with sharing the amount of steps that I've taken a day with a broad variety of people, but I wouldn't like people to know where those steps were taken. Same with sleep where it occurred, heart rate like when and where."*

In summary, the participants' perceptions of fitness tracker information reflect findings in prior studies [9, 49, 92]. While there are a few concerns about location information and negative consequences from insurance companies, the participants did not consider most information risky to share, and did so based on their personal health or fitness goals.

#### 4.3.1.3 Inference Perceptions and Attitudes

I then turned to perceptions of information inferred from their primary data. I first asked the participants what information they believed could be inferred. My interviewees believed that inferences are possible, but many of them were uncertain about what can be inferred and how. Several were aware of widely reported incidents; for example, P7 indicated: *"I remember when some soldiers where they were recording their training runs on Strava and because of their unique positions in the world, it was very easy to track and identify who they are even that was uploaded anonymously."* One participant (P16) distinguished between individuals and companies (e.g., device manufacturers) in their ability to make inferences. Unlike companies, this participant believed that people are unlikely to be able to infer his information because he can control the sharing of it with other people. Three other participants showed advanced understanding by pointing out that information can be aggregated from multiple sources, which increases the chance of predicting precise information:

> *"I use a variation on my date of birth just to not make it easy if any one of those services leaks information so I can't easily be linked from cross-*

> *tabulation to other services, and that's something I've always done since the 90s. I was always cautious about leaking my identity"* [P18].

To more deeply investigate users' comfort with inferences, I then provided our participants with seven scenarios (Table 4), each with different levels of sensitivity that implicitly or explicitly suggest certain information could be inferred from their fitness tracker data. The first four scenarios examine users' comfort when inferences can be made by a device or third parties, such as insurance companies and employers. The last three scenarios explore users' comfort regarding potential inferences made by other people. Many people were uncomfortable sharing their information across all the scenarios presented. Yet, the participants' reactions suggest that they took into considerations the purpose of the sharing, the recipients, and the anticipated risks of the information. Thus, I will first discuss specific reactions to each scenario before describing more general themes.

**Scenario 1— Background screening.** The participants indicated that they never heard of such data being used for background screening, and most of them were uncomfortable sharing with insurance companies, employers, and banks because they believed that the data would mostly be used by these parties in a negative way (e.g., insurance rate increase, promotion discrimination, or loan application rejection). However, a considerable number of the participants (n=10) said that they will be less uncomfortable if there are perceived benefits. For instance, P19 stated in response to this scenario: *"I wouldn't necessarily be concerned if I was going to be rewarded for good behavior. So, if I'm doing well and I would say get a discount because I'm sharing and doing good, then yes, I would be more than willing to share information."* However, the participants demanded detailed information, which may suggest a lack of trust about the purpose of sharing their information with the given recipients.

**Scenario 2— Sexual activity.** I expected to find a large number of people uncomfortable with the second scenario due to the sensitivity of the inferred information. Surprisingly, a considerable number of participants (n= 9) seemed indifferent and considered recording sexual activity as another interesting metric to track. Many participants also said that they would not mind their device inferring this information if it is anonymized. For instance, P5 stated: *"If it's only stored and seen by me, then I wouldn't have a problem with it. If it was anything that got to like the people in my family whom I'm okay with sharing other information, I definitely don't think that something I would be comfortable with."*

However, another participant (P15) pointed out that she did not even want the device to store a record of her sexual data because it will be embarrassing if the device gets hacked and the information was leaked.

Table 4:Scenarios on Inferences

| Level | Summary |
|---|---|
| **Device & Third parties** | **1#** Your device company shares your data with a background screening company who offers background check for different parties including employers, insurers, and banks. |
| | **2#** Your wearable device records a history of your sexual activity. |
| | **3#** A health insurance company classified you as overweight based on your wearable fitness data. |
| | **4#** Your employer uses your device data to predict your mood (e.g., if you are stressed). |
| **Socially** | **5#** You joined a fitness group where all members share fitness data collected by their trackers with each other, and some members are not personally known to you. |
| | **6#** Your friend asked you to share your activity data collected by your device with all friends on one of your social media accounts (e.g., Facebook). |
| | **7#** Strangers infer your social connections based on fitness tracker data you share over the app. |

**Scenario 3— Health insurance.** The third scenario presents a clear threat to the participants, with an insurance company classifying someone as overweight. However, a common response by the participants is that they would probably not mind if a notice about using their data for that purpose is provided in advance, and they optionally agreed to it.

Some participants also said that they would not be uncomfortable sharing their information if they are actually overweight.

**Scenario 4—Employer predicting mood.** With respect to an employer being able to infer mood, all the participants, except two, were extremely uncomfortable. They considered this an invasion of their personal privacy because they could be judged in their workplace based on irrelevant information. Many participants felt that if employers request this type of information, they will always use it to harm employees. One participant indicated: *"I would not like that at all because I think that it's a private thing that shouldn't affect your work life. So, I don't think it's any of their business to have that information."* [P22].

**Scenario 5— Online fitness group.** This scenario elicits participants' comfort regarding potential inferences made by other people, in particular if the information is shared with strangers. Overall, the participants were more comfortable with this scenario than any other scenario, because they anticipated value from sharing their information. For example, P7 pointed out that sharing fitness data with other people has helped him to move from being obese to normal weight. The participants were also comfortable since the sharing in this scenario is reciprocal. A few people noted that their decision will also depend on the type of data being requested, indicating that they would be comfortable disclosing fitness data they deemed insensitive. On the other hand, the few who were not comfortable did not want to share with strangers or did not want to be judged by others. Thus, they were expressing some concerns as to what other people would think about them based on their information.

**Scenario 6— Social media.** The sixth scenario aims to capture users' sharing comfort of fitness tracker data socially with people they know, but the participants also discussed sharing with a third party (e.g., Facebook). The participants showed a slight discomfort with this scenario for two reasons. First, participants expressed a general distrust of social media, such as Facebook, because they consider these platforms *"wide open,"* and thus their information can be subject to various risks, such as data leakage and targeted ads. For example, P18, an active user of Twitter, stated that he would create a secondary account with a new username if he decided to share his fitness information there to keep his real identity from being linked with his information. Secondly, the participants felt that social media platforms are not the right place to share fitness data.

**Scenario 7— Social connections.** Lastly, I examined users' comfort if their social connections (friends) were inferred. Overall, the participants were uncomfortable if strangers infer their social connections because that would then expose their connections to privacy risks. The participants struggled to figure out how this information can be inferred from their fitness tracker data. Many participants said that this information might be inferred through GPS data, and a few others mentioned through linked third-party apps.

#### 4.3.1.4 Emerging Factors

The interview participants' reactions to the given scenarios highlight four main considerations regarding inferences:

**Likelihood of a risk—** While participants provided examples of the potential threats for each given scenario, some of them believed that certain risks are less likely to happen. One participant explained: *"I haven't heard of data being used in that way, but if it's used in that way then definitely I would have to re-evaluate it"* [P23]. Another participant (P12)

said that some risks are possible but will not occur in the near future. However, many participants initially considered the data collected by fitness trackers insignificant, but changed their opinions after discussing the scenarios, indicating that many scenarios were credible.

**Notice and consent—** Eleven participants brought up in the discussion of scenarios 3 and 4 a notice and consent protocol as a factor that would make them more comfortable with sharing their information with insurance companies and workplaces. Our survey results also indicate the importance of this, particularly for third parties.

To ensure that their information will not be used against them, participants demanded a clear and full explanation of data usage. For example, P8 stated: *"I would always ask how the company [a health insurance company] gets my data and if I authorize data how they use it, where it goes, and how it is stored."* In addition, participants indicated that they wanted to be able to opt out, partially or completely, without storing their information after they opted out.

**Accuracy of data—** Eight participants stated that the data recorded by wearable fitness devices can be inaccurate. Even if the sensed data was accurate, those participants indicated that there can be different causes for certain measurements. For example, P9 commented about the ability of a device to record sexual activity: *"It wouldn't know if your heart rate goes up for a workout, if your heart rate goes up because you're sleeping and you have a nightmare, you're watching a movie or something like that, even if you have drugs, there's no way to say why your heart rate went up, so it would be a lot more difficult to determine if you had sexual activity versus if you didn't."*

The participants had two views related to accuracy. First, because they believed the inferred information would not be reliable, it would not likely be used by insurance companies or employers, for example. Second, accuracy also raises a concern that someone might be unfairly judged based on incorrect data.

**Benefit-risk tradeoff—** The results are in line with much privacy research that disclosure decisions are impacted by the perceived benefits [9, 14]. Ten of the interview participants indicated in response to some of the scenarios that they may be willing to share their information if there is a value. For some of them, they indicated that the obtained benefits from sharing their information outweigh the potential risk. In addition, the participants felt that they have limited control, but they *"have to give something to get something back."*

**Anonymization—** The findings provide evidence of the interplay between people's comfort and anonymization in the context of fitness tracker data sharing. The expectation that information is anonymized when shared with the device or third parties was mentioned by nine of our participants, indicating that they will be uncomfortable and most likely will not share their information in certain scenarios if the information is connected with their real identity.

**Trust—** This factor was mentioned by six participants in relation to their comfort with potential inferences. Our findings suggest that high-level trust can decrease privacy concerns and vice versa. For example, three participants (P8, P13, & P17), who are Apple Watch users, were comfortable about certain scenarios because, according to them, Apple will not jeopardize its reputation by abusing users' data:

> *"With Apple overall as a company with many instances over the years, especially toward encryption, that does alleviate some of those initial lack*

> *of trust that would be with other companies, lets' say [some fitness tracker company], for in- stance, doesn't necessarily have that record of fighting to keep the keys to the kingdom locked up and not pass it over"* [P13].

In contrast, three other interview participants were uncomfortable sharing their information, noting that they generally disbelieve companies regarding their data practices. One participant mentioned that she had grown more concerned over time with the data practices of fitness trackers:*" I have been using fitness trackers since I was young, so I didn't really think about it when I first got it, but I only recently have had more privacy concerns. The news shares not only data breaches, but also in general how companies use the data and data mining to establish profiles on their users"* [P2].

#### 4.3.1.5 Mitigation and Potential Solutions

In the last part of each interview, I asked the participants about the steps, if any, they took to prevent inferences. The participants also brainstormed some solutions to help them control these inferences.

More than half of the participants (n=14) reported undertaking a range of traditional practices, both actively and passively, to protect their information. These practices include limiting the sharing of information to trusted connections or limited disclosures to basic non-identifiable information both to people and to the device. Other participants reported changing the default settings, turning of some sharing options or hiding certain information:

> *"I still have my home address covered by a privacy zone which is a bit crazy actually because everyone that I share with already knows where I live. . . For someone like me, I will get through and think about each and every one of those. Most people will probably just stick with the defaults."* [P10].

Four people reported reading through the terms and conditions in advance to examine what data the device and the apps that are connected to it are requesting, and then consented

to only share information that was necessary. Four other participants mentioned security mechanisms, such as strong passwords and two-factor authentication.

In contrast, some of the interviewees said that they did not take any protective measures. The reasons for the lack of actions are the initial perspective by the interview participants that the data collected by fitness trackers is insensitive or harmless. The reasons also include some of the themes we just described— the belief that a threat is unlikely to occur and the expectation that the information is anonymized. In addition, some participants indicated that they trust that the device manufacturer will not abuse their data.

The interviewees brainstormed potential solutions. A number of participants (n= 7) expressed their willingness for a mechanism to process data locally instead of remotely on the manufacturer server. This will help them to be in control over their information and their concerns about undesirable data leakage will be mitigated. Five participants suggested up-to-date encryption to secure their data when it is synchronized with the mobile phone or transmitted to the server over untrusted networks; two of those participants stated that they are unaware if the device actually encrypts their data. Lastly, six participants proposed flexible controls to enable them to specify their sharing preferences:

> *"I remember when we got our mortgages on our house, when we find everything. You can check these boxes to limit sharing with companies and limit sharing with third party companies. So, I guess if there was some way within the app that you could check like boxes to show what you're comfortable sharing or not sharing"* [P15].

#### 4.3.1.6 Summary

To sum up, the interview findings suggest that users lack awareness about the personal details that can be derived from the data collected by wearable fitness devices. Users also questioned the likelihood and accuracy of some of the inference scenarios we presented.

Still, many expressed greater concern over the sharing and use of their fitness tracker information after discussing the scenarios.

### 4.3.2 Survey Results

The survey aimed to further examine my conclusion from the interview results that users lack knowledge regarding inferences made from fitness tracker data, and to more thoroughly investigate their comfort with sharing data with many different groups of recipients. I first provide an overview of the survey participants before moving into details of their knowledge and comfort with sharing fitness tracker information.

#### 4.3.2.1 Participants

The Mechanical Turk sample consisted of 65.4% males and 34.6% females. Their ages ranged from 19-64 years old with an average of 33.5 (SD = 8.1). In terms of education, 71.7% had a bachelor's degree or attended some college, 20.1% held a master or a doctoral degree, and 8.2% had not attended college. Participants utilized a variety of wearable devices for tracking fitness (summarized in Table 5).

Less than half of the survey respondents (47%) reported sharing their information with other individuals and only 30% shared it with companies and third parties. Of those who did share their information with people, 68% shared with friends, 35% with family and significant others, and 11% with a gym group, online fitness group, or work group. The respondents who stated that they shared their information with companies and third parties connected their data with an external wellness app (46%), a health insurance company (25%), or health provider (6%). Similar to the interview, the survey participants shared their information mainly to stay fit and accountable toward their fitness goals, track medical conditions, or receive incentives based on activity level.

Table 5: Devices Used by Survey Participants

| Fitness Tracker Band | # | % |
|---|---|---|
| Fitbit | 89 | 32% |
| Apple Watch | 76 | 27% |
| Polar | 12 | 4% |
| Misfit | 8 | 3% |
| Garmin | 14 | 5% |
| Samsung | 44 | 16% |
| Xiaomi | 20 | 7% |
| Nokia | 14 | 5% |
| Other | 4 | 1% |

#### 4.3.2.2 Knowledge of Data Practices

As part of understanding users' knowledge regarding inferences, I first asked them to rate their level of confidence on a scale from 1 to 5, where 1 means "not at all confident" and 5 means "very confident", about: how their fitness tracker collects data; and how the data is used and stored. As shown in Figure 2, the respondents had higher confidence in their knowledge of how their data is collected than in their knowledge of how it is used and stored. In a subsequent survey question, I asked the respondents if they ever read their fitness tracker company's privacy policy and terms of service, and 58% of them said that they did not or were unsure.

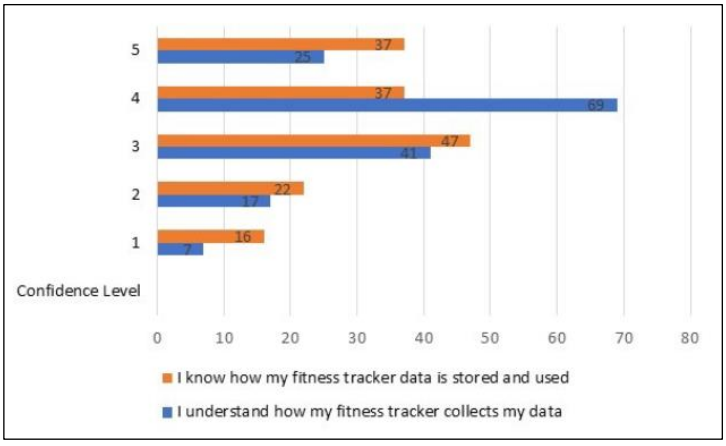



Figure 2: Participants' Knowledge Regarding Data Practices

#### 4.3.2.3 Sharing Comfort with Recipients

I presented the participants with a list of primary data (name; birthdate; height; weight; step count; sleep; heart rate; calorie intake; friends list, fitness challenges, distance/miles; exercise route) that most common fitness trackers collect. I asked the participants to select the recipients that they would be comfortable sharing that data with. I then asked questions about comfort with those same audiences if information is inferred from that primary data.

**Primary data—** Overall, the respondents were more comfortable sharing their data with family members and friends, followed by significant others and health providers. Respondents were least comfortable sharing with third parties, and most data with workplace connections. Across all kinds of recipients, respondents were more comfortable sharing step count, and less comfortable sharing their friends list. In addition, the sharing comfort with health providers increases with data that has health connotations, such as heart rate and height/weight. These patterns are similar to those found in other studies on fitness trackers [9, 23].

**Inferences based on primary data—** I then presented the participants with the following six statements where information can be inferred based on some of the primary data, and the participants were asked to choose all the recipients that they would be comfortable sharing with:

- Body Mass Index (BMI), as calculated based on the weight and height.
- A record of sexual activity, as calculated by the heart rate and movement data.
- Home location, as suggested by an exercise map/route.
- Stress level, as suggested by the heart rate data.
- A sedentary lifestyle, as suggested by the average step count.

- Personal connections, as shown by the user competition in fitness challenges.

For most information, patterns are similar to the primary data. Respondents were most comfortable sharing with family members and friends, followed by significant others and health providers. Third parties were chosen least often, especially for location information (2%).

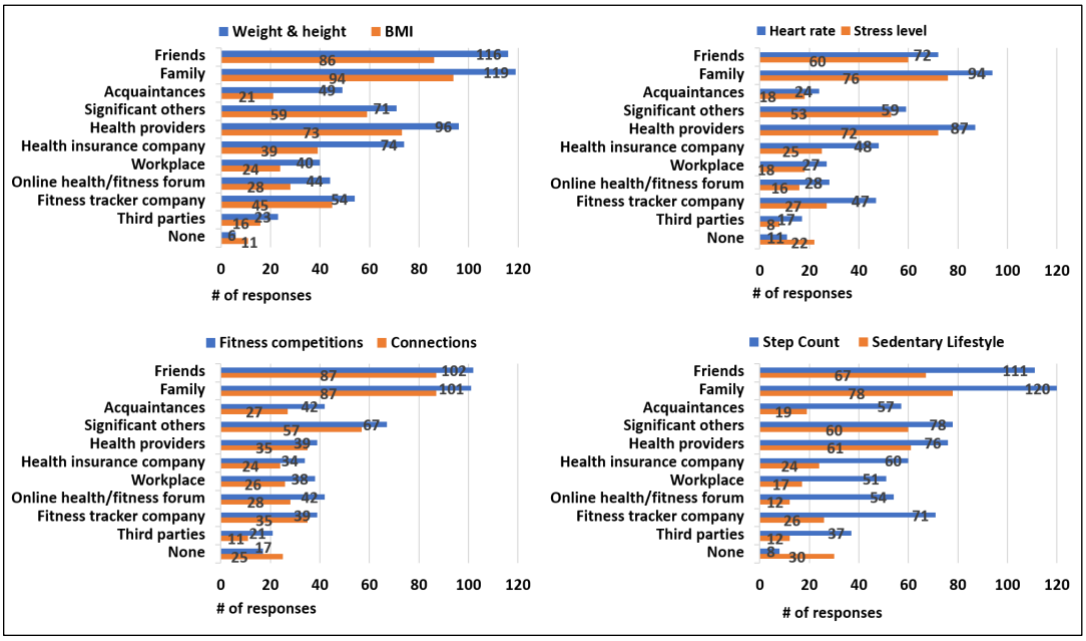



Figure 3:Users' Comfort with Sharing Primary Data vs. Derived Information

Figure 3 shows a comparison between the percentage of respondents who were comfortable with sharing primary data and the related inferred information (also see the appendix). Across all scenarios and audiences (except for "none"), fewer respondents are comfortable sharing derived information than primary. This suggests that at least some of the participants were not considering the potential for these inferences in their initial comfort responses.

I also conducted a series of McNemar's tests, as well as Cocheran's Q tests for sexual activity, to find out if there are statistical differences (i.e., $p < .05$) regarding users' comfort

with sharing primary data versus inferred information with the same group of recipients. The results show significant differences across most audiences in each scenario, with a few exceptions. As Table 6 shows, only the sexual activity scenario revealed significant differences across all the recipients. Respondents were also significantly uncomfortable sharing all information with strangers on online fitness communities. As might be expected, there are not many statistical differences in terms of respondents' comfort sharing with significant others.

Table 6: Stat. Dif. of Primary Data Vs. Inferred Information (Sig. p-values are bolded)

| | BMI | Sexual activity | Home location | Stress level | Sed. lifestyle | Connections |
|---|---|---|---|---|---|---|
| **Friends** | ***P*<0.001** | ***P*<0.001** | ***P*=0.015** | *P*=0.074 | ***P*<0.001** | ***P*=0.018** |
| **Family** | ***P*<0.001** | ***P*<0.001** | *P*=0.268 | ***P*=0.007** | ***P*<0.001** | ***P*=0.035** |
| **Acquaintances** | ***P*<0.001** | ***P*<0.001** | ***P*=0.009** | *P*=0.263 | ***P*<0.001** | ***P*=0.009** |
| **Significant others** | *P*<0.074 | ***P*=0.034** | ***P*=1.000** | *P*=0.429 | ***P*=0.010** | *P*=0.112 |
| **Health providers** | ***P*=0.002** | ***P*<0.001** | *P*=0.532 | ***P*=0.041** | *P*=0.064 | *P*=0.511 |
| **Health insurers** | ***P*<0.001** | ***P*<0.001** | *P*=0.719 | ***P*<0.001** | ***P*<0.001** | *P*=0.064 |
| **Workplace** | ***P*=0.021** | ***P*<0.001** | *P*=0.556 | *P*=0.124 | ***P*<0.001** | ***P*=0.038** |
| **Online fitness forum** | ***P*=0.012** | ***P*<0.001** | ***P*=0.003** | ***P*=0.023** | ***P*<0.001** | ***P*=0.026** |
| **Device Company** | *P*=0.137 | ***P*<0.001** | ***P*<0.001** | ***P*=0.001** | ***P*<0.001** | *P*=0.556 |
| **Third party** | *P*=0.092 | ***P*<0.001** | ***P*<0.001** | ***P*=0.006** | ***P*<0.001** | ***P*=0.006** |

I further investigated our respondents' perceptions regarding the likelihood that the six scenarios described would occur. The participants are asked to select "likely", "unlikely", or "unsure" in response to each scenario. As can be seen in Figure 4, users thought BMI and lifestyle inferences were most likely, with 82% and 84% respectively. In contrast, only about half of the respondents (53%) thought it was likely that a device can record sexual activity based on heart rate and movement data. Similar to the interview participants, the respondents were "unsure" whether personal connections can be inferred based on competition in fitness challenges.

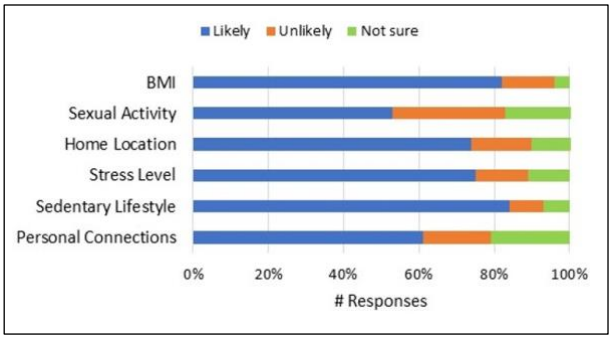



Figure 4: Likelihood That Each of The Six Scenarios Can Occur.

Lastly, the interview findings revealed that users' acceptance of inferences are also dependent on certain factors. Thus, I examined how important some of these potential factors are for users in the presented scenarios. I asked participants to select from a five-point Likert Scale (1 means "not at all important" and 5 is "extremely important") the level of importance of control, anonymization, benefits received, and notice/consent to their comfort sharing information in each scenario. Figure 5 shows a heatmap of the most important factors for respondents. As shown, anonymization is the most important aspect for some sensitive data, such as sexual activity, to be shared. The availability of controls as well as notice and consent are the two most important factors for participants in most scenarios, and the perceived benefit is the least important one.

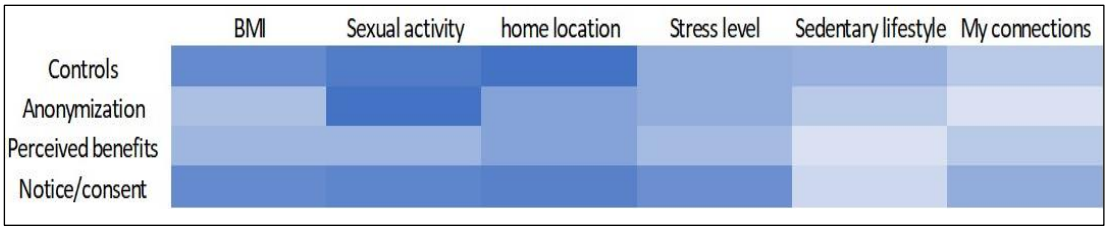



Figure 5: Importance of Specific Factors Based on Inferred Information

## 4.4 Limitations

As with many interview and survey studies, the sample is not representative of the broader population of fitness tracker users. I attempted to recruit participants from diverse age, gender, education, and technical backgrounds. However, 95.6% of the survey respondents were between 19 and 49 years old, and thus the perceptions of older users might be neglected. The survey sample also skewed toward male participants (65.4%). In addition, interview participants are on average more educated. Lastly, my study collects self-reported data, and thus may not necessarily be accurate.

## 4.5 Discussion and Implications

The overarching finding of this study is that users are less comfortable sharing personal details that can be inferred from the primary data collected by fitness trackers than they are with the primary data. This was demonstrated by comparing the interview participants' pre-and post-reactions to different scenarios, as well as by comparing the survey participants' comfort with sharing primary data versus information inferred from that data with the same recipients. Given the discrepancy between sharing primary vs. inferred information, the results also continue to suggest a lack of awareness of the potential for inferences.

Many participants were comfortable sharing a variety of fitness tracker data with other people and organizations. However, interview participants' opinions changed after I presented them with different scenarios— they were, in general, less willing to share their information after considering the information that could be inferred. Similarly, comfort sharing derived information in the survey was reduced for all kinds of data and recipients. This suggests that users are not thinking about inferences when considering their comfort

in sharing their information. The interview study fills the gap of previous related research by identifying themes elicited from participants that explain users' comfort with inferences in the IoT and fitness tracking domain.

### 4.5.1 Reasons for lack of awareness

While I did not ask participants directly about why they may lack awareness, the data provides several indications. First, the lack of awareness about inferences can partially be attributed to the limited knowledge about wearable device company data practices, understandably because privacy policies that describe these practices are generally not usable. As the survey results show, more than half of the respondents were unaware of their fitness tracker's privacy policy. Furthermore, prior research has shown that there is generally a mismatch between what fitness tracker companies address through their policies and what users need to know about companies' data practices [58].

In addition, most of the interview participants indicated that they had not experienced any risks from sharing their fitness tracker data, and thus they felt unthreatened— a mental bias known as "optimistic bias." While a few people recalled well-publicized previous incidents, such as Strava's leakage of location information [31], none provided examples of incidents related to other common types of information. For example, Fitbit was in the news years ago when details of sexual activity were inferred from information found on Google searches [68]. Yet, participants seemed unaware of the possibility of such an inference. In both studies, participants expressed doubts of the likelihood of the various scenarios, which aligns with Gabriele and Chiasson's study results that users found many potential threat scenarios unlikely [23].

Users were quite aware of the primary data collected by their fitness trackers, as they can easily view and interact with such information within their fitness applications. This is not the case for inferences. Rader and Slaker identified the importance of visibility for informing users' mental models of the relationships between fitness tracker data [65]. Thus, another issue that might contribute to the problem of users' lack of awareness about inferences is the lack of mechanisms and privacy nudges that provide some visibility into the inferences that are possible. I argue that nudges, in particular, could stimulate users' reasoning about potential inferences. Currently, users can only rely on what they learn from privacy policies or the news media to learn about inferences that are possible and probable. I discuss more on implementing interface privacy nudges in section 4.5.3.

### 4.5.2 Comfort with inferences

The participants' comfort sharing inferred information shows patterns similar to that of primary information – comfort varies with the type of information and the audience [9, 23], with people being most comfortable sharing information with those closest to them. Interview participants' reactions to the scenarios also suggest that their comfort with inferences is dependent on the perceived benefits, data accuracy, and anonymization. Some of the interview participants indicated that they would disclose their information if there is a value. Users' willingness to obtain a benefit even though a risk is knowingly involved can be described by the "Privacy Calculus" theory, which posits that users balance the perceived benefits (e.g., monetary or health benefit) against the privacy risks; if the benefits outweigh the risks, then users are likely to disclose personal information [73].

In both studies, participants reported little value in sharing inferred information with workplaces and insurance companies, for example. However, as prior studies have shown,

many people currently do share their sensed data with such organizations to gain discounts or participate in workplace health campaigns [9]. When users consider much of the primary information not sensitive, they see few risks involved in gaining those benefits. Yet, greater awareness of what information could be inferred from such information may change that privacy calculus.

Interestingly, interview participants expressed willingness to share information if done so anonymously. Fitness tracker users do expect that their information will not be linked to their real identities when stored or shared. Several participants mentioned strategies they already take or would take to protect their identities, such as providing incorrect personal information on accounts. Thus, users may not be against inferences being used in situations where they can remain anonymous. However, only a few of the interview participants recognized the possibility of combining and de-anonymizing data. Therefore, users may not recognize the risks of sharing what they think is non-identifiable information.

Finally, users also raised the issue of accuracy. Many participants believed that wearable technology is not smart enough to predict certain information (e.g., mood and sexual activity), thus impacting their judgements on the likelihood of the inference. A few of those participants who considered inferences useful seemed to value the accuracy of those inferences. Yet, accuracy perceptions also impact comfort, as users do not want people or organizations to draw judgements or use information about them that is inaccurate. Accuracy is especially important if data is used to determine consumer eligibility for benefits, for example. Yet, there are currently few mechanisms for reviewing the information that could be inferred from fitness tracker data.

### 4.5.3 Implications

The results have several implications for increasing users' awareness of possible inferences and for helping them to reason about and control the use of their data.

**Regulations and policies—** A commonly cited factor by the interview participants that can reduce their discomfort about inferences is the availability of a notice/consent protocol. In the context of sensor devices, Schneegass et al. [70] recommended that data collection requests should be presented to users at the derived information level rather than at the sensor level. Regulators should mandate companies and policy makers to adopt this approach by providing consumers with detailed information that explains what kinds of information can be inferred from their sensed data. However, a challenge is that users can be overwhelmed to manage a large amount of derived information. An alternative would be a system, such as the one presented by Liu, et al. [43] for mobile platforms, that builds privacy profiles to support users by predicting their privacy preferences. Such a system could ask users what data they want to disclose and provide them with what can be discovered based on this data. Users can then customize their privacy settings accordingly.

When additional information may be accessed, companies should use terms that convey inferences. For example, when an app requests permission from a user to access data, a statement such as the following could be helpful: "We use the heart rate sensor to predict your fitness level, sleep depth, and mood so we can create a customized plan." Thus, users will realize that other information can be revealed, which help them make more informed privacy decisions. In addition, privacy policies should clarify for consumers the level of data anonymization. While anonymity cannot always be assured because other data sources can be used to reveal one's identity, device companies should request as little personally

identifiable information as possible. For example, instead of asking users to provide their exact birthdate, users can be provided with a list of age groups (e.g., 25-35) to choose their age range.

I also found that accuracy influences users' comfort about certain inferences. Yet, users have no means to validate the accuracy of data generated about them by sensor devices. Users might be presented with a percentage that represents the degree of accuracy for each piece of data that can be sensed and generated by a device, so they can decide on what information they want to share.

**Awareness through experience and educational tools—** Privacy notices are currently the main method to make users aware of the use of their data. Yet, these policies are often complex and mostly ignored by users. The interview participants who initially expressed comfort with inferences explained that they had never experienced or heard of certain types of inferences. In contrast, those who were able to recall reading about relevant incidents believed that some scenarios are possible. Thus, stories and incidents presented in media seem to have an impact on users' attitudes and behaviors. This implication intersects with that by Rader et al. [64] about online inferences, in that awareness can be greater when users link inferences to their personal past behaviors and actions.

In addition, previous research proposed interactive tools, such as games, to improve people's awareness about privacy risks and to encourage behavior change [7, 88]. Given the limited work on such tools, future research is recommended to explore the opportunities of these tools in improving awareness, and to ultimately encourage users to achieve their desired privacy behaviors. Privacy awareness tools should focus on potential inferences from fitness tracker data that is generally considered trivial, such as step count, and should

explain how data collected by wearable devices can be aggregated to infer additional information. In addition, these tools may request users to input the data they usually share. Based on this data, the tool may show a user the information that could be inferred, the potential risks of inferring such information, along with protection techniques. Yet, the challenge is that users may not be bothered to find and use these tools, especially if they consider fitness tracker data innocuous.

**Interface nudges and cues—** As many have argued, I believe the best way to increase awareness of data use and risks is with cues within the interface itself that users will view during their regular interactions. Thus, my findings suggest exploring both visual cues as well as design mechanisms that nudge users to consider their disclosure decisions. Nudges have been proposed and implemented for other online services and mobile apps [8, 43], but not in this domain. Nudges presented by these prior studies have been reported to be effective in motivating users to adjust their settings. Inspired by these studies, wearable device nudges can be as simple as interface pop-ups that display on a device screen or mobile app to remind users to revisit their privacy settings. These windows can be designed to draw users' attention and may include annotations to illustrate which sensitive information is being used. For example, the current settings of fitness trackers do not quantify third party access to users' data. Nudges, therefore, can be designed to inform users how frequently an app accesses users' data and what is the potential purpose of accessing it [43]. Thus, users can be made aware of unexpected use of their data. Nudges in fitness trackers can also be visual indicators of dependencies among fitness and non-fitness data [65]; for instance, miles covered during an exercise that are calculated based on location traces.

**Customized controls based on recipients—** The results show that users have different levels of comfort if certain personal information is being inferred from their data by particular audiences, for example, employers inferring mood. However, current wearable fitness devices and their platforms lack customization in terms of audiences. Many devices offer private, friends, or public as the visibility options, but previous studies reported more audiences for whom users want to share fitness information with [9, 23]. In addition, most wearable devices do not provide options to control the sharing and privacy of data directly from the device, understandably because of the limited screen size of a device. Rather, users need to install a device app or to use the web service to adjust settings. To overcome the problem of an interface size, I recommend making setting options and icons scalable; for example, by occupying the entire screen when an option is being clicked by a user. To avoid unintended changes (e.g., clicking on the wrong option), nudges in the form of confirmation might be displayed to users before they make important changes within the settings.

**Local storage and processing—** The interview participants expressed a desire to keep their data local instead of uploading it to remote servers. While this option may not always be possible due to the need to process large volumes of users' data and tailor services, devices could improve privacy options by allowing users to opt in to cloud-based services where possible and instead rely on local storage and processing. Thus, since data storage and processing occur locally in users' devices, they may perceive more control over their data and less exposure to inferences and privacy risks. If local storage is not a possible option, then devices could have a mechanism to preserve users' data before it is sent to a remote server. For example, a data filter may be implemented to remove sensitive or

detailed data (e.g., heart rate variability) and to keep data in a general format (e.g., heart rate).

## 4.6 Summary

Sensor-based devices that collect health and fitness data can be used to derive personal and even sensitive information about users. My study findings contribute to the understanding of users' perceptions and attitudes about such inferences. While many of the interview participants were initially unconcerned about sharing fitness tracker data in general, they became more concerned after considering inferences. This finding was confirmed by the survey results, which show that the participants were less comfortable sharing inferred information across a range of audiences. Thus, awareness of inferences is likely not being considered as wearable fitness device users make privacy and sharing decisions. Yet, those decisions may go against their desires should their data be used to infer additional information. My findings also highlight important aspects that users do consider, including the probability that an inference can happen, the accuracy of data being used to make inferences, the benefit obtained in return for sharing information, and the belief that their real identity is anonymized. Overall, wearable device interfaces and privacy notices need to include additional awareness mechanisms to help users think about inferences.

# CHAPTER 5: EXPLORING THE DESIGN SPACE OF SHARING AND PRIVACY MECHANISMS IN WEARABLE FITNESS PLATFORMS

## 5.1 Motivations

Users' goals for sharing fitness information vary, and this may require sharing different levels of personal information with a variety of recipients. Yet, there are a number of common practices depending on those goals and the associated platforms used. Device platforms could ease this sharing and empower users to protect their information by providing controls and features centered around these common sharing goals. However, there is little research that examines existing mechanisms for sharing and privacy management, and what needs users have beyond their current controls.

In this chapter, I combined the findings from my first two studies to analyze five popular wearable device platforms regarding the commonalities and differences in controls and features available within these platforms. For instance, how and to what extent the current controls support users' sharing patterns shown in Table *2*, and what interface mechanisms are available for awareness about potential privacy problems resulted from the collection and sharing of users' information. I developed taxonomies of mechanisms based on common sharing patterns and boundaries, as well as data collection awareness. With this analysis, I identified design opportunities for supporting users' sharing and privacy needs.

## 5.2 Design Space Exploration

I explored the design space of sharing and privacy mechanisms in the context of wearable fitness technology. My study provides a broader view by examining five wearable brands that have mobile apps with some sharing features. The chosen platforms are Fitbit, Apple Watch Activity, Polar Flow, Garmin Connect, and Samsung Health. I analyzed these

platforms in May and June 2020. I purchased the devices in order to access all functionalities and to understand their different privacy controls and sharing mechanisms. In particular, I investigated these platforms regarding two main themes: sharing patterns and data collection awareness mechanisms.

First, I systematically examined all features within a particular device and made note of all features and screens I was able to. I focused on both sharing and privacy features and controls. I then organized these features to create a taxonomy of these mechanisms. I wanted to understand what features platforms have for supporting all possible sharing patterns, inside or outside a platform. Chapter 3 presents a comprehensive set of sharing patterns in wearable fitness trackers, and thus I considered these patterns through my analysis of the five platforms. Second, systems commonly make users aware of their own privacy through different means. I am interested in how a device platform may communicate privacy aspects to users during regular interaction with a system. This includes information requested from users in the account creation and any interface notifications or nudges related to privacy. The usability of privacy policies and Terms of Service (ToS) Agreements is a challenge that has been studied extensively. Thus, I consider this aspect outside the scope of this analysis. My study identifies commonalities and differences in controls and features available within these platforms and presents a set of taxonomies.

## 5.3 Findings

I first analyzed sharing mechanisms in these platforms based on several sharing patterns. Sharing fitness tracker data can generally occur in two ways: inside a platform with other users and communities (e.g., Fitbit communities), or on external compatible third-party

apps (e.g., social media apps). Users can utilize various controls to manage internal sharing and have general controls to manage sharing self-tracking data with third parties. I will discuss features and controls for both sharing methods in more detail. In the second part of this section, I briefly describe platform mechanisms for data collection awareness.

### 5.3.1 Sharing Mechanisms

Sharing decisions of fitness tracker users are goal-driven with audiences and specific practices related to those goals. For instance, a common practice by users who share with friends is to utilize popular social media channels, such as Facebook and Twitter. Thus, I focus on investigating whether platforms support these patterns and what mechanisms they have in common for each of these patterns.

Table 7: Taxonomy of the Sharing Patterns in Five Wearable Device Platforms

| Pattern | Sharing Mechanism | Fitbit | Apple Activity | Polar Flow | Garmin Connect | Samsung Health |
|---|---|---|---|---|---|---|
| Friends | Screenshot of activity | ✓ | ✓ | X | X | ✓ |
| | Photo with summary | X | X | ✓ | ✓ | ✓ |
| | Web link | X | X | X | ✓ | X |
| Family | Family account feature | ✓ | X | X | X | X |
| Strangers | Fitness groups feature | ✓ | X | ✓ | ✓ | X |
| | External fitness community | ✓ | X | ✓ | ✓ | X |
| Caregivers | N/A | | | | | |
| Incentive Programs | Rewards through connected 3rd party apps | ✓ | X | ✓ | X | X |
| Workplaces | Corporate Wellness Programs feature | ✓ | X | ✓ | ✓ | X |
| | Built-in fitness groups | ✓ | X | ✓ | ✓ | X |

**Friends Pattern.** All the examined platforms have social features that enable users to form a connection (e.g., friendship) with other individuals in these platforms. Typically, sharing with other people over these platforms requires that both sides have a device from the same manufacturer. To connect with other Apple Watch Activity and Samsung Health users, one needs their ID, such as the email or phone number that is linked to the account.

Given that these platforms have sharing features similar to those in common social network sites, I looked at their boundary mechanisms to categorize and further discuss the controls people can utilize when interacting with friends over these platforms (Table 8). Boundary mechanisms are interface controls that can be used to restrict other users' access to oneself. These controls have been extensively studied in social media platforms [40, 89], but not yet in the context of IoT device platforms.

The first boundary, relationship, refers to controlling who can be part of a personal social network. Regardless of the type of relationship with a user, all the examined platforms except Fitbit, which has a family feature, have the same settings for all connections including friends. There are two types of controls for managing connection boundaries that are similar in these platforms: accept/decline connection requests and remove/stop following friends. All platforms support these two options except for Samsung Health. There, any user can be followed by others if they know his or her account ID.

The territorial boundary is the regulation of who can view an individual's "personal space", in this case, their personal profile information, including their friends list. All platforms allow users to stay private or to share information with friends/followers. Garmin Connect provides more visibility options than the other platforms— it also offers users to

keep their data private or to share it with followers, groups and followers, or public. Apple Watch activity is the only one that allows users to hide information from particular friends.

Table 8: Taxonomy of Boundary Controls in Wearable Fitness Platforms

| Boundary | Controls | Fitbit | Apple Activity | Polar Flow | Garmin Connect | Samsung Health |
|---|---|---|---|---|---|---|
| Relationship | Accept/decline friendship | ✓ | ✓ | ✓ | ✓ | **X** |
| | Remove friend/stop following | ✓ | ✓ | ✓ | ✓ | ✓ |
| Territorial | Profile visibility | ✓ | **X** | ✓ | ✓ | ✓ |
| Disclosure | Information customization | ✓ | ✓ | ✓ | ✓ | ✓ |
| Interactional | Disable Friendship Request | **X** | ✓ | ✓ | ✓ | **X** |
| | Disable comments | **X** | ✓ | **X** | ✓ | **N/A** |
| | Disable likes/cheers | ✓ | **N/A** | ✓ | ✓ | **N/A** |
| | Block Users | ✓ | **X** | **X** | ✓ | ✓ |

There are several levels to control visibility of information contained within a profile (e.g., leaderboard, activity, training, and challenges), and these levels vary between the examined platforms (Table *9*). For example, Fitbit has controls for each piece of profile information, while Apple Activity settings are less flexible than the other platforms in that the entire profile will be hidden. Note that profile information in the Apple Activity differs from the other platforms in that it includes activity information only, rather than additional personal information, such as age and gender. Polar Flow and Garmin Connect links the visibility of the friends list to the entire profile visibility.

The disclosure boundary deals with controlling the disclosure of one's own personal information. Currently, there are three main categories of personal information that users

can disclose to other people over these platforms. First, the profile information which mostly includes gender, age, birthdate, weight, and height. I discussed the controls related to profile information in the territorial boundary. The second category of information that users will be able to disclose is the daily activity summary. The level of granularity differs depending on a platform. Users will mostly be able to share daily step count, distance, active minutes, and calories burned. Depending on the privacy settings selected by a user, Apple Watch Activity, Polar Flow, Garmin Connect, and Samsung Health automatically share a daily activity summary with friends. For Fitbit users, they need to push their data summary to other users. The third category is exercise sessions, such as walking, running, and cycling. Most devices will automatically detect this data with their various sensors, otherwise users need to log their workouts manually. This data requires an action by a user by pushing it to other people, except in Polar Flow, which will automatically upload data to connections based on the user's selected settings.

Table 9: Visibility Controls of Activity Information

| Level | Fitbit | Apple Activity | Polar Flow | Garmin Connect | Samsung Health |
|---|---|---|---|---|---|
| Private | ✓ | ✓ | ✓ | ✓ | ✓ |
| Followers | ✓ | ✓ | ✓ | ✓ | ✓ |
| Specific Followers | **X** | ✓ | **X** | **X** | **X** |
| My Groups & Followers | **X** | **X** | **X** | ✓ | **X** |
| Public | ✓ | ✓ | ✓ | ✓ | ✓ |

If users need further restrictions in terms of others' access to oneself, then they may utilize the interactional boundary controls. There are four areas where these types of controls can be used: disabling friendship requests, disabling comments, disabling likes/cheering, and blocking users. Except for Fitbit and Samsung Health, all users will be able to withdraw a friendship request that they sent to other users. One cannot post

comments to other Samsung users, and comments to Apple Watch users will be sent in the form of text messages. In addition, both Apple Watch Activity and Samsung Health do not offer features for liking or cheering. Fitbit and Polar Flow users can remove likes, but they cannot remove posted comments. Sometimes users need to prevent other users from being able to find their profiles or send them friendship requests, and thus they may take advantage of the block user feature. Currently, Fitbit, Polar Flow, and Garmin Connect users can block other individuals through the intended individual profile pages. Samsung Health allows one to hide his/her ID from being searched by other users but does not offer the block feature. Activity is the fitness tracking app for Apple Watch, and some of its data needs to be managed through the phone settings. Users can add their connections on the Activity app as contacts in the phone, and thus they will be able to block messages from them. However, other users will still be able to send someone a friendship request if they have his/her account ID. Only Garmin connect provides users controls to manage all forms of interaction with other people.

I found in the study of chapter 3 that users who share their activity data with friends commonly use social media sites outside of the device platform, but the participants faced concerns over the broad audience on those platforms. Thus, the most important design aspect in the context of this pattern is whether a platform supports sharing data on social media applications and how. All five platforms allow their users to share self-tracking data on the social media applications installed in the user's mobile phone by pushing a summary of data to these applications. Fitbit, Apple Activity, and Samsung Health allow users to push charts with a summary of data shown on them. Polar Flow, Garmin Connect, and Samsung Health users can also choose an existing photo in the phone or take a new one

and share it. Depending on an exercise type, Polar Flow allows sharing a map of exercise routes with a summary of data shown on it. Garmin Connect users can also share a web link that will take recipients into a Garmin page that has a variety of data about the exercise.

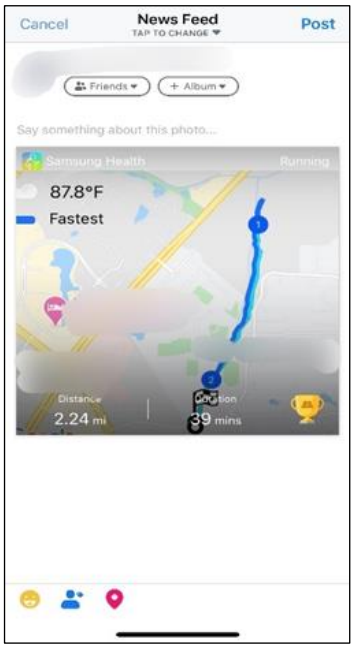



Figure 6: Sharing Fitness Tracker Data on Facebook (Samsung Health)

The level of data that can be shared on social media applications varies, depending on what can be collected by a device. For example, Samsung Health enables sharing a variety of granular data, such as movement data (e.g., step count, duration, and intervals), heart rate (e.g., average and resting heart rate) and calories consumed (e.g., carbs, fat, and protein). Apple Activity enables recording several exercises and data, but it visualizes three abstract rings that represent levels of "move," "exercise," and "stand" when data is shared externally with other people.

In terms of audiences, if users want to share their fitness data collected by trackers on social media applications and specify particular audiences, they need to adjust that from

the settings of the destination platform only (e.g., Figure 6). Facebook, for example, offers different categories of connection (e.g., acquaintances, friends, close friends).

In summary, all five platforms enable sharing activity data with friends within a platform and on social media sites. However, the level of granularity depends on the controls offered by a platform. The interpersonal boundary controls in these platforms include relationship, territorial, disclosure, and interaction. Overall, Garmin Connect is the best platform in supporting the identified interpersonal boundary controls, and Samsung Health provides the least support of these controls.

**Family Pattern.** Users seek mutual accountability and inspiration by sharing with those closest to them, namely family members and very close friends. Currently, only Fitbit distinguishes family from the other connections. Through the "My Family" feature in Fitbit, users can create a family account (Figure 7), create accounts for kids, and invite other family members or guardians. The other four platforms do not offer this feature. One limitation with the Fitbit family account feature is that one cannot customize data based on individuals, though this may not be a concern when sharing with family members as people are often most comfortable sharing detailed information with family. In Apple Activity, users can share their data with family members if each member has the watch. As in the friends' pattern, sharing with family in Apple Activity is peer to peer, which means that data shared by a user with one family member will not be accessible to the other members. Added family members will be considered as general friends in the remaining three platforms, and thus the visibility and interaction among them is dependent on the platform settings for friends.

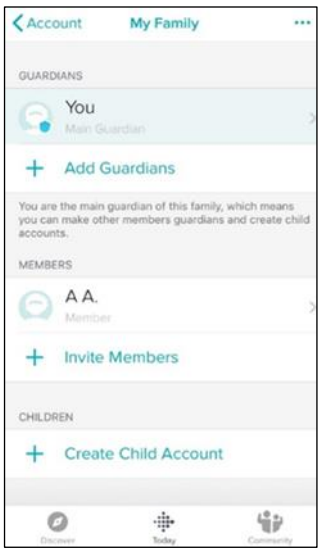



Figure 7: Family Feature within Fitbit

**Health/Fitness Support Groups Pattern.** Seeking advice and accountability related to health and fitness are common goals for sharing information by fitness tracker users. There are currently two methods offered by wearable device platforms for sharing data with health and fitness groups (mostly strangers): within-platform fitness communities and on external fitness communities, such as Strava.

Fitbit, Polar Flow, and Garmin Connect offer users the ability to join and create various health and fitness groups around personal interests such as weight loss and running. Samsung Health only offers a simple feature to compare step count with users of the same age group as well as with all users. For Polar Flow and Garmin Connect groups, they can be created using the web service only. These platforms have similar privacy settings for groups, as shown in Table 10. The discoverability of a group is dependent on the controls provided by a platform. Open groups and their posts are visible to all users. Private groups, their posts, and members are not visible to people outside a group and can be joined through an invitation. Closed groups are similar to private groups, but visibility of posts depends

on the platform. For example, a Fitbit closed group, their members, and posts will not be visible to other users. Thus, Fitbit in fact has two options for a group creation: an open or a closed group.

Table 10: Visibility Controls of Groups

| Level | Fitbit | Apple Activity | Polar Flow | Garmin Connect | Samsung Health |
|---|---|---|---|---|---|
| Private Group | ✓ | **N/A** | ✓ | ✓ | **N/A** |
| Closed Group | | **N/A** | ✓ | ✓ | **N/A** |
| Open Group | ✓ | **N/A** | ✓ | ✓ | **N/A** |

The other method to share fitness tracker data with groups is through external apps, such as Strava. Currently, all platforms except Apple Watch Activity and Samsung Health allow users to connect device data to different external partner apps. Prior versions of Samsung Health enabled users to connect to partner services; however, that option is no longer available according to Samsung. Apple Watch Activity users can connect their device data with third parties through the "Watch" app.

**Caregivers Pattern.** The examined platforms have no features to share data directly with health providers or to interact with them. Thus, the only method to share self-tracking data with healthcare providers is to have a health provider app compatible with a device platform in order to automatically pull out users' data. Samsung Health stopped supporting the "Expert" feature within their platform, a service that Samsung said was covered by most health insurance companies, which enabled users to directly contact doctors regarding any issue with their health or fitness data recorded by a device [3]. Apple Watch Activity provides interesting visualizations of health and fitness data because it can integrate with the Health app, which in turn can integrate with compatible health provider apps. One limitation with Activity is that it does not provide features to capture or track sleep data as the other four platforms do.

**Incentive Programs Pattern.** Different services that provide monetary incentives for healthy behaviors can be connected with wearable fitness devices. Only Fitbit and Polar Flow were found to have compatible services that offer financial incentives. For example, Fitbit enables users to connect their accounts with a pharmacy to earn points based on activity level, which can be used as discounts. For Polar Flow, some of the partner services can be connected through the web service only.

Users need to first provide permission to incentive apps to access their data. The examined platforms have different representations regarding how users' data will be accessed by third party apps. In addition, each platform can have different representations based on the type of third-party app (Figure 8). I found most of the descriptions presented to users by these platforms to be generic, and permission options are less granular. The Fitbit iOS interface, for instance, provides a list of data in a high-level format (e.g., activity and exercises).

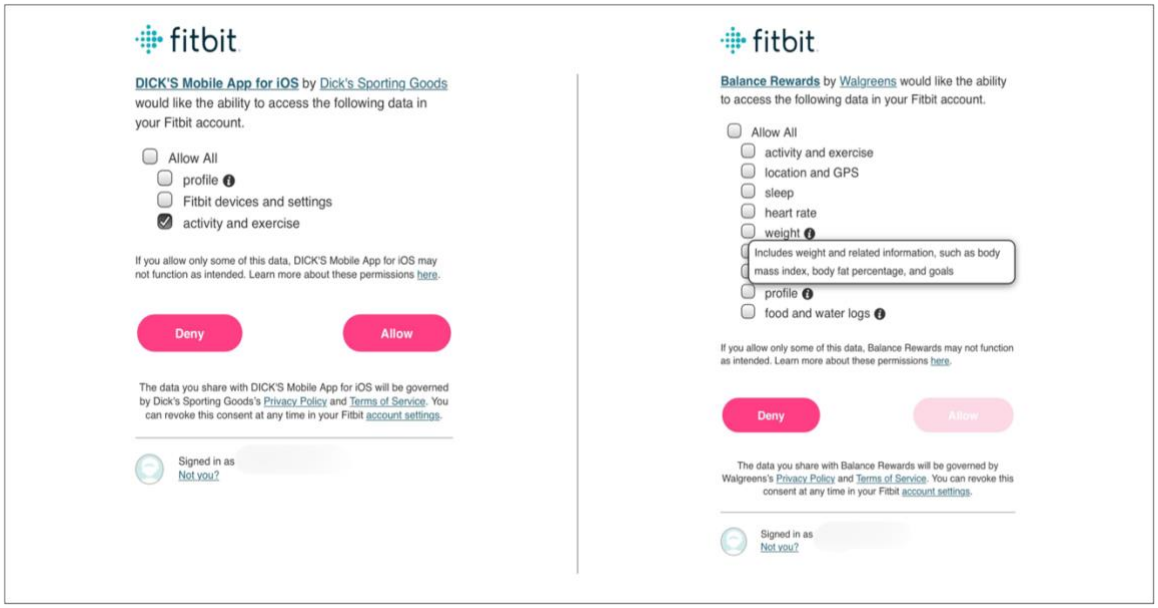



Figure 8: Two Data Access Representation by Fitbit for Two Third Party apps

**Workplaces Pattern.** To encourage employees to maintain a healthy lifestyle, some employers offer wellness programs in a workplace. Participated employees would be able to share data collected by their fitness trackers, compare, and compete with each other.

I found two primary methods to automatically share fitness tracker data, mainly step count, in workplaces. The first method is a feature offered by a wearable device company either within the mobile app or in the webpage as a service for employers, commonly called a Corporate Wellness Program. Thus, employees need to use the same fitness tracker brand to participate. This feature is currently supported by Fitbit [1], Polar Flow [2], and Garmin Connect [56]. Managing the privacy of participants depends on the configurations offered by the fitness tracker company. The second method is to simply create a workmate group within a platform, if this feature is offered. This method has two limitations: first, it is difficult to manage groups of a large size; and again, participants usually need to have the same fitness tracker brand.

As in the incentive programs pattern, employers can have their own third party app that can integrate with some wearable device platforms through their Application Programming Interfaces (APIs) to pull out users' data. Thus, the level of access to data depends on a device platform.

### 5.3.2 Data Collection Awareness Mechanisms

The purpose of a wearable fitness device is to automatically collect data and report it to users. All devices have detailed views of the sensed information (e.g., movement data and sleep pattern). Studies indicated that data collected by these sensor devices can be used to infer sensitive information. Therefore, I examined the collection awareness mechanisms of additional information in these platforms. I define data collection awareness mechanisms

as any interface notifications (e.g., pop ups), permission requests, feedback or statements within a device platform that inform users about what personal information will be collected and how it will be used. As a reminder, privacy policies and ToS Agreements are outside the scope of this analysis. In the following paragraphs, I summarize some of these awareness mechanisms in each platform.

One type of sharing that users are made aware of is third party apps. Overall, all platforms that can be connected to external services have similar awareness mechanisms for third parties. Descriptions and lists of data are presented to users in a high-level format (e.g., activity rather than steps, active minutes; sleep rather than sleep time and duration) when connecting an app. Fitbit and Polar Flow provide additional contextual information, such as when an app has been approved. In addition, Fitbit provides information about the type of access (read, write) and sometimes a short description of the purpose of collecting data by a third-party app. Note that in Polar Flow, this information can only be seen through its web service. Much of the Activity app data, such as access to location, is managed from the Watch app and the phone settings. Garmin Connect users can directly enable/disable phone permissions, such as camera and location information, from the app itself with information by Garmin about what data collected by these systems can be used for.

Another awareness mechanism related to the collection of data is when a user creates an account in these platforms. Some platforms provide users information about the personal details that can be inferred from the data they enter or enable through account creation. Overall, the platforms differ slightly in their mechanism and degree of transparency. For example, the Polar Flow web service has short, yet informative, statements about the

information that can be inferred from the data collected from users, such as predicting if a user is normal weight, underweight, or obese based on the entered weight and height. When installing a new device, Garmin Connect presents users with several health and fitness tracking features that can also be enabled from the settings, such as stress level based on heart rate variability, which Garmin stated would be visible to users only. The Apple Watch app provides users with short disclaimers, sometimes with links, about the data that will be collected if users enable certain tracking features. For example, if users click on the "Heart" feature, they will be presented with several statements with links that describe how heart data can be used to infer additional information.

In terms of notifications, I did not find notifications that deal with privacy in these platforms except those that alert users about friendship requests, likes, or comments by other users.

## 5.4 Discussion

Here I discuss gaps and potential design opportunities in relation to the sharing patterns and data collection awareness mechanisms I identified in the five platforms.

### 5.4.1 Sharing Patterns

**Friends.** Sharing with connections is the most feature rich pattern supported by wearable fitness devices. Platforms provide a number of controls for connecting and disclosing information. However, there appear to still be mechanisms that are missing. Specifically, users should be allowed to select which recipient they want to share their fitness data with. Currently, all platforms do not differentiate between connections with respect to their level of relationship with a user. A possible solution is to allow customization similar to Facebook Custom List (i.e., friends, specific friends,

acquaintances, etc.). Fitbit also has a limitation in that it does not enable sharing exercise data with all connections in a single click, but a user needs to repeat the action for all connections, which can be tedious. Apple Watch Activity has also room for improvement regarding this mechanism, particularly when data is shared on social media apps. Apple Activity users can only share three abstract rings that represent daily levels of: move, exercise, and stand. Yet, this abstract data does not tell all the story about one's activity level, and users may desire to share and compare granular details with peers.

**Family.** One group of people that users commonly feel comfortable sharing with is family. Among the five investigated platforms, only Fitbit provides a family-related feature. However, users' sharing behaviors are dynamic even with close connections, such as family, and the existing Fitbit family feature lacks controls that enable users to change their preferences. The family account main interface can be redesigned to enable users to specify their sharing preferences. For example, users might be allowed to click on a particular family member picture that takes the user to that member page, and then a tab could be added that allows users to choose what information they want to share with particular members. By making these improvements, I believe that the Fitbit family account would be a model for other platforms to integrate this feature.

**Health/Fitness Support Groups.** Wearables, such as Apple and Samsung Watches are primarily designed to be smart with some of the phone functionalities integrated in them. Therefore, they have fewer considerations for socializing. Incorporating some social features, such as fitness communities and groups in their fitness tracking apps could potentially improve users' wellbeing through competition and accountability. Group creation in Polar Flow and Garmin Connect can currently be managed via their websites.

Implementing this feature in the mobile app would be easier and more convenient for users to manage their data. As far as the sharing settings related to fitness groups, there are no controls across all the examined platforms that allow users to disclose different information with different group members.

**Caregivers.** People are increasingly utilizing wearable devices for different personal health and fitness goals, such as monitoring diabetes, weight management, injury recovery, etc. My findings of study 1 (chapter 3) show that users had dissatisfaction about the lack of support for communication with doctors regarding self-tracking data by the current platforms. Currently, there is no option in any platform that enables users to directly communicate with health providers regarding self-tracking data. Thus, I urge for providing mechanisms that enable integration with health provide systems, while also ensuring that controls are available to protect users' sensitive information. Other features could support composing summary views or downloadable data that are appropriate and customized for caregiving settings.

**Incentive Programs.** Increasing physical activity through financial incentives is a powerful strategy, but this is usually not without a price. Third party companies that provide these services may utilize users' health and fitness data for research and marketing purposes, which could lead to undesirable inferences about users, including personal identity exposure. In all the examined platforms, companies are allowed to access users' personal data at a high-level (e.g., Figure 8), which means that they could legally access detailed information without users' awareness. Users should be able to control access to all dimensions of their information. I noticed that while users do have some granular controls

and awareness, there are currently no mechanisms to enable users to audit what information a third-party has accessed.

**Workplaces.** Workplace health campaigns are popular and could be supported by wearable fitness trackers. Only three platforms integrate a workplace wellness feature in their platforms currently which mostly collects step count. Individuals who join these programs may do so in response to social pressure. While step count may not be of a huge concern for participants in these programs, such data may provide an impression about a person's health and fitness lifestyle. Thus, designers of these features should provide flexible controls that enable participants in these workplace programs to change their sharing preferences anytime and to accommodate different interpersonal boundaries. Aside from these interpersonal concerns, there is a wide concern that data collected in these programs could be used for secondary purposes, for example by employers or health insurance companies [59]. As of now, privacy policies appear to be the only possible mechanism to understand whether such data use could occur. Additional mechanisms within the app could be useful as well.

### 5.4.2 Data Collection Awareness

Data collection awareness mechanisms can help users understand what information about them will be used, and thus make informed privacy decisions. Apart from lengthy privacy policies and ToS agreements, I conclude that there are inadequate awareness mechanisms, both active and passive, in wearable fitness device platforms. Those few mechanisms that are already implemented, such as links to descriptions of how particular sensors work to measure some personal data, are mostly overwhelming or unseen by users. For example, Polar Flow provides short statements in the user account information about

how certain data users enter can be used to disclose additional information (e.g., if a user is normal weight, underweight, or obese based on height and weight). Yet, users would only view this information once, while creating an account. Rather, awareness mechanisms can be simplified in a way that could engage users more frequently. For instance, platform interfaces could display how certain pieces of activity information work together, such as showing how heart rate rhythms change and calories are burned while walking.

Another common limitation in the data collection mechanisms I found in these platforms is third party authorization, which are implemented to collect users' data at high levels. These mechanisms can be re-designed by adding granularity as well as contextual details, such as when a particular app was approved by a user and how frequently the app has accessed data. Lastly, the current platforms also fail in terms of privacy notifications, such as those that remind users about their sharing practices with third party apps. For example, a user could be reminded if they still want to keep connecting an app that has been given permission for a long period of time (e.g., more than 6 months). I suggest implementing these notifications periodically to help users in controlling the privacy of their personal information.

## 5.5 Summary

Platforms of wearable fitness devices could be redesigned to satisfy users' sharing goals and privacy needs. In this chapter, I examined the sharing and privacy mechanisms of five poplar wearable device platforms for tracking fitness. I presented a set of taxonomies based on sharing patterns, boundary controls, and data collection awareness mechanisms. I found similar mechanisms among the examined platforms. I also identified some design limitations where improvements could be made in these platforms to further users' ability

to useful share their data while still protecting their privacy. The taxonomies presented in this study can be valuable guidance for the design of sharing and privacy solutions in activity trackers, which is the purpose of the next chapter.

# CHAPTER 6: CO-DESIGN FOR SHARING AND PRIVACY IN WEARABLE FITNESS TRACKERS

## 6.1 Motivation

The social factor can be an important drive for continuous tracking of personal health and fitness data. Different features that support sharing have been integrated within fitness trackers. Yet, studies indicated that users do not utilize many of these features for different considerations, such as the lack of reaction by others [51] and the discomfort to share with strangers [21].

More importantly, manufacturers and designers may not pay sufficient attention to the privacy aspect in these devices. Users also may not be concerned about their privacy, and sometimes they may take the risk of disclosure to obtain the anticipated benefit. Studies indicated that users can be unaware about the potential risks associated with the disclosure of their personal information [7, 70]. Privacy policies alone may not be adequate to inform users about how their information is used and shared because they are often long, and thus ignored by users.

Privacy settings, on the other hand, can be improved in order to maximize the use of the different social features and to enable full control over personal information. Yet, previous related work has focused on exploring users' privacy attitudes, perceptions, and behaviors with little attention to the practical and design alternatives [23, 42, 60, 65, 70]. Such studies investigated the types of data that users consider sensitive [42], their comfort level sharing with different audiences [23, 60], and their awareness of aggregation and inferences [65, 70]. These studies can be a valuable foundation to understand users before building IoT

devices, but there is also a need for studies that present actual design solutions for sharing and privacy problems, especially in the context of the fitness tracking domain.

In chapter 5, I took an initial step by analyzing five commercial fitness tracker platforms regarding sharing patterns and privacy awareness mechanisms. I found commonalities in the controls and features of the examined platforms, identified several limitations, and built a taxonomy of their sharing and privacy mechanisms. Given that end users can differ in their sharing preferences, as well as in their use of privacy settings, it is crucial to involve them directly in the design of interfaces.

Thus, in this chapter I conducted a series of participatory design sessions with end users to further explore the design opportunities of sharing and privacy controls and features. I will ultimately use the combined analysis (chapter 5 and the current chapter), as well as my findings from the first two studies to recommend a set of sharing and privacy features for fitness tracker interfaces.

## 6.2 Methodology

To examine how fitness tracker users desire to share and protect their information, I conducted a set of participatory design sessions. Participatory design (also known as co-design and cooperative design), as the name suggests, is the involvement of users in the design process of products. The term participatory design was first coined by the Scandinavians who demanded democracy in the workplace [50]. The participatory design approach has received notable interest by HCI researchers in several domains, including graphic, software, and interface designs. An HCI researcher or a designer works with end-users (and maybe other stakeholders) to create design concepts and features that meet end-users' needs. Participatory design is especially useful if the design concepts are gathered

from people who directly interact with a system on a regular basis. Thus, one of the challenges of participatory design is to involve experienced people in order to collect valuable designs. A common drawback associated with the participatory design approach is that a sample size is often small and so may not be representative of a general population.

I conducted this participatory design study with Fitbit users who are familiar with the Fitbit app. I chose Fitbit because it is one of the top-selling devices in terms of fitness tracking [69]. Fitness tracker interfaces also have many commonalities in terms of sharing and privacy mechanisms; thus, recruiting only Fitbit users can provide consistency regarding the features designed by participants. Due to the Covid-19 pandemic, all study sessions were conducted online.

I recruited participants through Reddit communities, UNC Charlotte mailing lists, and by using snowball sampling. The recruitment post was framed as "a remote co-design study for sharing and privacy features in Fitbit." The post included a link to a screening survey, which collected demographic information. In addition, the screening survey had an option to sign up as a pair with any eligible Fitbit user (e.g., as a family member or as a co-worker). To be able to participate, the study required that potential participants be 18 years or older and Fitbit users. Each participant received a $25 Amazon gift card after the study. The research was cleared by the UNC Charlotte IRB.

The study had 32 participants in total (16 males and 16 females), and each session consisted of a pair of participants. Half of the recruited groups had some prior relationship— 3 are significant others, 2 are family, 2 are co-workers, and 1 is friends. Recruiting users in an existing relationship was suitable because they are likely to share their fitness information with each other, and thus those pairs may create features that

support their sharing needs. In addition, having only pair of users in each session was suitable given the relatively limited duration of each session (70 minutes, on average). The participants' ages ranged from 19 to 66, with an average of 31 years old. The participants came from different backgrounds, and several of them have a health-related degree. In addition, they had different occupations, such as accountants, health consultants, security analysts, advertisers, HR managers, students, and researchers. Table 11 presents participants' information.

Table 11: Participants' Information (Participatory Design)

| Group ID | Relationship | Participant ID | (Age, Gender, Occupation) |
|---|---|---|---|
| G1 | None | P1, P2 | (28, M, student), (26, M, structural analyst) |
| G2 | Family | P3, P4 | (66, F, retired), (32, F, advertiser) |
| G3 | None | P5, P6 | (38, M, health advisor), (36, M, student) |
| G4 | None | P7, P8 | (21, F, student), (28, F, administrative assistant) |
| G5 | None | P9, P10 | (25, M, crew member at a grocery store), (29, M, student) |
| G6 | Significant other | P11, P12 | (23, M, operations analyst), (23, F, clinical research associate) |
| G7 | None | P13, P14 | (34, M, assistant professor), (26, M, engineer) |
| G8 | None | P15, P16 | (34, M, student), (34, M, advertiser) |
| G9 | Significant other | P17, P18 | (29, F, HR manager), (29, M, data analyst consultant) |
| G10 | Friends | P19, P20 | (51, M, security researcher), (33, M, security analyst) |
| G11 | None | P21, P22 | (31, F, teaching assistant), (23, F, contract analyst) |
| G12 | Family | P23, P24 | (27, F, adjunct faculty), (31, M, electrical engineer) |
| G13 | Significant other | P25, P26 | (21, M, student), (20, F, student) |
| G14 | None | P27, P28 | (23, F, part-time receptionist), (19, F, leasing consultant) |
| G15 | Co-workers | P29, P30 | (52, F, budget analyst), (33, F, budget analyst) |
| G16 | Co-workers | P31, P32 | (36, F, HR clerk), (40, F, HR manager) |

The study consisted of three stages: a short pre-design interview, a design session, and a post-design presentation. The pre-design interview served as a warm-up for the design

session. In this stage, I asked the participants whether or not they share their information and what potential audiences they might be interested in sharing their information with. I also asked them if they had any concerns about the data that is collected by their devices, and how comfortable they are with the current sharing and privacy controls of the Fitbit. After that, I shared with participants a Google Slides link that directed them to the design sheet. I asked participants to design features that enhance sharing and preserve privacy in Fitbit (see the prompt in Appendix J). There, I prepared screenshots of the main interfaces of Fitbit settings, so participants could refer to them if needed. I also prepared a number of icons and shapes for participants to help them in the design. Early in this stage, I did not interact with the participants except to help them in locating any design icons or tools they needed. Later on, I introduced some design ideas based on my design space exploration of the Fitbit interface (Chapter 5), such as the use of some privacy nudges, if the participants did not design or think of such ideas. I informed participants that they do not have to incorporate the proposed ideas into their designs. Finally, I asked participants to present each of their designs and explain how the proposed design could improve sharing or privacy of Fitbit users. Each study lasted on average 70 minutes.

The collected data consists of video recordings and computer drawings. The recordings were transcribed and then qualitatively analyzed using thematic analysis. First, I deeply read through each transcript multiple times to gain insight. Then, I selected six transcripts and coded them to build an initial codebook. I coded the pre-design interview data, looking specifically for how comfortable the participants are with the existing controls, what data they need to share and with whom, and what data they need to protect. I also coded the features designed by participants, and this includes any discussion about features during

the design session and in the post-design presentation. After that, I used the codebook to code the remaining transcripts, and a few new codes appeared. I kept adding these codes to the codebook until no new codes emerged. I also took notes about the participants' drawings. Finally, I conceptually grouped both the transcription codes and the drawing notes into themes.

## 6.3 Findings

This study contributes actual designs and guidance about the sharing and privacy features that fitness tracker users value and desire, using Fitbit as a case study. To provide context to the findings, I first report the pre-design interview results, including participants' general sharing, their privacy concerns, and their use of Fitbit settings. I then introduce and explain the features designed by users. I will use the unique IDs in Table 11 to denote a participatory design group and an individual participant (e.g., G3 is group 3, P4 is participant 4).

### 6.3.1 Sharing, Privacy Concerns and Management

As a reminder, the main goal of the pre-design interview was to motivate participants to think about features and controls that match their privacy expectations and needs, which they may consider in the subsequent design session.

Most of the participants shared their self-tracking information with other individuals and with external apps (Table *12*). Those who shared their information shared it mainly with friends and family. In addition, P27 recorded food and sleep data using her Fitbit to share it with a doctor. Several participants indicted that they are part of several Fitbit communities where they share exercises such as biking, running, and hiking. Five participants mentioned sharing in a workplace. In addition, many participants connected

their Fitbit with external apps, including Strava, Lose it, RunKeeper, and Noom to take advantage of additional or better tracking features. P31 indicted that she connected her Fitbit with an app called Achievement to collect points and receive incentives based on her activity. Social media sites are another platform that participants used to share their fitness information. For example, P13 took screenshots of his exercises and shared it over Facebook. Participants stated several reasons for sharing their information, such as to compete with other users in order to stay accountable towards personal fitness goals. Due to the conditions of coronavirus quarantine and restrictions, two participants found their Fitbits helpful to track their steps while moving at home or when exercising in a neighborhood and to compare their data with other users.

I asked participants what privacy concerns, if any, they have about their information. A few participants mentioned that they are not worried, while most participants indicated that it depends on the data and the audience. Body weight and birthdate are two pieces of personal information that the Fitbit collects that many participants were uncomfortable sharing, especially with friends and family in regard to body weight. Other participants were unwilling to share heart rate and sleep data with third parties. Eight participants found location information concerning if it can be seen by strangers. One of these participants pointed out that people can find information such as home location in different ways, but location is particularly concerning if it is combined with information such as sleep and daily routine. However, many participants indicated that sharing location information, such as an exercise route, is actually an interesting feature that they still wanted to utilize. Participants proposed solutions for location privacy, such as privacy zones, which these participants mentioned seeing in other applications.

Table 12: Sharing Audiences of Participatory Design Participants

| Sharing Pattern | Participants | Quotation |
|---|---|---|
| Friends | P3, P4, P6, P7, P8, P9, P11, P12, P13, P14, P16, P22, P23, P25, P29, P30, P31, P32 | *"I share with family and **friends**. Sometimes I'll take screenshots, like if I really had a good stuff, I'll do screenshots and share them on Instagram and Facebook."* [P32] |
| Family | P4, P5, P6, P8, P15, P17, P23, P25, P27, P31 | *"I share but I was very selective about it. I only ever shared it with **my sister**."* [P17] |
| Relatives | P25 | *"When it comes to the sleep data that it collects, sometimes I'll show people the sleep patterns that are collected over tonight…. I usually share it with my parents or **my relatives.**"* [P25] |
| Significant others | P11, P12, P17, P18 | *"Before [**boyfriend**] got it, I didn't have any friends on Fitbit"* [P12]. |
| Health provider | P27 | *"I used to share sleep with my mom and my doctor, and I believe I used to record food, and I had to share that with **my doctor** as well."* [P27] |
| Incentive program | P32 | *"I do share it with an app called achievement where you can **get points** and it's like when you get 10,000 points, they will send you ten dollars or something like that."* [P32] |
| Workplace | P1, P17, P24, P29, P30 | *"I linked my Fitbit with **the work** app that tracks health and fitness relating to challenges that work will put up for the employees."* [P24] |
| Fitness group | P4, P5, P16, P22, P31 | *"I'm a part of a **mountain biking club**. So, we track our information there as well."* [P22] |
| Third party | P3, P5, P6, P9, P10, P12, P16, P21, P24, P27, P30 | *"I've connected **another app** called DietBet that's based on taking steps and losing weight, and I've connected Noom, which is like a tracking of meals and steps"* [P30]. |

During the discussion of privacy, participants seemed to be heavily concerned about secondary uses of their data, either by the device company or by connected third party apps. Examples of such uses, as provided by participants, include sharing with pharmaceutical, insurance, and sporting goods companies. Participants admitted that they do not read privacy policies and ToS agreements, and thus they were unaware if their information is

being shared for unintended purposes. With that being said, two participants shared similar thoughts that the Fitbit End User License Agreement (EULA) lacks transparency, and it needs to be made clearer and usable. In addition, two participants said now that Google owns Fitbit, they had concerns about targeted ads:

> *"I know that Google tracks a lot of information, and Fitbit is owned by Google now, so I feel that's one more way for them to track me and advertise to me"* [P21].

I then turned the discussion to the Fitbit sharing and privacy settings. More than half of the participants believed that Fitbit controls are straightforward. In other words, users have the option to share or not share their information. Yet, many of those participants indicted that they did not engage sufficiently with the Fitbit controls and features. A few of those participants, however, said that they would like to have more customization, such as controls to share certain data with close friends and primary doctors. P16 said *"there's no mix and match, like you can't say okay all of these people can have access to these features."* Another participant proposed two versions of the Fitbit setting: a basic and complex one. It is noteworthy, however, that the Fitbit app currently has an advanced, non-free version called "Fitbit Premium." Overall, customization seems to be a major issue for many participants as their dissatisfaction about Fitbit controls centered around granular sharing, which is also reflected by their designs that I introduce in the next section.

### 6.3.2 Co-design Sessions

In this section, I present participants' designs, focusing on the main features and themes. Table 13 conceptually categorizes these features. Note that one design might fall under more than one category. It is also noteworthy that Fitbit interfaces and features may be changed from time to time, and participants of this study may have used an older interface version or may not actually be aware of the existence of a particular feature.

Table 13: Summary of Features

| Category | Feature |
|---|---|
| Privacy | Granular controls |
| | Awareness and nudges |
| | Location privacy |
| | Prevent extended access |
| | Local storage and processing |
| Social Interaction | Customized audiences |
| | Trends and historical data |
| | Events |
| Considerations for health & fitness goals | Sharing with health providers |
| | Goal controls and features |
| | Tracking additional data |
| Clarity and consistency | Reduce information overload |
| | Prioritize tabs |
| | Direct controls |
| | Add/replace an icon |

#### 6.3.2.1 Privacy

**Granular controls—** The most common feature designed by participants are those related to granular sharing (appeared in 15 design sessions). A major limitation in the Fitbit privacy settings, as mentioned by participants, is that it does not allow the sharing of different information with different friends. Participants desired options to categorize audiences, such as close friends, people with similar fitness interests, and workmates, and then to choose which information they want to share with each category of audience.

Similarly, three design groups (G2, G5, & G6) proposed designs for granular sharing with authorized third-party apps. For example, G2 would like to set specific hours of the day where their data cannot be collected.

In addition, P3 wanted to show her friends how many steps she did per morning instead of having that shared per day or per week. P21, who has an office job, had a similar perspective. She is in a step competition with a friend who is standing and walking most of the day in a research laboratory.

To protect their identity and prevent any potential misuse of their personal information, G15 added the ability to challenges and the personal profile screen to pick an age range, (e.g., 20-30) instead of sharing the exact age. P30 explained: *"it would be fun to have a random challenger or the choice that you can pick someone within a certain age group, or gender, or activity level, but that's not giving away specific data that's personal to you. It's a range that you've agreed on."*

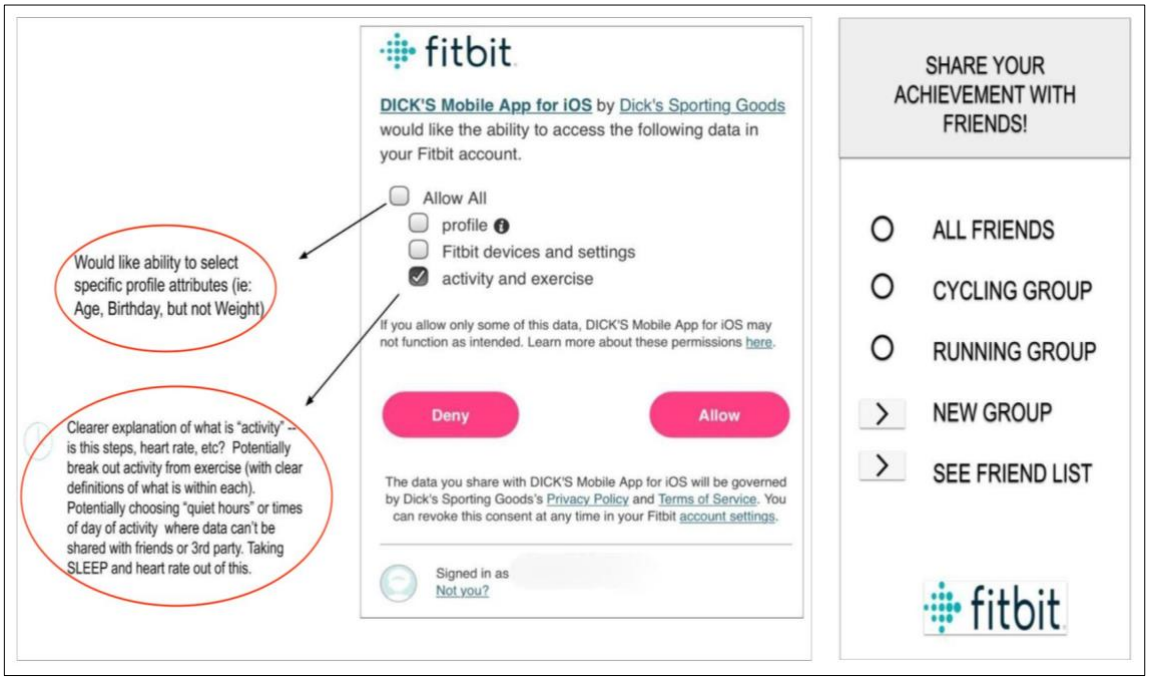



Figure 9: Customization

**Awareness and nudges—** Seven groups proposed privacy awareness and notification features. These features centered around three issues: third party access permission, usability and transparency of data practice statements, and profile access by other users.

First, participants wanted to be reminded of apps that they have given permission to for a long period of time and be asked if they still need to give access to these apps. P12 felt that it is weird that some third-party apps ask for access to certain data, and so she believed that they are likely using her information for other purposes. She commented: *"I'm sharing to an app that's like a step tracker app. Why do they need to see my heart rate and my sleep, right? If the whole thing this app is steps, why am I sharing all my activity and exercise? They are clearly doing something else with it."* In regard to transparency, G3, G7, and G11 were disappointed in the language that explains data practices by Fitbit, indicating that it is vague. For instance, participants demanded clarifications about what specific activity data an app needs to access, and whether they are still able to obtain a service if they did not grant full access to their data. In addition, several participants believed that Fitbit is limited in terms of privacy alerts. For instance, P15 said that he would like to receive notifications if another user accesses his profile, similar to LinkedIn notifications.

**Location privacy—** Fitbit enables users to share a map of their exercises with information, such as type of exercise, start and end points, and distance covered. Two groups (G1 & G14) felt that the way Fitbit users share this information is risky. G1 designed privacy zones to hide users' exact location when doing certain outdoor exercises, such as running and cycling. This group's design also aims to show other users, such as friends, live routes if they may be interested in joining them. G14's feature basically

depends on hiding certain information on the map while users are exercising, such as street names.

In addition to exercise routes, users have the option to share their location information (e.g., country state, and city) through their profile. Users may not be bothered to change their privacy settings after they start using the device, and thus several participants mentioned that location information should be private by default.

**Prevent extended access—** A few participants were uncomfortable about extended access (or increased access) when interacting with other users over the Fitbit platform. Extended access occurs when one user shares information, mainly posts, with another user, which can then be seen by other Fitbit users that are not friends of the first one. G7 proposed an icon that indicates that a user's comment and username are hidden. G2 designed an option to privately message and cheer other users.

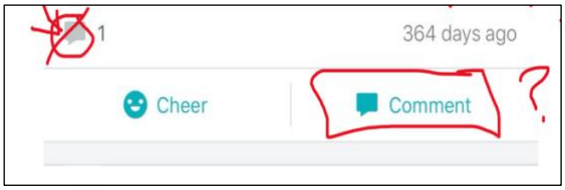



Figure 10: Marks Made by Participants about Privacy of Comments

**Local storage and processing—** Participants expressed an interest in keeping users' data locally as opposed to storing it in a remote server. According to P5, Fitbit users can record their sleep and other data which can be used as an indicator about sensitive information, such as mental health. He wished to have options to store self-tracking data locally; for example, on a user's phone or to have an option to keep data in the app without sending it to a remote server:

> *"There are certain things that you want to keep it to yourself, and you can do that without even storing it on the server, sort of using it on your*

*phone or on the app"* [P5].

### 6.3.2.2 Social Interaction

**Customized audiences—** Currently, the Fitbit sharing setting does not classify friends based on a particular relationship. Thus, six groups (G1, G2, G8, G11, G14, & G15) proposed features for sharing with selected audiences. While these features can help in preserving privacy, the main goal, as mentioned by participants, is to share with certain people that can help them to stay accountable towards their fitness objectives. For example, G1, G2, G11, G14, and G15 designed features to search for local or nearby Fitbit users (e.g., by determining an area within a 25 mile-radius or by using a zip code). P15 listed close friends as a subcategory of friends because he felt more comfortable to be motivated by close friends. It is noteworthy that Fitbit has the community feature, which enables users to create groups of Fitbit users. Yet, this feature cannot automatically categorize friends based on a relationship or location.

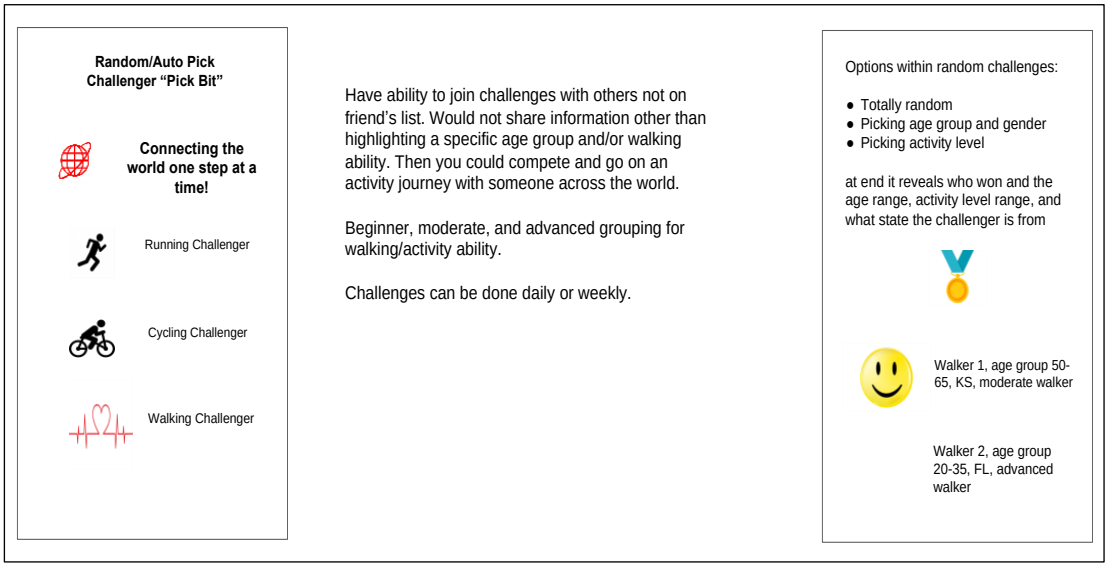



Figure 11: Features for Competitions

In addition, G15 was interested in a peer-to-peer (P2P) challenge with strangers. This group designed different options for the P2P challenge (Figure 11), that include picking a completely random challenger, picking a challenger with a customizable activity level or an activity level similar to that of a user, as well as a picking a challenger with certain demographics, such as of the same gender and age group.

**Trends & historical data—** Four groups (G2, G3, G10, & G11) stated that they would like to be able to track data over a particular period of time and then compare that with friends. Note that premium Fitbit users, however, already have the ability to track advanced data, including trends of their heart rate data and challenges. P5 broke data down based on a daily, weekly, and monthly basis (Figure 12). In addition, P3 stated that she would further want to see trends of her activity data based on certain hours of the day.

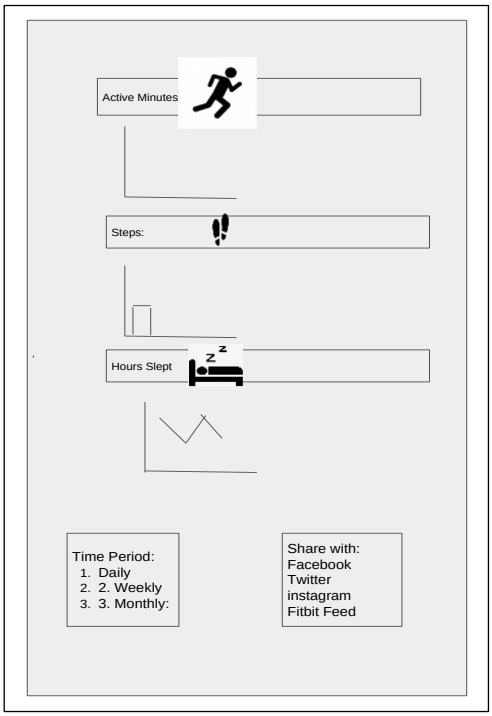



Figure 12: Feature Designed by a Group for Tracking and Analyzing Activity Trends

**Events—** Another feature mentioned is to promote social sharing by inviting other users and participating with them in events and discussions relevant to fitness. PD11 indicated that she would particularly be interested in events that match her fitness interests. She said *"I like events because you could probably do it at the different tiers. There could be community events, like my town does a lot of 5Ks, so things like that, or you could just invite your friends to a more private event."* This participant and her groupmate created an event interface that consists of several options, such as a search icon to find local events, as well as tabs to invite existing friends or to chat with other Fitbit users about certain events.

#### 6.3.2.3 Considerations of Different Health & Fitness Goals

**Sharing with health providers—** A common interest across five groups (G1, G8, G11, G12, & G14) was sharing self-tracking data with health providers. The goal of the participants is to gain a general view of their health, prevent chronic illness, and track specific information, such as fertility for female users. In addition, participants indicated that integrating this feature can be beneficial because it provides doctors with accurate and historical reports that can help them in their diagnosis and treatment. For instance, G11 designed features for analyzing heart rate and calorie information (Figure 13). This group also designed features to interact directly with doctors through comments, as well as a feature to alert users and advise them to seek help, such as in the case of high heart rate, which can be an indication of a stroke.

Participants had different perspective regarding how the health provider sharing feature could be implemented. G11's idea is that users will be taken into a third-party website, which can automatically pull-out patients' data from Fitbit. G12 proposed a similar

approach but with a PIN designated by doctors for security reasons, and users can then send specific data to their accounts in the providers' portal. G13 suggested that users click on an option (e.g., export for medical use) to receive a password protected link which can allow users to securely send their information to medical professionals.

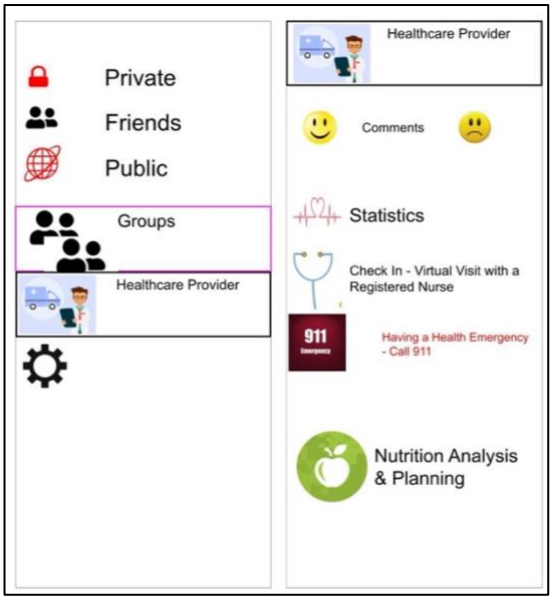



Figure 13: Interface for Sharing with Doctors

**Goal controls and features—** A few groups focused on designing controls and features that support their fitness goals with peers. For example, G11 proposed an independent interface for setting personal wellness goals, such as nutrition (Figure 14- right). Within this interface, the participants added a clock icon to set a particular goal and work towards achieving it with friends before a certain deadline. These participants also designed another interface and named it "Reminders" which aims to remind them about additional goals, such as water consumption per day (Figure 14- left). The Fitbit dashboard currently allows sharing information, including steps, miles, active minutes, and calories. However, G9 desired to display and share additional information in the dashboard, such as an average heart rate and sleep data.

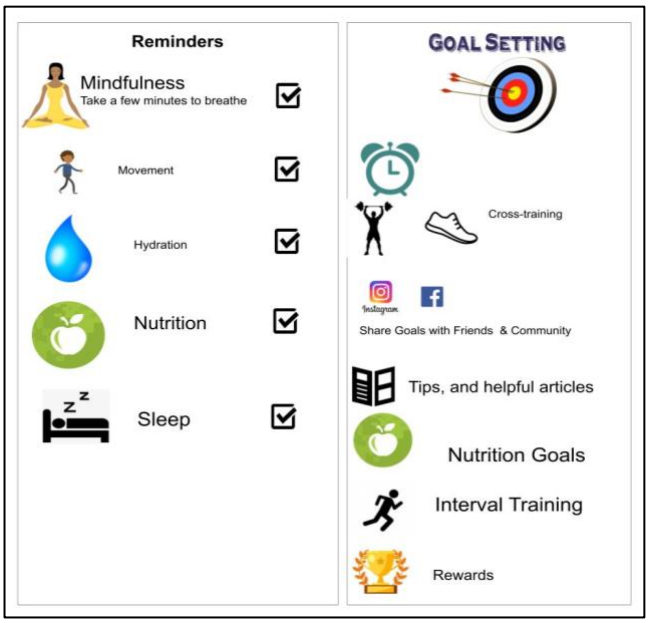



Figure 14: Feature with Different Options for Supporting Goals

A few participants raised a concern about not being able to attain a particular exercise goal when competing with peers, and thus they wanted flexible controls to change their exercise goals in a competition (e.g., 2 days/week). Participants also expressed a desire to track and share their progress in a competition, even if they could not hit the intended target. For example, P2 said that it would be interesting to allow competitors to see their progress, such as if one is in the top 20% of a particular competition. P16 proposed a similar idea— an option that provides detailed comparison of the activity data shared with friends and groups. This option shows a user rank among other people in terms of the age group and geographical location (Figure 15).

**Tracking additional information—** Groups also discussed data that may not currently be measured by Fitbit, which participants desire to be able to track and then share. P4 wished that Fitbit can tell if she is pregnant, she stated: *"There's one time I liked to tell somebody that I'm pregnant because it could maybe change what the expectations were,*

*and I could potentially send information to my doctor with heart rate and stuff, but there is no option to do that."* G2 and G11 added features that can help in reducing stress, such as dancing and yoga, and P5 wanted to be able to track mental health. Fitbit allows female users to track their menstrual cycle, but G13 wanted to be able to share this information with doctors only.

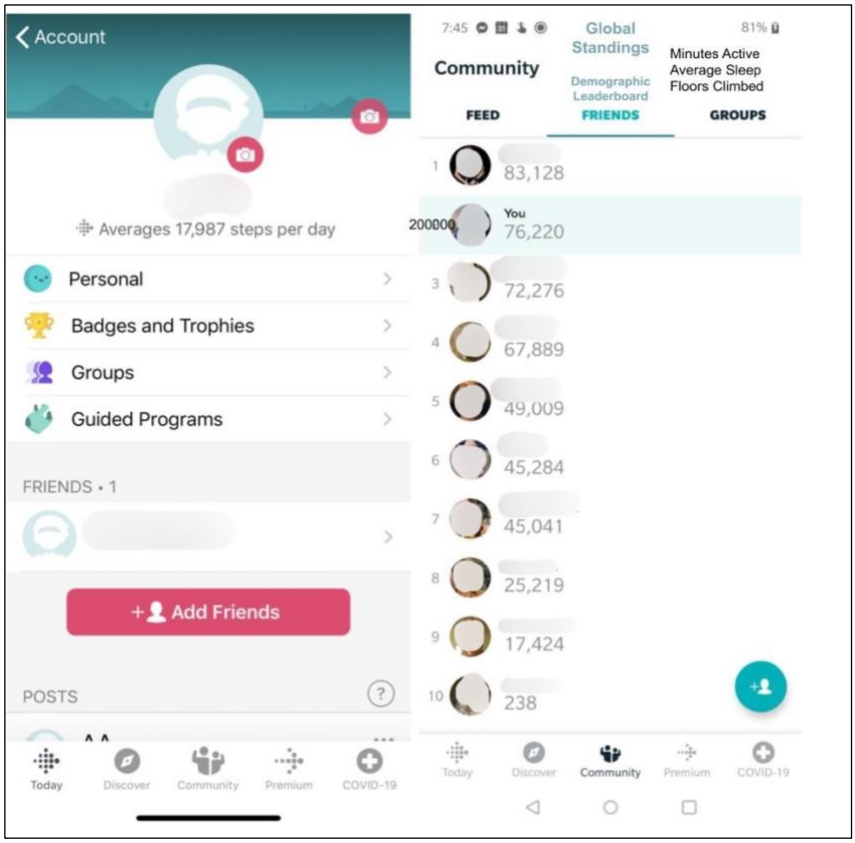



Figure 15: Feature for Comparing an Exercise Level Against Friends and Groups

#### 6.3.2.4 Clarity and Consistency

**Reduce information overload—** Several groups created designs to improve the privacy setting interface so users can easily manage the sharing and privacy of their information. According to G2 and G5, there is certain unnecessary information that can be visible to other Fitbit users, such as the number of participants in a group competition.

Thus, participants would like to be able to remove or hide such information. In addition, P13 felt that there is too much information in some of the setting screens, which can be distracting to users. He mentioned the "manage third party apps" interface as an example, indicating that there are too many links which can be confusing, especially when one is using the mobile app.

**Prioritize tabs—** Eight groups believed that certain Fitbit setting tabs need to be renamed and reordered based on their importance. For example, one of the issues commonly mentioned by participants is locating the privacy setting option, which is currently positioned under the "Social and Sharing" tab. P11 commented: *"I think it's a little misleading to have the privacy setting in the social and sharing, yeah, because that's not the first place when you're looking for privacy."* Similarly, P17 believes that the name of the tab can be misleading because it gives an indication that it is about sharing rather than hiding personal information. G10 broke social and sharing into "Social Media" (e.g., Facebook and Instagram) and "Privacy and Sharing," indicating that will make it easier and clearer for users to manage their sharing preferences. In addition, G7 and G9 indicated that tabs should be ordered based on their importance. Thus, they moved the privacy setting tab to the top and other options, such as "Shop Fitbit" to the bottom.

**Direct controls—** Three groups (G2, G6, & G13) found it easier to have controls directly placed next to each piece of data, instead of going to the setting options in a different interface. Due to the limited screen size, participants suggested that could be designed as a drill down menu (i.e., private, friends, public, etc.) Four other groups (G3, G4, G7, & G14) found it cumbersome to move from page to page in order to push a screenshot of their information to friends on social media sites, such as Facebook. Thus,

they proposed to list all the possible sharing recipients in the same interface. Currently, Fitbit does not allow users to share their information with multiple friends and groups in a single click, and participants found this inappropriate:

> *"You could only share to one at a time, that's silly… That's not something that I myself would want to have to do every time if I want to share a particular thing."* [P12].

**Add/replace an icon—** Lastly, a few participants proposed certain icons to represent some interface elements or to replace an existing icon. For example, P13 was concerned about the privacy of his comments posted on a friend's page (Figure 10). An option proposed by this participant's group is to add a lock as an indicator that a posted comment is hidden. Another participant proposed a magnify icon in the community interface to search friends by their actual name in addition to a username and an email.

## 6.4 Summary and Discussion

In this study, I used a participatory design approach, aiming to involve end-users in the design of sharing and privacy-related features and controls for fitness trackers. I used Fitbit as a case study because it is one of the most widely used fitness trackers with different sharing mechanisms. Participants' designs fall under at least one of four main aspects: privacy, social, clarity, and features for supporting specific health and fitness goals. Overall, many of the designs proposed by participants focused on supporting the need for granular sharing, thus suggesting that users indeed value the privacy of some of their fitness information. The ideas presented in this study can guide the design of sharing and privacy features and mechanisms. Next, I discuss the main themes and designs presented in each identified category.

**Privacy.** Some of the designs proposed by participants, such as privacy nudges, have been suggested in other domains, particularly in social media platforms. Yet, the value this study presents is insight and guidance about the desired privacy features when sharing fitness information that is collected by sensor devices. Participants' designs suggest that users sometimes want to disclose their fitness information to specific people based on their goals, which is consistent to the findings of other studies [23, 60]. Providing users fine-grained controls can encourage them to share while also allowing them to protect their privacy. These controls should be flexible enough to support different details of preferences; for instance, the ability to prevent the collection and sharing of information during certain times of a day. In addition, awareness features were also a common aspect proposed by several participants, which also confirms my findings in chapter 5 that fitness tracker interfaces lack privacy awareness features. Participants desired features that inform them not only about data practices of a device manufacturer and third parties, but also when other users access their information (e.g., browsing profile information). Participants' designs also covered other privacy-related aspects, including location protection and extended access prevention. Participants indicated that they may want to hide (e.g., blur) certain location points displayed on an exercise map and to hide their comments on friend's post from other users. Designers are recommended to take these considerations into account.

**Social Interactions.** Participants' designs covered different sharing features for supporting different personal fitness goals, such as customized audiences, which can also be relevant to privacy. One of the designs proposed by a group was to enable users to compete with other users with similar characteristics (e.g., users of a specific age group

and activity level). These features are valued because users differ in terms of their overall fitness level and their ability to exercise regularly. In addition, social influence is a powerful factor to keep users accountable towards healthy practices. Therefore, integrating features such as communities and events related to different fitness interests of users can leverage social interactions. However, as such features can encourage users to share their information, privacy risks are likely to increase.

**Considerations for different health and fitness goals.** Wearable devices help users collect different health information that support their goals. This self-tracking information can provide rich insights into a person's health and can be complementary to clinical diagnoses. Participants strongly desire to be able to share self-tracking data with their doctors; yet my analysis of sharing patterns in chapter 5 reveals that Fitbit and many other fitness trackers do not seem to support this option. Wearable device manufacturers and designers are encouraged to integrate this feature and include options, such as exporting self-tracking data, checking symptoms, and setting virtual appointments with doctors. However, participants stressed that they want such information to be shared with doctors only and want to be able to share specific information based on their goals. Thus, designers should also ensure that authentication and authorization controls are in place to eliminate any concerns by users.

**Clarity and consistency.** Preece et al. stated *"when functions are "out of sight," it makes them more difficult to find and know how to use"* [61, p.21]. Several participants were dissatisfied about how the settings were named and structured, which makes it difficult to find certain setting's options. The privacy setting tab is an example, which is placed under social and sharing, and participants found that counter-intuitive because

sharing is actually part of privacy. This raises a question by a few participants regarding whether a company pays sufficient attention to the privacy aspects of their fitness information, and many participants in this study considered it private information. A few participants said that they were unsure if some of their information is accessible to other users and companies.

# CHAPTER 7: DISCUSSION, DESIGN GUIDELINES, AND CONCLUSION

In this dissertation, I explored a variety of sharing and privacy-related issues about personal information in the context of fitness tracking wearables. One important contribution this research presents is a set of sharing patterns by fitness tracker users. I uncovered different practices users do within each pattern. For instance, a common practice by users when competing with friends was to utilize broader social media applications to share their information. Additionally, this research shows that users' comfort of sharing information in each pattern can differ depending on the audience. As such, this research also contributes to the related work by providing a comparison of users' preferences for sharing a set of fitness tracker data against a comprehensive list of audiences (section 4.3.2.3). Overall, users are comfortable sharing many types of data with their family, friends, and significant others and were less comfortable sharing with third parties.

However, I also showed that fitness tracker platforms may not support some of these sharing patterns. This can be disappointing for users because they may want to share information with specific audiences who can push them to pursue their health and fitness goals. Consequently, a considerable number of people recruited in this research reported disclosing their information on different external services, such as Strava, to meet desired goals that were not supported by their device's platform.

Although sharing in these patterns can support users' health and fitness goals, it also imposes privacy risks. I discussed some of these risks through several examples, including stalking, repurposing, and inferences. With that in mind, it is important to understand users' concerns as well as their awareness of these potential privacy risks. Clearly, individual's concerns and awareness of privacy problems can be impacted by common factors, such as

technology expertise. However, concerns and behaviors of individuals regarding privacy issues in health technologies were also assumed to be associated with their awareness of these issues [34]. My research examined users' concerns about the sharing of information collected by wearable fitness trackers. Participants in this research, overall, had different views about the privacy of fitness tracker information. While many people did not consider much of the fitness tracker information sensitive, and thus were unworried about it, others raised concerns. I found that users' concerns were primarily about sharing norms and self-presentation goals, which drive users' choices in what information to share and with whom. I discussed these two aspects in the light of the Contextual Integrity theory, indicating that users' privacy decisions vary based on the audience and platform used.

Yet, several participants in this research who cited examples of privacy risks seemed to be uncertain about how exactly their data could be used against them. Wearable fitness devices often consist of different embedded sensors to capture data about users and the context. This opens the door for further investigations about users' awareness of privacy issues known to be associated with these sensor devices, such as data inferences. I examined users' awareness about potential inferences through qualitative and quantitative studies that present users with several different scenarios. My findings present additional evidence to the related research that users lack awareness about the potential to infer personal information from the primary data collected by personal fitness trackers.

More importantly, this research presented several factors that explain users' perceptions towards inferences in IoT fitness trackers. First, the perception that certain inferences are unlikely to happen can potentially mitigate users' concerns. However, I argue that past incidents, especially those that are reported in the media, may change users' privacy

behaviors. Another implication this research presents is that people's reaction to inferences can be influenced by the accuracy of data recorded or generated by sensor devices. Those who were comfortable with inferences found an accurate inference helpful for them to track specific goals. In contrast, those who were uncomfortable believed that inaccurate inferences could provide negative impressions about them. My findings from both the interview and survey study in chapter 6 showed that data anonymization is a factor significantly associated with users' comfort with inferences. Users do not want their data collected by fitness trackers to be linked to their identity. However, many people in my research were unsure if their information is actually anonymized. Echoing privacy research in other domains, this research's findings also suggest that users can be less uncomfortable about certain inferences if a perceived benefit is involved. Discounts received from pharmacies and health insurance companies are an example, where users can be willing to disclose their personal fitness data. Awareness tools that demonstrate potential risks of inferences could change user's comfort regarding this trade-off. Lastly, this research also revealed that informed consent and trust in a device company are other factors that could impact users' acceptance of certain inferences. Clear notices can make users confident that their information will not be abused and increases their trust level.

I believe that many of the privacy issues addressed throughout this research can be tackled by empowering users to control their information. One way to provide users this control is to support them in making informed privacy decisions, which means transparent privacy policies. Presenting a privacy policy in wearable devices is a challenge because these devices are small with often no means to input data. Traditional privacy policies may not be effective to communicate data practices to users. However, in the case of fitness

wearables, Gluck et al., [24] noted that functions regularly seen by users, such the increase in step count as users move, are part of data collection practices by a device, which may increase users' awareness about such practices. Therefore, policies should focus on practices that users may not be familiar with [24]. Such a mechanism may not assure the protection of users, but it provides a higher chance to increase their awareness. In addition to policies, there should be clear and updated regulations that can respond to the continuing advancements in the data collection capability of wearable devices. This research still urges regulators to keep up with these changes.

Similar to privacy policies, interface mechanisms, such as privacy cues and nudges, can help users in understanding what might be collected about them. My exploration of the sharing and privacy mechanisms of the common fitness tracker platforms in chapter 5 indicated a lack of implementation of these mechanisms. There are different ways to include awareness nudges and cues in the interface. Awareness mechanisms could be related to users' sharing patterns (e.g., sharing with third party apps) and should focus on what sensitive information could be accessed. As I have previously argued, certain interface cues, while considered simple, can potentially change privacy behaviors; e.g., showing users, in real-time, how data impacts other data, such as heart rate variability and walking.

Privacy settings are a powerful tool to provide users control over their information. Yet, many participants recruited in this research reported not taking advantage of their settings. This is due to the limited sharing options in the settings or because of the perspective held by many people that much of the fitness information is insensitive. Nevertheless, my findings from the user studies also uncovered a wider variety of sharing preferences. The

participatory design study I conducted with Fitbit users demonstrates this finding as many of the participants' designs focused on controls for sharing different information with different types of audiences.

## 7.1 Design Guidelines

Based on the different lessons learned throughout this dissertation, I propose specific design guidelines:

- Provide users **clear, concise, and transparent notices**. These notices should focus on the information that users need to know in order to make the correct decision. For example, if the data is shared with third parties, what data will be shared exactly, with whom it will be shared, to what extent users' information is anonymized, and what will happen to this information if users opt out.
- Provide **real-time and contextual feedback**. This includes visual cues that motivate users to reason about the possible privacy risks of their sharing practices during real-time interaction with a device, as well as mechanisms that nudge users to rethink their disclosure decisions with third party apps.
- Support **granular sharing of data and recipients**. Users should be able to choose pieces of information to share with specific audiences rather than general categories.
- Design mechanisms that support the **norms** of sharing fitness-related information with different audiences on different platforms.
- Provide users more **flexibility over data collection**. Users should be able to choose what and when data can be collected.

- Provide mechanisms to **integrate self-tracking data with a health provider's system**. Design features that facilitate users' interaction with health professionals.
- Make **"private" the default option**. Users may not change their controls after starting to use a device. Thus, default options should be the options that protect users' information.
- **Prevent any chance of extended or indirect access**. Users should be able to hide their information, such as their connections, from unintended recipients.
- **Protect sensitive and personally identifiable information**. Notify users when sensitive information is being accessed and recommend actions to prevent or mitigate the potential risks. Provide features that support anonymity and prevent aggregation of data.
- **Support the different interpersonal boundary controls**. This includes controls, such as hiding data, deleting posts, disabling friendship requests, and blocking users.
- Allow **local storage and processing**, if possible.
- Make important **settings options**, such as privacy settings, **visible** to users and easy to change.
- Allow users to track and share trends of their activity data.

## 7.2 Future Research

One of the key insights this dissertation presents is that users' awareness about potential privacy risks associated with the collection and sharing of sensed fitness data is limited. This raises an important issue for investigating the factors and mechanisms that might

improve users' awareness. My studies uncovered some factors based on users' responses. My findings suggest that users who experienced a risk or were aware of previous privacy incidents in fitness trackers may have a better understanding of related privacy issues. Future research could investigate the impact of this issue on users' awareness, as well as how could that impact users' concerns and protective actions. In addition, researchers have been advocating that visual cues and nudges in the interface can improve users' awareness, and thus help users in their decision making. Yet, there is limited research that examines visual cues and nudges in terms of wearable fitness device's interfaces. Furthermore, privacy notices, while generally ignored, remain the main method to learn about data collection practices at this time. Previous studies (e.g.,[58]) analyzed privacy policies of fitness tracker companies to gain an insight into these companies' practices to protect users' information. There is a need to investigate these practices from the end-users' perspective to examine the extent to which these practices align with users' expectations.

This research examined users' concerns about the sharing of fitness tracker information. However, participants recruited in this dissertation's user studies are not representative of a particular cohort of users. In the future, investigating concerns of users from particular user groups or cultures that are not well represented (e.g., elderly) would enrich the understanding related to privacy issues concerning the sharing of information in these ubiquitous devices.

## 7.3 Conclusion

Technology has been shifting our lifestyle. With the use of wearable devices, individuals can easily collect and track a variety of information related to their health and wellbeing, including physical activity, diet and weight, and chronic diseases. Sharing this information

with different audiences by users is now normal practice, in order to better support their health and fitness goals. Yet, the collection of large amounts of personal information by sensor devices and the sharing of it can expose users to privacy threats that users may not be aware of. This requires a clear understanding of users in order to design effective controls and features that help in protecting users' privacy while also supporting their health and fitness goals.

Through this dissertation, I investigated various sharing and privacy aspects of information in fitness trackers. I expanded previous related work by describing more sharing patterns by users in this domain. I found different sharing considerations for types of information and audiences with specific practices. My research also developed an increased understanding of users' perceptions and attitudes regarding inferences associated with sensor devices that collect fitness data. I developed a set of taxonomies for sharing and privacy controls and mechanisms in fitness tracker platforms and identified several design needs. My research also empowered end-users by directly involving them in the design of sharing and privacy controls and features. Finally, my research proposes a set of design guidelines for supporting sharing and protecting information in these ubiquitous devices. I hope that the increased understanding presented in this research, combined with the analysis of the different interfaces and the design ideas, pave the way for building effective sharing and privacy solutions in wearable fitness devices.

# REFERENCES

[1] Fitbit, “Fitbit.” https://healthsolutions.fitbit.com/employers/ (accessed Oct. 28, 2019).

[2] Polar.com. https://www.polar.com/us-en/b2b_products/corporate_fitness (accessed May 16, 2020).

[3] Samsung.com. https://www.samsung.com/uk/support/mobile-devices/what-is-samsung-health-ask-an-expert-powered-by-babylon/ (accessed Jun. 04, 2020).

[4] A. Act, “Health insurance portability and accountability act of 1996.” p. 191, 1996.

[5] G. Addonizio, “The privacy risks surrounding consumer health and fitness apps, associated wearable devices, and HIPAA’s limitations,” Law Sch. Student Scholarsh., no. Paper 827, 2016.

[6] C. Aiello, “Under Armour says data breach affected about 150 million MyFitnessPal accounts,” 2018. https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html (accessed Feb. 19, 2019).

[7] A. Aktypi, J. R. C. Nurse, and M. Goldsmith, “Unwinding Ariadne’s identity thread: Privacy risks with fitness trackers and Online Social Networks,” in MPS 2017 - Proceedings of the 2017 Workshop on Multimedia Privacy and Security, co-located with CCS 2017, Oct. 2017, vol. 2017-January, pp. 1–11, doi: 10.1145/3137616.3137617.

[8] H. Almuhimedi et al., “Your location has been shared 5,398 times! A field study on mobile app privacy nudging,” in Conference on Human Factors in Computing Systems - Proceedings, Apr. 2015, vol. 2015-April, pp. 787–796, doi: 10.1145/2702123.2702210.

[9] A. Alqhatani and H. R. Lipford, “‘There is nothing that I need to keep secret’: Sharing practices and concerns of wearable fitness data,” Proc. 15th Symp. Usable Priv. Secur. SOUPS 2019, pp. 421–434, 2019.

[10] A. Alqhatani and H. R. Lipford, “Exploring the Design Space of Sharing and Privacy Mechanisms in Wearable Fitness Platforms,” Workshop on Usable Security and

Privacy (USEC), 7 May 2021, Aukland, New Zealand, doi: 10.14722/usec.2021.23009.

[11] I. Altman, “Privacy Regulation: Culturally Universal or Culturally Specific?,” J. Soc. Issues, vol. 33, no. 3, pp. 66–84, 1977, doi: 10.1111/j.1540-4560.1977.tb01883.x.

[12] P. Bahirat, Y. He, A. Menon, and B. Knijnenburg, “A data-driven approach to developing IoT privacy-setting interfaces,” Int. Conf. Intell. User Interfaces, Proc. IUI, pp. 165–176, 2018, doi: 10.1145/3172944.3172982.

[13] M. Becker, “Understanding Users’ Health Information Privacy Concerns for Health Wearables,” Proc. 51st Hawaii Int. Conf. Syst. Sci., vol. 9, pp. 3261–3270, 2018, doi: 10.24251/hicss.2018.413.

[14] I. Bilogrevic and M. Ortlieb, “‘If you put all the pieces together...’ - Attitudes towards data combination and sharing across services and companies,” Conf. Hum. Factors Comput. Syst. - Proc., pp. 5215–5227, 2016, doi: 10.1145/2858036.2858432.

[15] R. Bosua, K. Clark, M. Richardson, and J. E. B. Webb, “Intelligent Warning Systems: ’ Technological Nudges ’ to En- hance User Control of IoT Data Collection , Storage and Use,” Good Data, pp. 420–429, 2010.

[16] M. Christovich, “Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information,” Hast. Commun. Entertain. Law J., vol. 38, no. 1, p. 91, 2015.

[17] S. Chung, C. F., Gorm, N., Shklovski, I. A., & Munson, “Finding the right fit: understanding health tracking in workplace wellness programs,” in In Proceedings of the 2017 CHI conference on human factors in computing systems, 2017, vol. 49, no. 7, pp. 4875–4886.

[18] C. Dolin et al., “Unpacking perceptions of data-driven inferences underlying online targeting and personalization,” Conf. Hum. Factors Comput. Syst. - Proc., vol. 2018-April, pp. 1–12, 2018, doi: 10.1145/3173574.3174067.

[19] M. Dong, L. Chen, and L. Wang, “Investigating the User Behaviors of Sharing Health- and Fitness-Related Information Generated by Mi Band on Weibo,” Int. J. Hum.

Comput. Interact., vol. 35, no. 9, pp. 773–786, 2019, doi: 10.1080/10447318.2018.1496968.

[20] S. Egelman, R. Kannavara, and R. Chow, “Is this thing on? : Crowdsourcing privacy indicators for ubiquitous sensing platforms,” Conf. Hum. Factors Comput. Syst. - Proc., vol. 2015-April, pp. 1669–1678, 2015, doi: 10.1145/2702123.2702251.

[21] D. A. Epstein, B. H. Jacobson, E. Bales, D. W. McDonald, and S. A. Munson, “From ‘nobody cares’ to ‘way to go!’: A Design Framework for Social Sharing in Personal Informatics,” pp. 1622–1636, 2015, doi: 10.1145/2675133.2675135.

[22] T. Fritz, E. M. Huang, G. C. Murphy, and T. Zimmermann, “Persuasive technology in the real world: A study of long-term use of activity sensing devices for fitness,” Conf. Hum. Factors Comput. Syst. - Proc., no. April, pp. 487–496, 2014, doi: 10.1145/2556288.2557383.

[23] S. Gabriele and S. Chiasson, “Understanding Fitness Tracker Users’ Security and Privacy Knowledge, Attitudes and Behaviours,” in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1–12, doi: 10.1145/3313831.3376651.

[24] J. Gluck et al., “How Short Is Too Short ? Implications of Length and Framing on the Effectiveness of Privacy Notices This paper is included in the Proceedings of the Implications of Length and Framing on the Effectiveness of Privacy Notices,” Symp. Usable Priv. Secur., no. Soups, pp. 321–340, 2016.

[25] N. Gorm and I. Shklovski, “Sharing steps in the workplace: Changing privacy concerns over time,” in Conference on Human Factors in Computing Systems - Proceedings, May 2016, pp. 4315–4319, doi: 10.1145/2858036.2858352.

[26] N. Gorm and I. Shklovski, “Steps, choices and moral accounting: Observations from a step-counting campaign in the workplace,” Proc. ACM Conf. Comput. Support. Coop. Work. CSCW, vol. 27, pp. 148–159, 2016, doi: 10.1145/2818048.2819944.

[27] G. Gsenger, R., Human, S. and Neumann, “End-user Empowerment: An Interdisciplinary Perspective,” 2020.

[28] X. Gui, Y. Chen, C. Caldeira, D. Xiao, and Y. Chen, “When fitness meets social networks: Investigating fitness tracking and social practices on WeRun,” Conf. Hum. Factors Comput. Syst. - Proc., vol. 2017-May, no. October, pp. 1647–1659, 2017, doi: 10.1145/3025453.3025654.

[29] M. Haghi, K. Thurow, and R. Stoll, “Wearable devices in medical internet of things: Scientific research and commercially available devices,” Healthc. Inform. Res., vol. 23, no. 1, pp. 4–15, 2017, doi: 10.4258/hir.2017.23.1.4.

[30] S. Hautea, A. Munasinghe, and E. Rader, “‘That’s Not Me’: Surprising Algorithmic Inferences,” in Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1–7, doi: 10.1145/3334480.3382816.

[31] A. Hern, “Fitness tracking app Strava gives away location of secret US army bases,” The Guardian, 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (accessed May 10, 2020).

[32] CCS Insight, 2018. Success of Apple Watch Means More Growth in Sales of Wearable Technology - CCS Insight. https://www.ccsinsight.com/press/company-news/3695-success-of-apple-watch-means-more-growth-in-sales-of-wearable-technology/ (accessed Apr. 20, 2019).

[33] A. Jackson, “Couple never expected their Fitbit would tell them this ... - CNN,” CCN Health, 2016. https://www.cnn.com/2016/02/10/health/fitbit-reddit-pregnancy-irpt/index.html (accessed May 10, 2020).

[34] G. Kenny and R. Connolly, “Drivers of health information privacy concern: A comparison study,” AMCIS 2016 Surfing IT Innov. Wave - 22nd Am. Conf. Inf. Syst., no. August 2016, 2016.

[35] P. Klasnja, S. Consolvo, T. Choudhury, R. Beckwith, and J. Hightower, “Exploring privacy concerns about personal sensing,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5538 LNCS, pp. 176–183, 2009, doi: 10.1007/978-3-642-01516-8_13.

[36] D. S. C. Kreitzberg, S. L. Dailey, T. M. Vogt, D. Robinson, and Y. Zhu, “What is your fitness tracker communicating?: Exploring messages and effects of wearable fitness

devices," Qual. Res. Reports Commun., vol. 17, no. 1, pp. 93–101, 2016, doi: 10.1080/17459435.2016.1220418.

[37] J. Kröger, "Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things," in IFIP Advances in Information and Communication Technology, Sep. 2018, vol. 548, pp. 147–159, doi: 10.1007/978-3-030-15651-0_13.

[38] J. L. Kröger, P. Raschke, and T. R. Bhuiyan, "Privacy implications of accelerometer data: A review of possible inferences," ACM Int. Conf. Proceeding Ser., pp. 81–87, 2019, doi: 10.1145/3309074.3309076.

[39] P. Lamkin, "Wearable Tech Market To Be Worth $34 Billion By 2020," 2016. https://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/?sh=17e5f71e3cb5 (accessed Nov. 08, 2018).

[40] A. Lampinen, "Interpersonal Boundary Regulation in the Context of Social Network Services." 2014.

[41] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," Int. J. Med. Inform., vol. 88, no. 555, pp. 8–17, 2016, doi: 10.1016/j.ijmedinf.2015.12.010.

[42] C. Lidynia, P. Brauner, and M. Ziefle, "A step in the right direction – understanding privacy concerns and perceived sensitivity of fitness trackers," Adv. Intell. Syst. Comput., vol. 608, pp. 42–53, 2018, doi: 10.1007/978-3-319-60639-2_5.

[43] B. Liu *et al.*, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016, pp. 27–41.

[44] B. Lowens, V. G. Motti, and K. Caine, "Wearable Privacy: Skeletons in the Data Closet," Proc. - 2017 IEEE Int. Conf. Healthc. Informatics, ICHI 2017, pp. 295–304, 2017, doi: 10.1109/ICHI.2017.29.

[45] D. Lupton, "Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps," *Cult. Health Sex.*, vol. 17, no. 4, pp. 440–453, 2015.

[46] D. Lupton, “Quantifying the body: Monitoring and measuring health in the age of mHealth technologies,” Crit. Public Health, vol. 23, no. 4, pp. 393–403, 2013, doi: 10.1080/09581596.2013.794931.

[47] S. Mare, L. Girvin, F. Roesner, and T. Kohno, “Consumer smart homes: Where we are and where we need to go,” HotMobile 2019 - Proc. 20th Int. Work. Mob. Comput. Syst. Appl., pp. 117–122, 2019, doi: 10.1145/3301293.3302371.

[48] Ü. Meteriz, N. F. Yıldıran, and A. Mohaisen, “You Can Run, But You Cannot Hide: Using Elevation Profiles to Breach Location Privacy through Trajectory Prediction,” Oct. 2019, [Online]. Available: http://arxiv.org/abs/1910.09041.

[49] V. G. Motti and K. Caine, “Users’ privacy concerns about wearables: Impact of form factor, sensors and type of data collected,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 8976, pp. 231–244, doi: 10.1007/978-3-662-48051-9_17.

[50] M. J. Muller and S. Kuhn, “Participatory design,” *Commun. ACM*, vol. 36, no. 6, pp. 24–28, 1993.

[51] S. Munson and S. Consolvo, “Exploring Goal-setting, Rewards, Self-monitoring, and Sharing to Motivate Physical Activity,” in 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2012, pp. 25–32.

[52] P. E. Naeini *et al.*, “Privacy expectations and preferences in an IoT world,” in *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, 2017, pp. 399–412.

[53] M. W. Newman, D. Lauterbach, S. A. Munson, P. Resnick, and M. E. Morris, “It’s not that i don’t have problems, i’m just not putting them on facebook: Challenges and opportunities in using online social networks for health,” Proc. ACM Conf. Comput. Support. Coop. Work. CSCW, no. May, pp. 341–350, 2011, doi: 10.1145/1958824.1958876.

[54] H. Nissenbaum, “Privacy As Contextual Integrity,” Washingt. Law Rev. Assoc., vol. 119, 2004.

[55] J. Ojala, “Personal content in online sports communities: motivations to capture and share personal exercise data,” Int. J. Soc. Humanist. Comput., vol. 2, no. 1/2, p. 68, 2013, doi: 10.1504/ijshc.2013.053267.

[56] A. Pai, “Garmin offerse mployers wellness portal, health challenges Garmin,” 2015. https://www.mobihealthnews.com/39362/garmin-offers-employers-wellness-portal-health-challenges (accessed Jun. 01, 2020).

[57] K. Park, I. Weber, M. Cha, and C. Lee, “Persistent sharing of fitness app status on twitter,” Proc. ACM Conf. Comput. Support. Coop. Work. CSCW, vol. 27, pp. 184–194, 2016, doi: 10.1145/2818048.2819921.

[58] G. Paul and J. Irvine, “Privacy implications of wearable health devices,” ACM Int. Conf. Proceeding Ser., vol. 2014-Septe, pp. 117–121, 2014, doi: 10.1145/2659651.2659683.

[59] S. R. Peppet, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 TEX,” 2014. [Online]. Available: https://scholar.law.colorado.edu/articles/83.

[60] A. Prasad, J. Sorber, T. Stablein, D. L. Anthony, and D. Kotz, “Understanding User Privacy Preferences for mHealth Data Sharing,” mHealth Multidiscip. Verticals, pp. 279–296, 2014, doi: 10.1201/b17724-17.

[61] J. Preece, Y. Rogers, and H. Sharpe, “Interaction Design: Beyond Human-Computer Interaction.” John Wiley & Sons, 2002.

[62] A. Pressman, “Apple Took a Commanding Lead In Wearables Fourth Quarter, As Fitbit Slipped.” (March 1 2018). Retrieved October 28, 2018 from http://fortune.com/2018/03/01/applewatch-fitbit-wearable-ranking/ (accessed Oct. 28, 2018).

[63] E. Rader, “Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google,” Symp. Usable Priv. Secur., pp. 51–67, 2014, [Online]. Available: http://bierdoctor.com/papers/rader_privacy_soups14_final.pdf.

[64] E. Rader, S. Hautea, A. Munasinghe, “‘ I Have a Narrow Thought Process ’: Constraints on Explanations Connecting Inferences and Self-Perceptions,” in Sixteenth Symposium on Usable Privacy and Security ($\{$SOUPS$\}$ 2020), 2020, pp. 457--488.

[65] E. Rader and J. Slaker, “The importance of visibility for folk theories of sensor data this paper is included in the proceedings of the the importance of visibility for folk theories of sensor data,” Proc. Thirteen. Symp. Usable Priv. Secur., no. Soups, pp. 257–270, 2017.

[66] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava, “Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment,” Conf. Hum. Factors Comput. Syst. - Proc., pp. 11–20, 2011, doi: 10.1145/1978942.1978945.

[67] A. Railean and D. Reinhardt, “Let there be LITE: Design and evaluation of a label for IoT transparency enhancement,” in MobileHCI 2018 - Beyond Mobile: The Next 20 Years - 20th International Conference on Human-Computer Interaction with Mobile Devices and Services, Conference Proceedings Adjunct, 2018, pp. 103–110, doi: 10.1145/3236112.3236126.

[68] L. Rao, “Sexual Activity Tracked By Fitbit Shows Up In Google Search Results | TechCrunch,” TechCrunch, 2011. https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/ (accessed May 13, 2020).

[69] C. Russey, “Wearables Market to grow to $27 Billion in 2022 | Wearable Technologies,” Wearable Technologies, 2018. https://www.wearable-technologies.com/2018/11/wearables-market-to-grow-to-27-billion-with-137-million-units-sold-in-2022/ (accessed Apr. 22, 2019).

[70] S. Schneegass, R. Poguntke, and T. Machulla, “Understanding the impact of information representation on willingness to share information,” Conf. Hum. Factors Comput. Syst. - Proc., 2019, doi: 10.1145/3290605.3300753.

[71] S. Seneviratne et al., “A Survey of Wearable Devices and Challenges,” IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 2573–2620, 2017, doi: 10.1109/COMST.2017.2731979.

[72] L. Sly, “U.S. soldiers are revealing sensitive and dangerous information by jogging,” 2018. https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-

doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html. (accessed Oct. 26, 2018).

[73] H. J. Smith and T. Dinev, “Information privacy research: an interdisciplinary review,” MIS Q., vol. 35, no. 4, pp. 989–1015, 2011.

[74] J. Stragier, T. Evens, and P. Mechant, “Broadcast yourself: An exploratory study of sharing physical activity on social networking sites,” Media Int. Aust., no. 155, pp. 120–129, 2015, doi: 10.1177/1329878x1515500114.

[75] Q. Tang, D. J. Vidrine, E. Crowder, and S. S. Intille, “Automated detection of puffing and smoking with wrist accelerometers,” Proc. - PERVASIVEHEALTH 2014 8th Int. Conf. Pervasive Comput. Technol. Healthc., pp. 80–87, 2014, doi: 10.4108/icst.pervasivehealth.2014.254978.

[76] R. Teodoro and M. Naaman, “Fitter with Twitter: Understanding personal health and fitness activity in social media,” Proc. 7th Int. Conf. Weblogs Soc. Media, ICWSM 2013, pp. 611–620, 2013.

[77] E. Thomaz, I. Essa, and G. D. Abowd, “A practical approach for recognizing eating moments with wrist-mounted inertial sensing,” UbiComp 2015 - Proc. 2015 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput., pp. 1029–1040, 2015, doi: 10.1145/2750858.2807545.

[78] I. Torre, O. R. Sanchez, F. Koceva, and G. Adorni, “Supporting users to take informed decisions on privacy settings of personal devices,” Pers. Ubiquitous Comput., vol. 22, no. 2, pp. 345–364, 2018, doi: 10.1007/s00779-017-1068-3.

[79] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, “Smart, useful, scary, creepy: Perceptions of online behavioral advertising,” SOUPS 2012 - Proc. 8th Symp. Usable Priv. Secur., vol. 2012, 2012, doi: 10.1145/2335356.2335362.

[80] J. Vitak, Y. Liao, P. Kumar, M. Zimmer, and K. Kritikos, “Privacy attitudes and data valuation among fitness tracker users,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10766 LNCS, pp. 229–239, 2018, doi: 10.1007/978-3-319-78105-1_27.

[81] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh, “A field trial of privacy nudges for facebook,” Conf. Hum. Factors Comput. Syst. - Proc., pp. 2367–2376, 2014, doi: 10.1145/2556288.2557413.

[82] T. Yan, Y. Lu, and N. Zhang, “Privacy Disclosure from Wearable Devices,” pp. 13–18, 2015, doi: 10.1145/2757302.2757306.

[83] X. Zhao, C. Lampe, and N. B. Ellison, “The social media ecology: User perceptions, strategies and challenges,” Conf. Hum. Factors Comput. Syst. - Proc., pp. 89–100, 2016, doi: 10.1145/2858036.2858333.

[84] Y. Zhu, S. L. Dailey, D. Kreitzberg, and J. Bernhardt, “‘Social Networkout’: Connecting Social Features of Wearable Fitness Trackers with Physical Exercise,” J. Health Commun., vol. 22, no. 12, pp. 974–980, 2017, doi: 10.1080/10810730.2017.1382617.

[85] I. Wagner, Y. He, D. Rosenberg, and H. Janicke, “User interface design for privacy awareness in eHealth technologies,” in 2016 13th IEEE Annual Consumer Communications and Networking Conference, CCNC 2016, Mar. 2016, pp. 38–43, doi: 10.1109/CCNC.2016.7444728.

[86] J. Warshaw, N. Taft, and A. Woodruff, “Intuitions, analytics, and killing ants: Inference Literacy of High School-educated Adults in the US,” SOUPS 2016 - 12th Symp. Usable Priv. Secur., no. Soups, pp. 271–285, 2019.

[87] B. Weinshel et al., “Oh, the places you’ve been! User reactions to longitudinal transparency about third-party web tracking and inferencing,” Proc. ACM Conf. Comput. Commun. Secur., pp. 149–166, 2019, doi: 10.1145/3319535.3363200.

[88] M. Williams, J. R. C. Nurse, and S. Creese, “(Smart)Watch Out! Encouraging Privacy-Protective Behavior through Interactive Games,” 2018. [Online]. Available: http://kar.kent.ac.uk/contact.html.

[89] P. Wisniewski, D. C. Wilson, and H. Richter-Lipford, “A new social order: Mechanisms for social network site boundary regulation,” 17th Am. Conf. Inf. Syst. 2011, AMCIS 2011, vol. 2, pp. 851–858, 2011.

[90] A. K. Witte and R. Zarnekow, “Is open always better? -A taxonomy-based analysis of platform ecosystems for fitness trackers,” MKWI 2018 - Multikonferenz Wirtschaftsinformatik, vol. 2018-March, pp. 732–743, 2018.

[91] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the internet of things: Threats and challenges,” Secur. Commun. Networks, vol. 7, no. 12, pp. 2728–2742, 2014, doi: 10.1002/sec.795.

[92] M. Zimmer, P. Kumar, J. Vitak, Y. Liao, and K. Chamberlain Kritikos, “‘There’s nothing really they can do with this information’: unpacking how users manage privacy boundaries for personal fitness information,” *Inf. Commun. Soc.*, vol. 23, no. 7, pp. 1020–1037, 2020, doi: 10.1080/1369118X.2018.1543442.

# APPENDIX A: CHAPTER 3 INTERVIEW SCREENING SURVEY

Part 1:

1. Please select all the wearable devices you own:

☐ Fitbit
☐ Jawbone
☐ Misfit
☐ Polar
☐ Garmin
☐ None
☐ Other, please specify: _____

2. How long have you been using the device(s)?

☐ Less than three months
☐ More than three months

3. Have you ever shared your information recorded by the device(s) with others?

☐ Yes
☐ No

Part 2:

4. What is your first name?

_____

5. What is your age?

☐ 18-20 year
☐ 21-30 year
☐ 31-40 year
☐ 41-50 year
☐ 51-60 year
☐ >60 year

6. What is your email address?

_____

Thank you! Your response has been recorded. We will contact you soon to schedule an interview.

# APPENDIX B: CHAPTER 3 INTERVIEW QUESTIONS

**Demographic Questions:**

What is your age?
What is your gender?
What is your level of education?
What ethnicity do you identify with?
What is your current occupation?

**Questions related to the use of the wearable device:**

1. List all the wearable health devices that you own.
2. (If more than one), which do you use most frequently?
3. Have you used any other devices before? Why?
4. What are your goals of using the device?
5. How frequently and when do you use the device?
6. How and when do you look at your data on the device?
7. How has using the device impacted you?
8. What is your overall impression/satisfaction about using the device?

**Sharing preferences and behaviors:**

9. Have you ever shared your information with other people on the device platform?
   If yes:
   a. What information do you share and why?
   b. With whom do you share this information?
   c. Do they also share information with you?
   d. How do you share the information (what context, how frequently, and when)?
   e. How does the sharing impact your behavior and use of the device?
   f. Does sharing your information on the device help you achieve your goals? How?
   g. Has your sharing behavior changed over time?
10. Can you walk me through your profile? Show me what type of settings you have.
11. Did you change the sharing controls in the interface at any point?
    If yes:
    a. Why?
    b. Did you change it for a particular person or a group? Why?
12. Did your choice of sharing recipients affect how you shared the recorded information?
    If yes:
    a. How?
13. Did the sharing controls in the interface allow you to set your sharing preferences easily?
    If no:

   a. Why not?
   b. What changes/omissions/additions would you suggest to make the interface more usable?
   c. If it had been easier to change the privacy preferences, would you have shared differently? How?
14. Have you ever shared your wearable fitness data on popular SNSs, such as Facebook?
    If yes:
   a. Which ones, how, and why?
   b. With whom?
   c. What types of information and how frequently?
   d. Does anyone share such data with you as well?
   e. How does sharing your information on the SNS(s) impact your behavior and use of the device?
   f. Does sharing your information on SNS(s) help you achieve your goals? How?
   g. Do the controls on the SNS help you to share and manage your information?
   h. Do you have any preferences between platforms (i.e., a device platform or an SNS platform) to share your fitness information? Why?
15. Do you have any other way of sharing your information, other than what we have discussed?
16. In general, does the device's platform support your sharing preferences and goals?

**Questions related to privacy:**

17. What are your concerns regarding the privacy of your information on the device?
18. Have these concerns impacted your use of the device?
19. How do you manage your information on the device?
20. To what extent are you comfortable with the existing privacy settings?
21. Do you feel that you are sufficiently protected, or do you desire more protections? What kinds of protection do you need?
22. How do you think your information could be misused?
23. Are you worried that your daily activities will be monitored by another person or party when you use the system?
24. Do you have any additional comments about the privacy and sharing of the device data?
25. Would you like to say anything else before we end the interview?

# APPENDIX C: CHAPTER 4 INTERVIEW SCREENING SURVEY

What wearable fitness devices do/did you use?
☐ Fitbit
☐ Garmin
☐ Apple Watch
☐ Polar
☐ Samsung Galaxy Watch
☐ Other, please specify: _____

What is your first name?
_____

What is your email address?
_____

Thank you! Your response has been recorded. We will contact you soon to schedule an interview.

# APPENDIX D: CHAPTER 4 INTERVIEW QUESTIONS

How would you rate your skills in using technology devices and applications?
(a)Novice (b)competent (c)expert

I see that you use a [device name]. What are you goals in choosing and using this device?

**Behavioral Questions:**

1. What information collected by your device do (did) you share?
2. With whom do (did) you share this information and why?
3. How do (did) you share your fitness information?
4. What influence your decisions to, or not to, share your activity information?
5. What are your concerns when sharing your activity information?
6. Are there any other people or organizations that you think may have access to your activity information?

**Inferences:**

7. What information do you think your device is collecting about you?
8. What do you think about the possibility that others can infer some personal information from fitness tracker data? (others can be people, or organizations)
9. Have you thought about it before? Why/why not?
   If yes:
   Is this part of your decisions when sharing your data? How?
10. What do you think can be inferred from the data that your fitness tracker is collecting about you?
11. How comfortable are you if others infer this information? Why? What concerns do you have about others making those inferences?

**Examples & Scenarios:**

12. How concerned are you with sharing data like step, sleep, and heart rate? What would you possibly worry about?
13. How comfortable are you with sharing activity data that includes at least the previously mentioned data in the following scenarios [ask the participant why, and what could be the risk in each scenario]?
    a. Your device company shares the data with a background screening company who offers services for different parties including employers, insurers, and banks.
    b. You joined a fitness group where each member in the group shares their fitness tracker' data, and some members are not personally known to you.
    c. Your friend requested that you share your activity data with all friends on one of your social media accounts (e.g., Facebook, twitter, Instagram, …).
    a. A health insurance company classified you as overweight based on your fitness data that is collected by your wearable device.
    b. Your device infers your sexual activities.
    c. Your employer uses data in the tracker to identify your mood (e.g., if you are stressed.

d. Strangers infer your social connections based on the information you share over the app.

**Needs & Recommendations:**

14. What do you use to prevent others from inferring your personal information?
15. What do you suggest to help users like you become aware of what could be inferred about them from fitness trackers and other sources?
16. What features would you wish to have in order to help you protect your activity data in the device against inferences?
17. In general, do you have any comments before we end this interview?

**Background questions:**

- What is your age?
- What is your gender?
- What is your current job?
- What is your level of education?
- What is your ethnic group?

# APPENDIX E: CHAPTER 4 ONLINE SURVEY QUESTIONS

**PART A**

**Select all the wearable brands that you use/d?**

- ☐ Fitbit
- ☐ Apple Watch
- ☐ Polar
- ☐ Misfit
- ☐ Garmin
- ☐ Samsung
- ☐ Xiaomi
- ☐ Nokia
- ☐ Other, please specify: _____

**Have you ever shared any data collected by your fitness tracker with companies or third parties (e.g., health insurance company; health tracking app; other apps)?**

- o Yes, please indicate with whom:
  _____
- o No
- o Not sure

**Have you ever shared any data collected by your fitness tracker with other people (e.g., friends; online fitness groups)?**

- o Yes, please indicate with whom:
  _____
- o No
- o Not sure

**PART B**

**My goals for sharing information are (select all options that apply):**

- ☐ To stay fit
- ☐ To stay accountable
- ☐ To track health status/medical conditions
- ☐ To compete with others
- ☐ To encourage other people
- ☐ To receive incentives (e.g., discounts on purchases or health insurance rate)
- ☐ To brag about fitness achievements
- ☐ For enjoyment
- ☐ Other, please specify: _____

**On a scale of 1 to 5, how confident are you with the following:**

1) I understand how my fitness tracker collects my data

   1 2 3 4 5

2) I know how my fitness tracker data is being stored and used

   1 2 3 4 5

**Have you ever read your fitness tracker privacy policy and terms of conditions?**

- o Yes
- o No
- o Not sure

**Have you ever changed your fitness tracker account privacy settings?**

- o Yes
- o No
- o Not sure

**Have you ever taken any action(s) to protect the privacy of your fitness tracker data?**

- o Yes, please specify: _____
- o No
- o Not sure

**PART C**

**SELECT ALL THAT APPLY**

I am comfortable sharing my **name** with the following recipients:

- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **birthday** with the following recipients:

- ☐ Friends
- ☐ Acquaintances
- ☐ Workplace
- ☐ Health insurance company
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **weight and height** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **daily step count** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)

- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **sleep graph** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **heart rate data** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **calorie intake** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company

- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **Friends list** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **competitions/challenges** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **distance/miles** covered with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company

- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

I am comfortable sharing my **exercise route/map** with the following recipients:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

**PART D**

**For each given scenario below, select all the recipients that you would be comfortable sharing with:**

1. My Body Mass Index (BMI), as calculated based on my weight and height:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

2. A record of my sexual activity, as calculated by my heart rate and movement data:

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

3. My home location, as suggested by the exercise map/route

- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

4. My stress level, as suggested by my heart rate:
- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

5. If I have a sedentary lifestyle, as suggested by my average step count:
- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

6. My connections, as shown by how I compete in fitness challenges:
- ☐ Friends
- ☐ Family
- ☐ Acquaintances
- ☐ Significant others
- ☐ Health providers (e.g., primary doctor)
- ☐ Health insurance company
- ☐ Workplace
- ☐ Online health/fitness forum
- ☐ Fitness tracker company
- ☐ Third parties (health/fitness tracking apps, incentive programs, marketers)
- ☐ None

**PART E**

**For each given scenario, select: "likely", "unlikely" or "not sure"**

1. It could be determined if I am overweight based on my weight and height from my fitness tracker:

Likely ○ Unlikely ○ Not sure ○

2. My heart rate and movement data can indicate a record of my sexual activity:

Likely ○ Unlikely ○ Not sure ○

3. My home location can be determined from my exercise map/route:

Likely ○ Unlikely ○ Not sure ○

4. My heart rate data can be used to suggest that I am stressed:

Likely ○ Unlikely ○ Not sure ○

5. My average step count can suggest if I have a sedentary lifestyle:

Likely ○ Unlikely ○ Not sure ○

6. My competitions in fitness challenges can reveal my personal connections:

Likely ○ Unlikely ○ Not sure ○

**PART F**

**On a scale of 1 to 5, indicate the importance of the following factors regarding your comfort level with sharing in each scenario:**

1. **My body mass index, as calculated by my weight and height:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|
| If I can control who can see this information | ◯ | ◯ | ◯ | ◯ | ◯ |
| If the information is anonymized | ◯ | ◯ | ◯ | ◯ | ◯ |
| If there is perceived value/benefit | ◯ | ◯ | ◯ | ◯ | ◯ |
| If notice/consent is provided in advance | ◯ | ◯ | ◯ | ◯ | ◯ |

2. **A record of sexual activity, as calculated by my heart rate and movement data:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|
| If I can control who can see this information | ◯ | ◯ | ◯ | ◯ | ◯ |
| If the information is anonymized | ◯ | ◯ | ◯ | ◯ | ◯ |
| If there is perceived value/benefit | ◯ | ◯ | ◯ | ◯ | ◯ |
| If notice/consent is provided in advance | ◯ | ◯ | ◯ | ◯ | ◯ |

3. **My home location, as suggested by my exercise map/route:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|
| If I can control who can see this information | ◯ | ◯ | ◯ | ◯ | ◯ |

| | | | | | |
|---|---|---|---|---|---|
| If the information is anonymized | ○ | ○ | ○ | ○ | ○ |
| If there is perceived value/benefit | ○ | ○ | ○ | ○ | ○ |
| If notice/consent is provided in advance | ○ | ○ | ○ | ○ | ○ |

**4. My stress level, as suggested by my heart rate data:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|
| If I can control who can see this information | ○ | ○ | ○ | ○ | ○ |
| If the information is anonymized | ○ | ○ | ○ | ○ | ○ |
| If there is perceived value/benefit | ○ | ○ | ○ | ○ | ○ |
| If notice/consent is provided in advance | ○ | ○ | ○ | ○ | ○ |

**5. If I have a sedentary lifestyle, as suggested by my average step count:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|
| If I can control who can see this information | ○ | ○ | ○ | ○ | ○ |
| If the information is anonymized | ○ | ○ | ○ | ○ | ○ |
| If there is perceived value/benefit | ○ | ○ | ○ | ○ | ○ |
| If notice/consent is provided in advance | ○ | ○ | ○ | ○ | ○ |

**6. My connections, as shown by how I compete in fitness challenges:**

| | Not at all important | | | | Very important |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| If I can control who can see this information | ○ | ○ | ○ | ○ | ○ |
| If the information is anonymized | ○ | ○ | ○ | ○ | ○ |
| If there is perceived value/benefit | ○ | ○ | ○ | ○ | ○ |
| If notice/consent is provided in advance | ○ | ○ | ○ | ○ | ○ |

**(Demographic Information)**

**What is your age?**

_____

**What is your gender?**

- Male
- Female
- Other

**What is the highest level of education you have completed?**

- High school or equivalent
- Some college
- Bachelor's degree
- Master's degree
- Doctoral or Professional degree

**On a scale from 1 to 5, where 1 is novice and 5 is expert, how would you rate your skills in using technology?**

1 2 3 4 5

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

_____

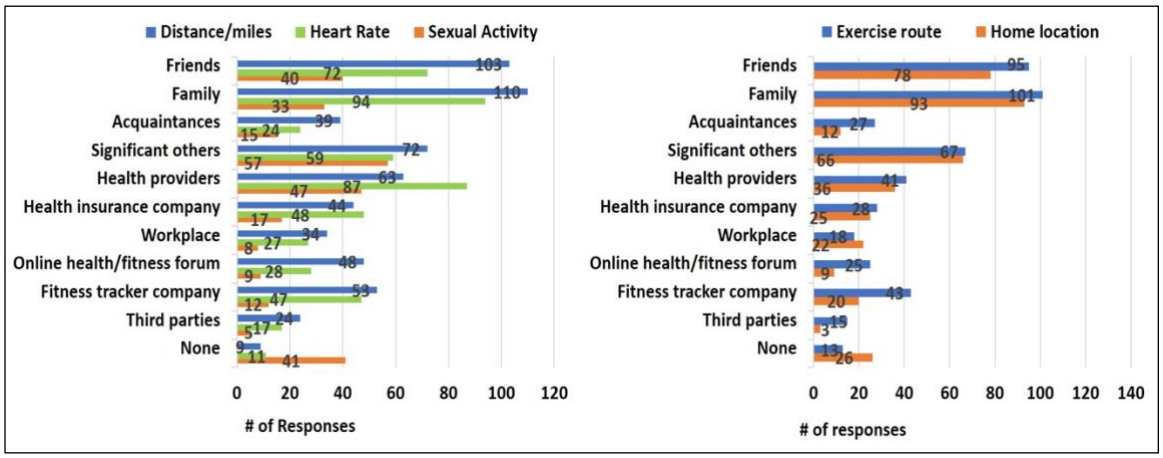
**What is your occupation?**

_____

**What ethnic group do you identify yourself with?**

_____

# APPENDIX F: CHAPTER 4 ADDITIONAL SURVEY RESULTS



# APPENDIX G: CHAPTER 6 EMAIL RECRUITMENT

**Co-design Study**

I seek Fitbit users who are familiar with the Fitbit app to take part in a remote co-design session that will last approximately 90 minutes. The goal of the design is to improve Fitbit sharing and Privacy settings. The meeting will be held over Google Meet. You can sign up in pairs or as an individual and I will match you with a design partner.

Participation criteria:

- English speaker
- 18 years or older
- Fitbit user

You do not need to have designing skills to participate in the study. You will receive a **$25 Amazon gift card** if you complete the entire study! Learn more and sign up at:

http://uncc.qualtrics.com/jfe/form/SV_4UeolicCxAIdtyJ

This study is approved by UNC Charlotte Institutional Review Board—IRB# 21-0033.

Thank you,
Abdulmajeed Alqhatani, PhD Student, UNC Charlotte.
Research advisor: Dr. Heather Lipford, Professor, UNC Charlotte.

# APPENDIX H: CHAPTER 6 SOCIAL MEDIA POST FOR RECRUITMENT

Hello,
We are researchers in the Human Computer Interaction lab at UNC Charlotte. We seek to recruit Fitbit users who are familiar with the Fitbit app to be part of a remote co-design session that will last approximately 90 minutes. The goal of the design is to improve Fitbit sharing and Privacy settings. You can sign up in pairs, or individually and we will match you with a design partner. In order to participate, you must be 18 years or older, Fitbit user, and must have a Google account to join to the study meeting via Google Meet.
You do not need to have designing/drawing skills to participate in the study. This study is cleared by our university Institutional Review Board, IRB: 21-0033.
You will receive a $25 Amazon gift card if you complete the entire study! Learn more and sign up at:
http://uncc.qualtrics.com/jfe/form/SV_4UeolicCxAIdtyJ

Thank you,
Abdulmajeed Alqhatani, PhD Student, UNC Charlotte.
Heather Lipford, Professor, UNC Charlotte.

# APPENDIX I: CHAPTER 6 SCREENING SURVEY

**What is your name?** *

**What is your email address?** *

**Would you like to sign up in pairs or individually?** *

(Note that if you chose to sign up in pairs, your partner needs to fill out this survey as well. Please provide our link to your designing partner. If you chose to sign up individually, we will find a design partner for you)

- Yes, please enter the other person's name below:
- No

*

What is your gender? (optional)

- Male
- Female
- Other

What is your age? *

What is your current job? *

What is your level of education? *

- High school or lower
- Some college
- Bachelor's degree
- Master's degree
- Doctoral or Professional degree

What is your area of expertise/major? *

# APPENDIX J: CHAPTER 6 PARTICIPATORY DESIGN

**Script:**

*Hi, thank you for joining this design session. My name is Abdulmajeed Alqhatani, a PhD student at UNC Charlotte.*

*I am conducting research on wearable device platforms sharing settings. My goal is to improve the design of these platforms in terms of sharing and privacy controls, so they can better support users' sharing goals with different recipients, such as friends, family, health and fitness communities, and can help users in protecting their information. Therefore, the purpose of your participation is to design or redesign together some of the sharing and privacy features in Fitbit.*

*This study will consist of three tasks. The entire study is expected to last no more than 90 minutes. The first stage may last for no more than 15 minutes and will occur as a dyad. I will ask you some questions related to sharing and privacy management over Fitbit. In the second stage, you will together redesign some of the Fitbit features that deal with sharing and privacy. I will provide you with a link that will take you to a Google Drawing sheet where you both can start designing. There, I prepared some designing shapes and icons for you. Before this stage begins, I will share my desktop screen so I will be able to record the design task in the Google drawing sheet. Don't worry about your design skills. Everything you design is going to be helpful. You will need to sign in using any Google account in order to access the sheet. This stage may last about 60 minutes. In the last stage, you will together present your designs, and I will ask you some questions about your designs. This stage may last for no longer than 15 minutes and will occur as a dyad.*

*The study will be video recorded for data analysis purposes. It will be stored confidentially and will be used for research purposes only.*

*Do you have any questions?*

**Pre-design Interview Questions:**

1. How do you use your Fitbit?
2. What concerns do you have about your information in Fitbit?
3. How do you manage your privacy on Fitbit?
4. Do you share any information collected by your Fitbit? How, what, and with whom?
5. What apps, if any, have you provided permission to access your Fitbit data?
6. What type of recipients would you most likely be interesting in sharing your information with?
7. How comfortable are you with the current sharing and privacy settings of Fitbit?

**Design Session:**

- **Part A**
  *Now, I will send you a link to a Google Drawings sheet. Please click on this link, and if you were asked to sign in, use any of your Google accounts.*

*This sheet is where you will work together to re/design features that improve the Fitbit settings regarding sharing and privacy. On the top of the sheet, I have prepared some icons and shapes, such as boxes, buttons, and arrows, so they can help you in designing your features. If you need help in locating additional design elements, please let me know. Everything you design would be helpful. I encourage you both to discuss your designs together. I will share my desktop screen in order to record the design session while you are both working on the drawings sheet.*
*Do you have any questions before we start the design session?*

- **Part B**
  *I have some design ideas and would like your feedback. You can use any of them, but you do not have to. The first idea is to improve the way that third party apps access users' data by giving users the ability to share granular data with third parties. Right now, third parties access users' data at a high-level. My second idea is to redesign the Fitbit sharing interface by allowing users to select which recipients they want to share their different activity with. It could be something similar to the Facebook Custom List. My last idea is to give users details about what other information can be learned about them based on the information they provide for a device. For example, heart rate variability can be an indicator of stress level.*

**Post-Design Interview Questions:**

8. Could you walk me through each of your designs?
9. How do you think these designs could support your sharing goals?
10. How do you think these designs could improve your privacy?
11. What additional sharing and privacy-related features do you wish Fitbit settings to have?
12. Do you have any comments about your designs or about sharing and privacy controls in fitness trackers in general?