August 2021

Interaction Techniques for In-the-Moment Privacy Control Over Data Generated by Wearable Technologies

Byron M. Lowens
Clemson University, bmlowens@gmail.com

Interaction Techniques for In-the-Moment Privacy Control Over Data Generated by Wearable Technologies

---

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Human Centered Computing

---

by
Byron M. Lowens
August 2021

Accepted by:
Dr. Kelly Caine, Committee Chair
Dr. Julian Brinkley
Dr. Bart Knijnenberg
Dr. Eileen Kraemer
Dr. Jacob Sorber

Abstract

Wearable technologies provide users with actionable insights regarding personal health information because of their ability to capture and analyze data continuously and in-the-moment through their rich set of sensors. While these technologies offer the advantages of conveniently capturing personal health data and behaviors outside of a clinical setting, they pose significant privacy challenges. Wearables continuously collect and store sensitive personal information about the wearer. In some instances, personal information amassed by a wearable may be shared without user awareness. In addition to the privacy-invasive risks posed by wearable technologies, executing usable privacy control directly on wearables poses an even greater challenge due to lack of input space and constrained interaction. Most privacy controls options for wearables are separate from the device itself, which prevents the user from having integrated and in-the-moment control over the data they are producing.

In light of the privacy risks and challenges for usable privacy-enhanced design for wearables, this dissertation uses a human-centered approach to advance the design space for usable and effective privacy control mechanisms. In particular, this research focuses on understanding how to develop privacy control mechanisms that provide adopters and potential adopters of wearables with integrated, in-the-moment control over personal information collected by wearables. This is accomplished through four user studies.

In the first study, I investigate the preferences of adopters and potential adopters of wearable health technologies as they relate to privacy and sharing of extra-clinical health information generated from a wearable. This study also examines whether individual preferences vary based on the recipient, type, and valence (e.g., positive or negative rating) of health information. I found that the recipient and valence of data predicted privacy and sharing preferences for extra-clinical data generated by wearables. Participants were more willing to share extra-clinical data with healthcare

providers, family, and friends compared to their employer or broader social network. Participants were also less willing to share negatively valenced data.

Applying the knowledge that users have granular preferences for sharing data from wearables, the second study evaluates the impact of the location of privacy control and decision timing for privacy control on wearables. I designed four privacy interfaces that provide different combinations of location (e.g., integrated versus decoupled) and decision timing (e.g., in-the-moment/synchronous versus a priori/asynchronous) of privacy control. To evaluate the interfaces, I conducted a 2x2 between-subjects experiment where different groups of participants interacted with each interface and assessed the ease of use, perceived privacy control, and perceived oversharing threat for the assigned interface. The results show that only the location of control significantly influences the overall ease of use of the privacy interface. In further exploratory analyses, I find that intentions to adopt a settings interface are influenced by the timing of when privacy decisions can be executed, if it is easy to manage those decisions, and if the privacy settings interface reduces the threat of oversharing personal information.

Adding more detail to understanding user preferences for privacy controls for wearables, the third study is an interaction-elicitation study that identifies a set of device-independent interactions that allow integrated and in-the-moment privacy control over data from a wearable. I found differences in the types of interactions people produced for situations requiring more versus less subtlety. In this study, I also establish a taxonomy that organizes interactions based on interaction mapping and physical characteristics of the interaction.

In the final study, I extend the findings of the interaction-elicitation study by further exploring the identified interactions in terms of their noticeability. This is done to determine a set of additional interactions wearers could adopt when they need to provide input to their device privately without being noticed. The results from this study produce a set of interactions(e.g., teeth click, single head nod) that are subtle enough to be used with any existing or emerging invisible wearable device.

The overall findings of this dissertation offer privacy researchers and designers of wearable technologies insight into the future development of wearables. The findings of this dissertation also present hardware and software considerations to designers as they design interfaces that provide a usable and effective means for adopters and potential adopters to maintain their privacy over data produced by wearables.

Acknowledgments

First and foremost I would like to give all praises to The Most High, for I know with God, all things are possible. My grounded spirituality and faith has guided me through this emotional undertaking of pursuing my Ph.D. even at times I wanted to give up, I always knew that something greater than myself was guiding me and leading me throughout this process. There is evidence of a divine presence, and I am forever grateful for that presence that has never left my side.

To my parents, Bobby and Marion Lowens, who set the foundation for who I am today. From an early age, you always suggested the importance of further educating myself and awarded my keen sense of inquiry at an early age through books and mathematics. I am grateful for all the sacrifices you both made for me to be where I am today. Both of you did everything you could to ensure my success, and those things will never be forgotten. I am sincerely grateful for all you have done for me.

To my brother, Milan Taylor, who transitioned during my doctoral studies. You always told me you were my biggest fan, and you always had my back growing up. Although we only got to spend a short time together, and you were taken away sooner than we all would have preferred, I am grateful for your presence in my life. Thank you for all the lessons you taught me and for being an example of a "fearless warrior" who never gave up regardless of any obstacle that stood in your way. During the latter part of your life, I saw you struggle with health issues, but you never gave up without a fight! I adopted that same mentality in pursuing something so difficult. I wish you could be here to see the man I have become, but I know you are in heaven smiling down on me. I can hear your response to me telling you I finally finished. "Oh, yea?" That response always meant you were proud of me, although you were a man of very few words. Our bond and connection will never die, and I am forever grateful for you. I know you are resting in peace. As you always told me "Brothers for life."

To my dear family members. Thank you all for always supporting and celebrating me. You all are the reason I was able to push through. There is no way I could let any of you down, and I am forever grateful for every one of you for always being there for me. Special thanks especially to my Uncle George, T-Dot, Uncle Brother, Uncle Jefferey, Uncle Carl, Uncle David Lewis, Aunt Patricia, Uncle Robert, my cousins Brienne and Semora , and my sister Nett. This degree is dedicated to all of you!

To all my friends, thank you for your endless support, especially the ones I made over the past six years while at Clemson. I came to this place alone, with one goal, and that was to get a Ph.D. I never knew along the way I would gain a family. Many of you saw me at my lowest point, but never stopped uplifting me and doing all you could to support me. Thank you all for holding me down through my troubled times and genuinely showing me that "Friendship is essential to the soul." Special thanks to Dr. A.D. Carson, Dr. Ashley Isreal, Dr. Aris Hall, Dr. Diane Beltran, Barry Kelly, Dr. Courtney Allen, Hakeem, Dr. Jerone Dunbar, Joey, Jumah, Pauline Matthey, Dr. Pauline Tholozany, Phillip Hall Jr, Marcus Curry, Shauna, and Dr. Travis Smith. I am grateful to you all.

To all my colleagues within the Clemson Hatlab, thank you for all your endless support. I am grateful for each and every one of you. You all were always willing to support and provide feedback on my research and helped me get through graduate school. Special thanks to Moses, who spent plenty long nights in 220 with me pushing through and working hard until the AC kicked on. I'll never forget those times brother! Also, special thanks to Reza and Dr. Paritosh Bahirat, who spent generous amounts of time helping me refine my statistics and research methods. When I was stuck, you never hesitated to lend a helping hand, whether in person or on zoom, and I am sincerely grateful for you both.

To all the mentors I had throughout my time at Clemson, thank you all for encouraging me, enabling my professional development, and just being there to keep me going. To Dr. Vivian Motti, thank you for your kindness and depth of insight early on during my graduate studies. You were always willing to help me and set the springboard for my academic journey. Special thanks to Dr. Curtis White. You were the first person I met when I came to Clemson, and you have been there to support me every step of the way. Special thanks also to my mentor and my Brother, Bryant K. Smith. You always told me like it was, and you never held back. Thank you for your time, affection, patience, and love. I am grateful to you all.

To my amazing committee members Dr. Julian Brinkley, Dr. Eileen Kramer, and Dr. Jacob Sorber. I am profoundly grateful for all of your and your support. Special thanks to Dr. Bart Knijnenberg for sharing your insight and brilliance throughout my graduate studies and always helping me with data analysis and interpretation. You are an amazing human who is always supportive and patient with each and every one of your students. I am sincerely grateful to you. To Dr. Emily Sidnam, thank you so much for helping me through the final stage of my dissertation. You had one goal when you started working with me, and that was to make sure I graduated. You never backed down from that goal, even at times when I could not see the light at the end of the tunnel; you always pushed me and motivated me to keep pressing on. You are an amazing human being, and I am so grateful that our paths crossed.

Thanks to Dr. Juan Gilbert for your relentless and tireless efforts in promoting the success of African Americans in pursuing Ph.D.'s and presenting me with the opportunity to earn my Ph.D. in computing. You made this dream a reality, and I am grateful for your presence in academia.

Lastly, to my amazing advisor and committee chair, Dr. Kelly Caine. I am immensely grateful for your wisdom, guidance, patience, and enthusiastic support of my research career. Thank you for taking a chance on someone like me and seeing me through these past seven years in my pursuit of my Ph.D. At times, I know this task was difficult, but you never backed down. Thanks for always having my back and ensuring my success. Thank you for never giving up on me, even at times when I was on the brink of giving up on myself. Thank you for teaching me how to become a scientist and for all the valuable advice you have given me from day one. Wherever my career takes me, just know you played a vital role in my success, and I am forever grateful to you, and I will never forget all you have done for me.

Special thanks to the National Science Foundation and the Clemson Graduate School, who provided financial support throughout my academic studies.

Table of Contents

Title Page . . . . . **i**

Abstract . . . . . **ii**

Acknowledgments . . . . . **iv**

List of Tables . . . . . **ix**

List of Figures . . . . . **xi**

1 Introduction **1**
1.1 Problem Motivation 1
1.2 Research Motivation 2
1.3 Research Motivation 3
1.4 Research Objectives 4
1.5 Overview and Summary of Studies 5

2 Literature Review **8**
2.1 Wearable Privacy 9
2.2 Privacy Controls and their Challenges 19
2.3 Elicitation Studies for Input Interactions 21

3 Study 1: Privacy and Sharing Preferences for Health Information Generated by Wearables **26**
3.1 Introduction 26
3.2 Background and Significance 28
3.3 Method 29
3.4 Results 34
3.5 Discussion 42
3.6 Limitations 47
3.7 Chapter Conclusion 48

4 Study 2: An experiment to assess the impact of location of privacy controls and decision timing. **49**
4.1 Introduction 49
4.2 Method 57
4.3 Quality Checks for construct measures 67
4.4 Reliability and validity check for each construct to measure user experience 68
4.5 Results 69
4.6 Discussion 73
4.7 Limitations 77

4.8 Chapter Conclusion 78

5 Study 3: User-Defined Interactions for Integrated and and In-the-Moment Privacy Control on Wearable Devices 80
5.1 Introduction 80
5.2 Method 85
5.3 Results 92
5.4 Discussion 103
5.5 Limitation and Future Work 110
5.6 Conclusion 112

6 Study 4: Invisible Input for Invisible Devices 113
6.1 Introduction 113
6.2 Methods 115
6.3 Results 123
6.4 Discussion 127
6.5 Conclusion 130

7 Discussion of all Four Studies of the Dissertation 131
7.1 Contributions 132
7.2 Impact on Privacy Research 134
7.3 Impact of the Future Design of Wearables 135
7.4 Broader Implications of this work 137
7.5 Recommendations For Future Work 138
7.6 Summary 139

Appendices 140
A Study 1 Materials 141
B Study 2 Materials 153
C Study 4 Materials 202

References 230

List of Tables

2.1 Summary of Systematic Literature Review(1st Iteration) 9
2.2 Summary of Systematic Literature Review(2nd Iteration) 9

3.1 Independent Measures and Description (as provided to recipient) Note: (+) or (-) indicates valence of scenario. (+) indicates positive valence and (-) indicates negative valence 31
3.2 Experimental Trials Presented to Participants 33
3.3 Participant Demographics. Note that for wearable device ownership, the numbers do not sum to 100 because participants can be counted in multiple categories. 35
3.4 Percentage of participants who something, everything, or nothing 36
3.5 Effect of Sharing on each IV 42

4.1 Description of Each Experimental Condition 60
4.2 Description of Independent and Dependent Variables 60
4.3 Constructs used to measure overall user experience 65
4.4 Participant Demographics 68
4.5 Mean and Standard Deviation for all constructs used to measure overall user experience per condition 69
4.6 Regression results from hypothesis testing. 70
4.7 Hierarchical Regression Analysis Results for Predictors of Likelihood to Adopt . . . 72
4.8 Mean and Standard Deviation for Likelihood of adoption for each interface condition 72

5.1 Demographics of Study Participants 87
5.2 Taxonomy of interactions for Integrated and In-the-Moment privacy decisions for wearables based on 128 unique interactions collected interactions from 460 trials . . 93
5.3 Table showing all interactions that met at least one criterion. Interactions are organized by corresponding referent and social context along with an indication of whether the interaction met each of the three criterion. Interactions that meet a given criterion are marked with an * NOTE: Frequency is the individual frequency of unique occurrence with a minimum of five and max consensus is medium or high only. . . . 98
5.4 The referent and social context along with the interactions participants produced with the highest consensus. The overall max-consensus and consensus-distinct ratios are shown for each referent and included context. The highest scoring referent(s)/context(s) for each metric are shaded in grey, whereas the lowest scores are indicated in **bold**. 99
5.5 Interactions with medium and high max-consensus. Interactions with high max consensus (>0.30) are marked with an *. Note: None of the interactions from the *share; discreet* condition achieved high or medium max-consensus. 100
5.6 Frequency of interactions produced by participants during the interaction elicitation. Only interactions that met the threshold of five are included. No interactions in the *share; discreet* referent condition met the threshold of five. 101

6.1 Researcher Classification of Interactions 117
6.2 Reclassification of Interactions From Pilot Testing. Note: Interactions with a * were originally classified as subte. Interactions with a ** were originally classified as obvious 119
6.3 Participant Demographics 121
6.4 Interaction Identified as Subtle Along With Original Classification 130

List of Figures

1.1 Illustration of different phases of the dissertation 7

3.1 Stimuli presented to participants via two wearable devices. Fig. a shows the WWD, and Fig. b shows the HMD 31
3.2 An example scenario used as stimuli for the experiment. 33
3.3 An overview of the differences between levels of the IV for the type of data, recipient, and valence categories. **The red bar signifies percentage of instances people would be willing to share at least some type of data (29% indicates overall instances of sharing) 37
3.4 An overview of the differences in sharing based on type and recipient of data 39
3.5 An overview of the differences in sharing based on type and valence of data 40
3.6 An overview of the differences in sharing based on recipient and valence of data . . . 41

4.1 The privacy notice design space developed by [297]. This model is defined by four main dimensions:timing, channel,modality, and control. 52
4.2 Stimuli presented to participants via mock-up for the Integrated Synchronous Condition 61
4.3 Stimuli presented to participants via mock-up for the Integrated Asynchronous Condition. 62
4.4 Stimuli presented to participants via mock-up for the Decoupled Synchronous Condition. 63
4.5 Stimuli presented to participants via mock-up for the Decoupled Asynchronous Condition. 64
4.6 Overall Ease of Use for Decoupled Versus Integrated Interfaces 71
4.7 Overall Ease of Use for Decoupled Versus Integrated Interfaces 73
4.8 Proposed Design Space For Privacy Control on Wearable Technologies 76

5.1 Stimuli Used in Interaction Elicitation 88
5.2 Proportion of interactions from each dimension of the taxonomy. 92
5.3 Proportions of interactions involving each part of the body. 95
5.4 Highest Max-Consensus Ratio for the referents and included social contexts used during the interaction elicitation exercise. Interactions that had the highest consensus are shown in the Figure. Agreement rates of less than 10%, between 10% and 30%, and between 30% and 50% are considered low, moderate, and high agreement respectively [335]. *Note: The referent *share* while in the presence of others;discreet, had no max-consensus as none of the 13 interactions were repeated. 96
5.5 The user-defined set of interactions across social context. The leftmost interaction in the symmetrical pair satisfies the referent *share*, and the rightmost interaction of the pair satisfies the referent *withhold*. 105

6.1 Mean Action and Confidence of Response Across All Categories 124
6.2 Mean Interaction and Confidence of Response Across All Categories 124
6.3 Interactions Perceived As Actions and Corresponding Interaction Score 125
6.4 Interactions Perceived as Subtle and corresponding interaction score 126

6.5 Perceived As Interactions With Technology 127
6.6 Interaction Perceived as Invisible 128

1 Recruitment Flyer For Study 1 141
2 Informed Consent For Study 1 142
3 Study Script For Study 1 (page 1) 143
4 Study Script For Study 1 (page 2) 144
5 Pre-Survey Demographic Questionnaire For Study 1 (page 1) 145
6 Pre-Survey Demographic Questionnaire For Study 1 (page 2) 146
7 Pre-Survey Demographic Questionnaire For Study 1 (page 3) 147
8 Pre-Survey Demographic Questionnaire For Study 1 (page 4) 148
9 Post-Survey Questionnaire For Study 1 (page 1) 149
10 Post-Survey Questionnaire For Study 1(page 2) 150
11 Post-Survey Questionnaire For Study 1 (page 3) 151
12 Post-Survey Questionnaire For Study 1 (page 4) 152
13 Recruitment Flyer used on Prolific For Study 2 153
14 Page to record participants unique Prolific ID For Study 2 154
15 Informed Consent For Study 2 155
16 Screener Questionnaire For Study 2 (page 1) 156
17 Screener Questionnaire For Study 2 (page 2) 157
18 Experimental Condition For IS Interface 158
19 Attention Check question used to to check if participants were attentive during the IS Conditions 159
20 Interface Evaluation for the IS Condition (Perceived Ease of Use page 1) 160
21 Interface Evaluation for the IS Condition (Perceived Ease of Use page 2) 161
22 Interface Evaluation for the IS Condition (Perceived Ease of Use page 3) 162
23 Interface Evaluation for the IS Condition (Perceived Privacy Control page 1) 163
24 Interface Evaluation for the IS Condition (Perceived Privacy Control page 2) 164
25 Interface Evaluation for the IS Condition (Perceived Privacy Control page 3) 165
26 Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 1) . . 166
27 Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 2) . . 167
28 Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 3) . . 168
29 Experimental Condition For IA Interface + Attention Check question used to to check if participants were attentive 169
30 Interface Evaluation for the IA Condition (Perceived Ease of Use page 1) 170
31 Interface Evaluation for the IA Condition (Perceived Ease of Use page 2) 171
32 Interface Evaluation for the IA Condition (Perceived Ease of Use page 3) 172
33 Interface Evaluation for the IA Condition (Perceived Privacy Control page 1) 173
34 Interface Evaluation for the IA Condition (Perceived Privacy Control page 2) 174
35 Interface Evaluation for the IA Condition (Perceived Privacy Control page 3) 175
36 Interface Evaluation for the IA Condition (Perceived Oversharing Threat page 1) . . 176
37 Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 2) . . 177
38 Interface Evaluation for the IA Condition (Perceived Oversharing Threat page 3) . . 178
39 Experimental Condition For DS Interface + Attention Check question used to to check if participants were attentive 179
40 Interface Evaluation for the DS Condition (Perceived Ease of Use page 1) 180
41 Interface Evaluation for the DS Condition (Perceived Ease of Use page 2) 181
42 Interface Evaluation for the DS Condition (Perceived Ease of Use page 3) 182
43 Interface Evaluation for the DS Condition (Perceived Privacy Control page 1) 183
44 Interface Evaluation for the DS Condition (Perceived Privacy Control page 2) 184
45 Interface Evaluation for the DS Condition (Perceived Privacy Control page 3) 185

46 Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 1) . . 186
47 Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 2) . . 187
48 Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 3) . . 188
49 Experimental Condition For DA Interface + Attention Check question used to to check if participants were attentive 189
50 Interface Evaluation for the DA Condition (Perceived Ease of Use page 1) 190
51 Interface Evaluation for the DA Condition (Perceived Ease of Use page 2) 191
52 Interface Evaluation for the DA Condition (Perceived Ease of Use page 3) 192
53 Interface Evaluation for the DA Condition (Perceived Privacy Control page 1) 193
54 Interface Evaluation for the DA Condition (Perceived Privacy Control page 2) 194
55 Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 1) . 195
56 Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 2) . 196
57 Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 3) . 197
58 Post-Survey Questionnaire For Study 2 (page 1) 198
59 Post-Survey Questionnaire For Study 2 (page 2) 199
60 Post-Survey Questionnaire For Study 2 (page 3) 200
61 Post-Survey Questionnaire For Study 2 (page 4) 201
62 Recruitment Flyer Used On Amazon Mechanical Turk For Study 4 202
63 Informed Consent For Study 4 (page 1) 203
64 Informed Consent For Study 4 (page 2) 204
65 Pre-Survey Demographic Questionnaire For Study 4 (page 2) 205
66 Pre-Survey Demographic Questionnaire For Study 4 (page 3) 206
67 Pre-Survey Demographic Questionnaire For Study 4 (page 4) 207
68 Pre-Survey Demographic Questionnaire For Study 4 (page 5) 208
69 Pre-Survey Demographic Questionnaire For Study 4 (page 6) + Training Instructions (page 1) 209
70 Training Instructions For Study 4 (page 2) 210
71 Training For Study 4 (page 1) 211
72 Training For Study 4 (page 2) 212
73 Training For Study 4 (page 3) 213
74 Training For Study 4 (page 4) 214
75 Training For Study 4 (page 5) 215
76 Training For Study 4 (page 6) 216
77 Training For Study 4 (page 7) 217
78 Training For Study 4 (page 8) 218
79 Instructions For Study 4 219
80 Study 4 Experimental Stimuli(Issue With Video Question) 220
81 Study 4 Experimental Stimuli(Action Question) 221
82 Study 4 Experimental Stimuli(Confidence of Action Question) 222
83 Study 4 Experimental Stimuli(Interaction Question) 223
84 Study 4 Experimental Stimuli(Part 2 Page 1) 224
85 Study 4 Experimental Stimuli(Part 2 Page 2) 225
86 Study 4 Experimental Stimuli(Part 2 Page 3) 226
87 Study 4 Experimental Stimuli(Part 2 Page 4) 227
88 Study 4 Experimental Stimuli(Part 2 Page 5) 228
89 Study 4 Compensation Question 229

Chapter 1

Introduction

1.1 Problem Motivation

Wearable technologies are a class of devices that are small enough to be worn directly on the body or kept within close proximity to the body and integrate computational sensing capabilities to offer specific features to wearers [123, 210, 232]. The evolution of wearables has led to a paradigm shift in healthcare [21, 40] and fitness [83, 106, 117, 132]. A great deal of change has been that data formerly collected inside a clinical setting, can now be collected outside of a clinical setting [95, 346, 367] while still providing innovative methods to provide users with actionable insights regarding the quality of health and well being [96, 225, 316]. Wearable technologies have also become valuable to other application domains, industries, and services, including workplace safety, gaming, consumer financial applications, security, and entertainment[211, 276].

While the benefits of wearable technologies seem evident [123], critical issues concerning the management of information privacy associated with the collection and retention of sensitive information still exist, mainly because the data collected is personal to the wearer [377]. These issues pose unfavorable privacy risks for adopters and potential adopters [202, 321].

The privacy issues associated with the use of wearable technologies span from the unintended misuse of personal health information [202, 265, 275] to ineffective privacy control mechanisms that fail to imperfectly enable individuals' control over personal information [296]. Additionally, wearables are equipped with high-quality sensors that allow adversaries to make behavioral inferences (e.g., location, demographics, health status, and physiological/emotional behaviors) about a wearer

without their awareness or consent [178, 181, 281, 373]. An even more concerning issue is that most wearable users are not always aware of the threats, risks, and implications posed by the use of these devices [139]. In other instances, wearers may have explicit misconceptions about privacy implications associated with the usage of these devices or may feel they have no other choice than to sacrifice their privacy [202, 329]. These misconceptions of the privacy implications associated with wearables, the lack of knowledge of privacy-related threats among users, along with lack of adequate privacy mechanisms to control personal information could have an adverse impact on existing, and potential adopter's in the future [202].

Consequently, unless wearable technologies are carefully designed to minimize inherent privacy risks by affording the wearer control over their personal information, their adoption may reduce the level of individual privacy afforded during and beyond the use of the device [202].

1.2 Research Motivation

A number of research approaches have been explored by the HCI community to understand privacy perceptions about the adoption of wearable technologies. Several works have highlighted different user concerns based on the type of data collected, the type of sensor used, and the purpose of the wearable device [91, 202, 221, 221, 234, 266, 275].

For example, Motti et al. [234] analyzed users' privacy concerns about wearable devices using qualitative data from various sources such as e-commerce websites, forums, and social media where users expressed their concerns about the privacy of wearables. As a result, concerns were categorized into three categories: whether the concern was related to the physical device or the associated application, sensor-specific, or user's data. Findings suggest that privacy concerns toward wearables are similar, but some instances are more specific than privacy concerns related to mobile devices. Results also show that users possess a keen awareness of impending privacy implications of wearables, but primarily during data collection and sharing. This work also claims that users' lack of concern arises from a lack of awareness of how privacy can be threatened when organizations collect granular data about users over a long time. While this work offered valuable contributions to research on wearable privacy and provided general insights on users' concerns about it, this work collected data anonymously from online comments, and we do not know much about the profiles or demographics of the people contributing data to this study. Also, the methods in this study that

collect and analyzed online data employ a relatively new research approach that is both exploratory and empirical and does not have a well-established and validated protocol concerning data collection and analysis.

1.3 Research Motivation

A number of research approaches have been explored by the HCI community to understand privacy perceptions about the adoption of wearable technologies. Several works have highlighted different user concerns based on the type of data collected, the type of sensor used and the purpose of the wearable device [91, 202, 221, 221, 234, 266, 275].

For example, Motti et al. [234] analyzed users' privacy concerns about wearable devices using qualitative data from various sources such as e-commerce websites, forums, and social media where users expressed their concerns about the privacy of wearables. As a result, concerns were categorized into three categories: whether the concern was related to the physical device or the associated application, sensor-specific, or user's data. Findings suggest that privacy concerns toward wearables are similar, but some instances are more specific than privacy concerns related to mobile devices. Results also show that users possess a keen awareness of impending privacy implications of wearables, but primarily during data collection and sharing. This work also claims that users' lack of concern arises from a lack of awareness of how privacy can be threatened when organizations collect granular data about users over a long time. While this work offered valuable contributions to research on wearable privacy and provided general insights on users' concerns about it, this work collected data anonymously from online comments, and we do not know much about the profiles or demographics of the people contributing data to this study. Also, the methods in this study that collect and analyzed online data employ a relatively new research approach that is both exploratory and empirical and does not have a well-established and validated protocol concerning data collection and analysis.

Prasad et al. [274] investigated users' willingness to share personal information, collected using wearables with a given set of recipients. Results from this study show that user preferences for sharing data from wearables are granular and suggest that designers create flexible controls that allow granular sharing preferences. This work also suggest that when designing privacy controls for wearables designers should consider privacy controls that are usable so that users understand what

choices they have and know how to execute those choices. However, we are now aware of any work that has applied these recommendations and empirically evaluated the recommendations using a user-centered approach.

To address these research gaps, in my doctoral thesis, I leverage the behavioral privacy model [51] to inform my research, gain understanding of privacy parameters, and examine privacy protection methods to inform the design of usable privacy mechanisms for wearable devices.

1.4 Research Objectives

The behavioral privacy model describes three everyday behavioral mechanisms associated with use of technology to regulate privacy that include: avoidance, modification and alleviation [52]. Within this model two elements are also identified that could affect a users' privacy - *content* and *recipient* of information- when examined in combination [52]. Aiming at offering more effective privacy controls for wearables, I leverage this model to first understand the two parameters, information type, and recipient of information. In addition to information type and recipient, I also examine valence of information, which is the is the affective quality of intrinsic "good"-ness or "bad"-ness of an "event, object, or situation" [116]. I further examine different privacy control interfaces that would allow usable, and effective privacy control, and follow up this exploration by evaluating alternative in-the moment privacy control mechanisms for wearables that afford a more effective and usable means of privacy control by integrating sharing decisions with privacy interfaces using user-defined input interactions. I also provide design guidelines for effective and usable privacy protection mechanisms for wearable technologies.

To achieve this goal, I plan to answer the following research questions.

- Understand user preferences for sharing data from a wearable based on recipient, type, and valence of information:
  - **RQ1:** What types of health-related data generated by wearable technologies are users willing to share or keep private? **(Chapter 3)**
  - **RQ2:** With which potential recipients are users more willing to share their health-related data generated by a wearable device? **(Chapter 3)**
  - **RQ3:** Are users' sharing preferences associated with the valence (e.g.positive/negative rating) of the health-related information? **(Chapter 3)**

- Study and propose effective privacy control interfaces for wearables that allow granular sharing preferences over data from wearables:
  - **RQ4:** Does location of control, timing of control or the combination of the two impact the user experience for users of wearable technologies **(Chapter 4)**
- Develop a set of device-independent user-defined interactions for in-the-moment privacy control over data from a wearable:
  - **RQ7:**What interactions do users propose to communicate privacy decisions about data from a wearable?
  - **RQ8:** Does social context (e.g., whether people are alone,with others or or in a situation where they need to be discreet) affect the type of interactions people propose to communicate privacy decisions? **(Chapter 5)**
  - **RQ9:** Are there differences in the types of interactions people propose for situations requiring privacy(e.g., when they are around others, but need to be discreet) vs. situations that require less privacy? **(Chapter 5)**
- An evaluation of noticeable and unobservable interactions for invisible input on wearables.
  - **RQ10:** Which interactions proposed under a discreet social context are perceived as: an action, an interaction with some technology, invisible to the naked eye, and deemed as subtle when viewed by a second group of participants?

1.5 Overview and Summary of Studies

To answer the proposed research questions, we conducted four studies.

Study 1: Understanding user preferences for sharing data from a wearable based on recipient, type, and valence of information. Focusing on the behavioral theory of privacy, controlling for type of data and recipient of data, we must know what type of data individuals would be willing to share with a given recipient and if those sharing preferences vary based on whether or not the type of data is deemed as positive or negative. In a 4 (type) x 4 (recipient) x 2 (valence) within-subjects repeated measures scenario-based experiment, I assessed adopters and potential adopters of wearable technologies preferences for sharing extra-clinical health information collected via a wearable device. Participants in this study completed two questionnaires and a scenario-based experiment that elicited sharing preferences,

Study 2: Investigate the impact of the location of privacy controls and decision timing for wearables. Based on the formative research I conducted to see what type of information users would be willing to share and with whom, I explore user perceptions toward making privacy decisions over data from a wearable via four privacy interfaces. Using a 2x2 between-subjects experimental design with location of privacy control and timing of privacy control being the between subjects factors, four groups of participants were presented a privacy interface where privacy decisions were made (1)on the wearable in the moment, on the wearable, but not in the moment (e.g., before data collection),(2) off the wearable (e.g., via mobile phone) (3)in the moment, and (4)off the device not in the moment (e.g., before data collection). The assessment focused on ease of use, perceived privacy control, and perceived oversharing threat. Our results show that there was no interaction effect for location and privacy in terms of perceived ease of use, perceived privacy control, and perceived oversharing threat, but there was a significant main effect for the location of control. We also find that the ease of use, the timing of control, and perceived privacy threat impacts the likelihood to adopt a given privacy interface

Study 3: Identifying a set of device-independent interactions that enable in-the-moment privacy control for wearables. In study 3, we conducted an an open-ended elicitation study [27, 361] with 32 participants, where we elicited intuitive interactions that imply binary sharing preferences of some data collected by a wearable (e.g., activity data) with a given recipient (e.g., social network) across three social contexts: *alone*, *with others*, and *discreet*. Results from this study include an interaction taxonomy for in-the-moment privacy control on wearables that describes the mapping and physical characteristics of the interactions, and a user-defined consensus set of 20 device-independent interactions, along with criteria that were used to develop this set.

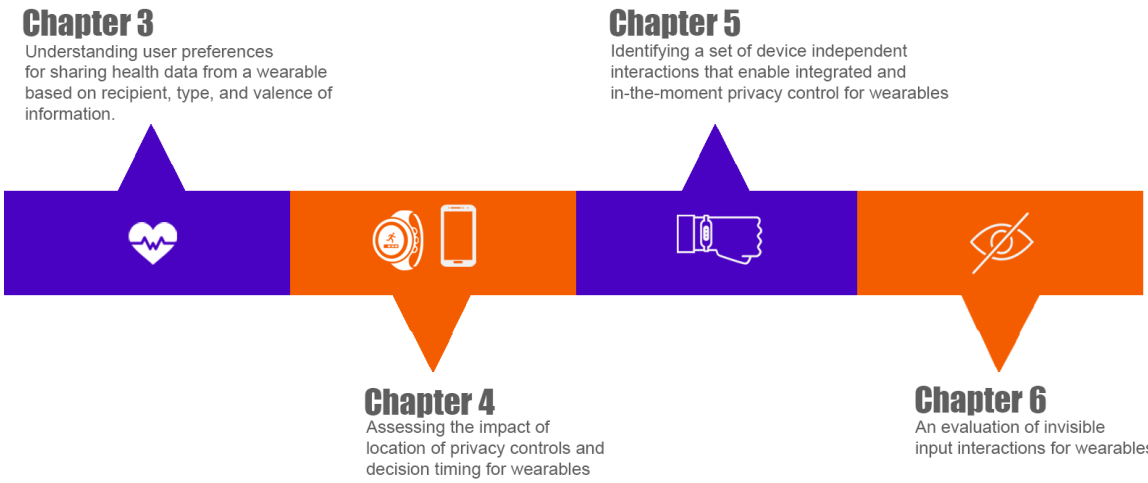


Figure 1.1. Illustration of different phases of the dissertation

Furthermore, we describe the implications of this work, including the need for discreet interactions, the promise of symmetrical interactions, and hardware and software needs for the development of device-independent interactions that give users control over personal information from a wearable.

Study 4: Invisible Input for Invisible Devices In study 3, we identified a set of user-defined interactions that could enable in-the-moment privacy control for wearables. We found that when we asked participants to propose interactions for situations where they needed to be discreet, there was very little consensus among interactions for that social context. In this study, I focused exclusively on the subset of interactions that participants proposed where they were asked to be discreet. In this study, I evaluated 50 interactions in terms of perceived action, the confidence of perceived action, perceived interaction with a wearable, and confidence of that perceived action. Results from this reveal a set of interactions that are subtle enough to allow a user to interact with a wearable technology without being noticed or disrupting others around them.

Chapter 2

Literature Review

To acquire a broad understanding of the current state of literature about wearable technologies and privacy control mechanisms for wearables, I conducted a literature review of research published in the ACM Digital Library, IEEE Xplore, and Google Scholar. I used various search queries and combinations to search both titles and abstracts within each database and limited the search to conference proceedings and journals published between May 2000 to May 2020. During the initial iteration of the search, I found a total of 112,263 articles within the ACM Digital Library and a total of 71,757 within the IEEE XPlore Library (See Table 2.1). Because of the large number of results (N=184,020) I decided not to search google scholar for any additional works that used the terms in the 1st search iteration.

During the next iteration, I narrowed the search down to the search queries shown in table 2.2. After the initial search, I manually excluded articles that are duplicated and/or not directly relevant to the scope of my research. For example, when searching on Google scholar using the search term, "Wearable" AND "Privacy" several works were duplicate papers I initially found in the ACM and IEEE Explore Library (N=38). After the additional screening, I found that of the (N=63) that remained, (N=45) were not relevant to the context of this dissertation. For example, several works mentioned security and authentication vulnerabilities on wearables. While these works are important, our focus is more related to privacy for wearable technologies. After narrowing the search to only relevant articles, I found a total of (N=18) articles that I did not come across on the ACM or IEEE XPlore digital library for this search term.

After screening each article and removing duplicates not relevant to the scope of this work,

Search Queries	ACM Digital Library	IEEE XPlore
Wearable	3,629	24,240
Privacy	11,139	46,658
Wearable Privacy	14,817	735
Wearable Privacy Control	82,678	124
Total	112,263	71757

Table 2.1. Summary of Systematic Literature Review(1st Iteration)

Search Queries	ACM Digital Library		IEEE XPlore		Google Scholar	
	Initial Search	After Screening	Initial Search	After Screening	Initial Search	After Screening
"wearable" AND "privacy"	14	11	24	16	101	18
“wearable” AND “privacy” AND “control”	1	N/A	0	N/A	0	N/A
“gesture” AND “elicitation”	14	13	0	N/A	18	14
gesture AND wearable privacy	53	43	0	N/A	0	N/A
Gesture AND Wearable AND Privacy	0	N/A	20	19	0	N/A
Total	82	56	44	35	119	32

Table 2.2. Summary of Systematic Literature Review(2nd Iteration)

I identified a corpus of N=123 articles. In addition to the results of this literature review, please see each chapter for a brief review of literature relevant to that study.

2.1 Wearable Privacy

Privacy is one of the most persistent social issues connected to information technology [243] and is a complex concept that can take on various definitions in different contexts [300]; in the scientific [89], industrial domains [187] and standardization bodies [71]. No privacy consensus exists [187], as users perceive it differently, due to personal [52, 240], or cultural [330] aspects. Sharing information can be critical or trivial depending on individual perceptions and involving circumstances. In the context of this dissertation, privacy refers to the ability to not exhibit information, to prevent external access or observation by the society when unintended.

One important stream of privacy research is privacy for wearables. Wearable technologies and their dynamic sensing capabilities are progressively popular among consumers [97, 134, 186, 341] and have seen exponential growth within the last few years [186]. Market reports estimate that the market for wearables (e.g., fitness trackers and smart watches) will increase from 27 billion in 2019 to 64 billion by 2024 [3]. Studies also demonstrate that the number of Americans who own wearables has increased from 12% in 2015 to 25% in 2019 [4]. Historically, wearables have mostly appealed to younger users, but recently there has been an increase in adoption across all age groups [368], with ages 25-34 adoption rates increasing from 24% to 38%, ages 55-64 from 6.5% to 13.2% [368].

Wearable form factors such as head-mounted devices (HMDs) (e.g., devices worn above the

neck, in the ear, or on the face); and wrist-worn devices (WWDs), along with related applications and services permit users to collect personalized data. This data may include details about physiological parameters, including heart rate and blood pressure, location data, steps taken throughout the day, food intake, and sleep patterns [158, 202, 236, 266]. Consumers are enthusiastic about how they can visualize and analyze their health-related data, set and meet goals, and improve their overall behavioral patterns and quality of life [14, 102, 178, 234, 255, 305]. These components give wearable technologies increasing potential to improve the quality of healthcare and progress personal wellness and pubic health for all through early detection of diseases and personalized treatment of medical conditions [140, 178, 202, 246].

Despite the prevalent adoption and acceptance of wearable technologies [118, 124, 266] several risks and concerns related to the collection and sharing of personal information exist and continue to arise [118, 202, 322]. Scholars note privacy as a fundamental concern among adopters of ubiquitous technologies [314, 349]. More recent scholars also note privacy as a key concern for wearables [20, 118, 190, 232, 234, 266, 274]. Wearables collect and transmit large amounts of physiological, and environmental data that some users consider harmless [202, 234, 246, 265, 281, 313]. Sensors on wearables facilitate in continuously collecting personal information about a user, while processing and further aggregating this data [28, 118]. Wearables are not primarily designed to address privacy related issues [379]. As a result, adoption may expose users to privacy-related threats, often without their acknowledgment or consent [118, 190, 202]. Over time, this data can disclose an accurate representation of an individual's identity [118] possibly becoming what Lowens et al. refer to as "a skeleton in the data closet"[202]. For example, the popular fitness application, Strava unknowingly revealed the precise location of military personnel on active service, along with their fitness activity and habits [311]. Other popular fitness trackers (e.g., Fitbit) has had several privacy vulnerabilities associated with user personal health information. For example, in 2011 Fitbit users found that named categories of identifiable data disclosing their activity data could be found via a simple Google search [283]. In other instances, users may be aware of the privacy-related risks posed by wearables, but may not be able to negotiate complex and unusable privacy settings that meet their needs and preferences [202]. Though the concerns exist, issues relevant to privacy and wearable technologies are still poorly understood by users [118, 202, 281] and not appropriately addressed by stakeholders [84, 121, 202, 236]

2.1.1 Theories on Privacy

There is a noticeable effort from previous literature on theories of privacy management that treat privacy as a nuanced process. [23, 31, 252, 268, 353]. For example, Westin describes privacy as an individual's ability to control the conditions in which their personal information is collected and used [353]. Other works focus on privacy based on the sensitivity of information [7, 249] while others evaluate privacy as awareness and control over personal information [209]. Private information belonging to an individual or a group of individuals should be protected and not disclosed to third parties without that individual's intention, and consent [114]. To ground my research within a more recent theoretical framework of privacy, I looked to Contextual Integrity (CI) [41, 244], and the behavioral privacy model [52] to situate our work within the larger theoretical work on privacy particularly relevant to the experimental design I adopted in this dissertation.

In contrast to theories of privacy that define privacy as control over information about oneself (e.g., Westin [353]), CI is a philosophical model of privacy that views privacy from the lens of ethics. This model suggests that appropriate information flows are those that conform with contextual information norms that evolve over time [244]. The concept of contextual integrity [243] was introduced as an alternative benchmark for privacy, demanding that data collection and distribution be suitable to that context and observe governing norms of distribution within it. Private data should have a corresponding degree of confidentiality that aligns with specific user needs. When considering privacy for personal health information (PHI) collected from wearables, this model may not be suitable because the attribute can only be a type of information, and the subject is primarily only the user themselves. Moreover, PHI from a wearable is an important parameter that is not covered in the CI model. More recent theoretical analysis of privacy in computing systems has posited the application of CI "is not ready for prime time" and that CI still needs to be sharpened or expanded to be more actionable to computer scientists"[41]. Limitations in the application of CI for computing systems indicate its dependence on the system architecture and also different interpretations of "context" within the literature[41].

The psychological model of behavioral privacy [52] describes behaviors such as avoidance (e.g., deciding to withhold data prior to collection due to concerns), modification (e.g., making a privacy decision in-the-moment), and alleviation (e.g., making a privacy decision after some data is collected). This model also identifies two elements that could affect a users' privacy - *content* and

recipient of information [52]. In the wearable privacy domain, *recipient* can be viewed as the receiver of personal information (e.g., health care provider or employer) along with the *type* of information which can be interpreted as sensitive or positively or negatively valenced. While we are informed by all the theories previously mentioned, this dissertation is driven by Caine's behavioral privacy model. [52] Framing our work within Caine's model suggests that we focused on participants' binary decision (e.g., share or withhold) over data from a wearable in the experimental design noted in Chapter 3.

2.1.2 Privacy Risks Unique to Wearable Technologies

Prior research in wearable computing has explored different aspects of users' privacy including, but not limited to user concerns, attitudes and behaviors about privacy [19, 54, 108, 118, 121, 131, 156, 185, 190, 217, 234, 274, 373]. In the section, I present and discuss related work, highlighting privacy risk unique to wearable technologies and privacy regarding to health information.

Wearables provide users with feedback about location, fitness and activity levels, nutrition habits, sleep habits, physiological indicators, and other vital signs [147]. Consequently, due to interconnectedness and increased adoption of wearables by consumers and health care providers, a complex challenge emerges concerning the protection of sensitive information and potential for information leakages [111, 179]. Similar to mobile phones, wearables continuously collect personal information about the wearer and their interaction with the device. Unlike mobile phones, wearables are attached to the body of the wearer for extended periods of time [155]. Despite the advantages of wearables and potential for societal benefits in terms of improved health [246], managing privacy with these technologies is increasingly difficult, mainly because the data collected is personal to the wearer [377]. Moreover, there is also the potential for behavioral inferences (e.g., location, demographics, health status, emotional state) that could be made about the wearer without their awareness or consent, which could pose a severe threat to their privacy [179, 181, 282].

Physiological and environmental data produced by wearables can comprise sensitive information that can be looked at as emergent medical records [140]. This data can insinuate records of one's activity levels that could be potentially used by a third party to evaluate an individual's health and well-being, possibly impacting insurance benefits, costs, or health premiums [140, 246, 313]. Wearable devices are also often synchronized with social media sites for sharing information, which presents additional privacy risks [140]. Criminal actions may also be planned using location information collected by wearable devices shared on social media sites. For example, a thief may plan a

robbery according to the analysis of displacement patterns of individual users [356]. Previous works also identified privacy as a critical concern associated with wearable devices from the user perspective [190, 232, 314]. Because of these unique concerns, scholars have explored user perspectives and concerns related to the privacy of wearables.

2.1.2.1 User Perceptions and Perspectives Over Data Generated By Wearables

Several studies have examined users' perceptions and perspectives of sharing data from wearables on different platforms and different recipients [132, 190, 234, 274, 356]. For example, Prasad et al. [19, 118, 274] investigated users' willingness to share personal information collected via a wearable with family members, friends, third parties, and the public through a social experiment. During this study, participants wore a wearable that used accelerometer data to estimate their calories burned, steps taken, and sleep quality. Following the study, participants were interviewed to understand their sharing behavior. This study suggests that participants have dynamic sharing behavior when it comes to sharing data from a wearable. For example, study participants prefer to share demographic information less than sensed information. This study also showed that participants share personal information more with strangers than their family members and close friends. The results suggest that flexible controls are needed to support individual preferences for sharing. Thus, in chapter 3, I further explore user preferences for privacy and sharing of data generated from a wearable device based on recipient, type, and valence of data to understand what types of data users are more willing to share and if that preference is contingent on the recipient of the information. In Chapter 4 I further explore what interface mechanisms that would allow proper privacy control over data from a wearable.

Lee et al. investigated the perception of the general public linked to the risk of information disclosure associated with wearables through a survey of internet users [190]. The findings from this work suggest that privacy and security are at the top of users' overall concerns. The results from this study also indicate that users' self-reported privacy preferences correspond to how they may react, even in situations they are unfamiliar with. While this work provides insight into user acceptability about data disclosure and general user concerns about wearable devices, 83% of participants from this study reported they did not own a wearable device. As the researchers mentioned, participants may not have a clear sense of the technology and may be overestimating or underestimating the risk associated with the use of wearable devices. Thus, I only recruited participants who owned wearable

devices in studies mentioned in Chapters 3,4 and 5

Gorm and Shklovski [132] examined privacy about wearable health technologies in the workplace through an observational study. This work challenged the assumption that users are becoming comfortable with perceived risks with wearable technologies. In this work, the scholars conducted a study of a workplace health promotion campaign that depended on the use of step counting technologies and daily self-reporting of steps over three weeks. This research explored the types of concerns employees express about disclosing step counts and how they change over time. Findings from this work suggest a difference in concerns toward data disclosure to organizations that support health promotion campaigns between people who chose to participate in health promotion campaigns versus those who do not. This study also illustrates that concerns over data disclosure to employees, bosses, or friends change over time. Although these results offer insight into privacy concerns toward wearable health technologies in the workplace, being held responsible for tracking physical activity at work can be unwelcoming for users and may be quickly abandoned when the intervention is complete [132].

Using a qualitative content analysis of online comments from wearable device users, Motti and Caine [234] identified the privacy concerns of wearable users who commented online. Findings from this work suggest that users' privacy concerns about wearables are similar, but some cases are more specific than privacy concerns for mobile devices in general. Findings from this work also illustrate that users have perceptive awareness of impending privacy implications of wearable devices, but mainly during data collection and sharing. This work also claims that users' concerns about wearable privacy cover different aspects of user interaction with wearables, and in some cases, users are somewhat oblivious to potential privacy implications associated with using wearables. While this work offered valuable contributions to research on wearable privacy and provided general insights on users' concerns about it, this work collected data anonymously from online comments and did not know much about the user's profiles and demographics from the study population sample. Also, the methods in this study employ a relatively new research approach that is both exploratory and empirical and does not have a well-established and validated protocol concerning data collection and analysis.

To further understand why people use wearables despite the privacy risks Wieneke et al. [356] conducted in-depth interviews with 22 wearable users in a qualitative study, that examined the perceived values of wearables that drive individuals' usage and disclosure of their data and the reasons

why these values outweigh the privacy risk of wearable usage. The findings of this study reveal eight values (e.g., social belonging, social acceptance, contentment, exploration, success, health, and self-optimization, and quality of life) that individuals perceive through the use of wearable devices. The results suggest that users are willing to disclose personal information if they expect the perceived value of that information will outweigh the perceived risk.

In a qualitative study of wearable users, Alqhatani and Lipford [19] explored users' sharing goals and practices, and privacy concerns associated with their wearable device. This study also examined what users do to manage their privacy. Findings illustrate that users are primarily concerned about acceptable norms and self-presentation [125] associated with their wearable data and less concerned about the sensitivity of the data. Researchers believe this factor impacts what types of information people are willing to share and with whom they are willing to share it with. By examining user perspectives regarding sensitive information from wearables, findings show that users do not perceived fitness data as sensitive similar to prior work [260]. This limited perspective may lead to users not taking the appropriate actions to protect their data, leaving them exposed to privacy-related threats.

As illustrated in prior works, people have different perceptions over data generated by wearables. While some users are concerned about potential threats to privacy over data from wearables [190], in some cases they may have a limited perception over the risk imposed by the use of wearables [356] and may not be aware of the potential privacy implications associated with using wearables [19, 234]. In the following section I further explore how lack of awareness over how wearable data in handled poses an even greater threat to user privacy.

2.1.2.2 Lack of Awareness of Data Practices and Inferences Posed by Wearables

Several studies have examined users' understanding about personal information collected by wearables [15, 202, 280, 301, 341, 356]. Findings from these works suggest that users have a limited understanding of the data practices of organizations that develop and distribute wearables and are unaware of the potential inferences made based on the data collected by their wearable. For example, in a qualitative study that explored why the perceived value of using wearables prevail over privacy risk associated with their usage among wearable users, Wieneke et al. [356] illustrates that users have limited knowledge about the privacy consequences of using a wearable device. This study also demonstrates that many users do not want to invest the time and effort required to understand

how their data can be used and potentially exploited by stakeholders. Participants in this study also noted that the perceived risks of using wearables did not influence their decision process and tended to ignore the likelihood of negative consequences.

Findings from a qualitative study by Lowens et al. [202] reveals that users have an incomplete understanding of privacy risks associated with wearables and, at the same time, their privacy concerns vary, ranging from no concern to highly concerned. Those that were not concerned consider "daily activity" data not very sensitive. Participants also believed that the lack of a physical keyboard on the device prevented them from entering and storing sensitive information, leading to a false sense of privacy. Additionally, the authors found that the users often had no idea about what type of data and how much data is being collected and stored by these wrist-worn devices. Those concerned about their privacy were aware of risks associated with their data but were still willing to give up confidentiality. Users were also worried about the lack of control they have over how their data is used.

In an online survey of wearable users, Vitak et al. [341] investigated how users value personal health information generated from wearables, how much they know about the data collection policies of fitness tracking companies, and how their sharing behaviors compare to their overall privacy concerns and protection strategies. Findings from this work reveal that users have a general lack of knowledge of company data collection practices. Results also suggest that general privacy concerns and data sensitivity play a significant role in how users value their personal information.

Radar and Slaker [280] conducted semi-structured interviews with current and former users of wearable devices to investigate the impact of folk theories [120] about data collected by wearables. Before the interviews, participants completed a free list activity that elicited folk theories. The findings from this study demonstrate that users' folk theories about data from wearables are contingent on the interactions between the users and their wearable. While these beliefs help users speculate about the dependencies toward types of data wearables collect, participant folk theories did not support their understanding of what additional information can be inferred from the data collected by their wearable. For example, none of the participants in the study who mentioned the data types GPS, location, or distance said their tracker could infer where they live. This lack of understanding poses a threat to their privacy and does not allow them to make informed choices regarding sensor-related data collection. We know from prior work [279] that people who have a greater awareness of data aggregation techniques tend to have a greater understanding of concerns

toward undesirable inferences and take action to mitigate these concerns.

To further explore users' data practices and understandings related to wearable privacy, Gabriele and Ciasson [118] explored users' knowledge, attitudes, and behaviors related to privacy associated with the use of their wearable through an online survey. Findings demonstrate that users do not believe certain inferences can be made from data collected by their wearable. Results illustrate that users are unaware of how easily wearable data can be manipulated and used negatively. Users are also unaware of the potential threats posed by the collection of personal data from a wearable. When presented with plausible risks scenarios based on sharing activities, participants believe threat scenarios are possible, but they do not think they would occur. As a result, users do very little to protect their personal information.

Schneegass et al. [301] also explored users' understanding of inferences that can be made from wearable sensor data. This study also assessed users' willingness to share potentially private information from a wearable when the data is collected on the sensor level. Findings demonstrate that users' understanding of the relationship between the data collected by the sensor and the information that can be derived from sensor data is limited, especially among non-expert users. Study participants underestimate the risk of using their wearable and are unaware of the types of information inferred from their wearable. Findings also suggest that the type of derived information impacts users' willingness to share. Users seemingly prefer to share information that can be inferred as positive (e.g., step count) compared to information that can be inferred as negative (e.g., stress). In chapter 3, I further examine user sharing preferences over data from wearables to understand if the valence of the data impacts their sharing preferences with a given recipient. We learn from the review of this literature that designers of wearable technologies must consider granular control options in their design of wearables [19, 118, 202, 274]. It is also crucial that designers educate users on the potential privacy risk associated with personal information collected by a wearable to encourage them to take control of their personal information to reduce privacy-related threats [118, 279, 301].

While prior works have investigated and provided insight to these concepts, wearable computing faces dynamic changes and widespread adoption. There is a need to better understand current users' behaviors and concerns in regard privacy risks, concerns and wearable technologies [49, 88, 121, 165, 356] which is the motivation behind this dissertation. In the next section, I discuss some existing solutions that researchers have already proposed to mitigate privacy related risk posed

by wearables.

2.1.3 Existing Solutions

Through our extensive review of the literature, I find that solutions to address issues with wearable privacy vary. Prasad et al. [274] suggest that users have dynamic sharing behavior, and flexible controls are needed to support preferences. Because users have dynamic sharing preferences, data collected by wearables should be clearly presented to users, and the controls should be easy to use. Lowens et al. also suggest that users should be aware of what type of data is collected from wearables, how that data is collected, and when it is shared and with whom it is shared with [202]. Results from this study also suggest that transparency can reduce the misuse of personal health information from wearables and suggests that data collection and transmission should be precise and reliable to reduce critical consequences from the mishandling of personal information, and granular controls should be implemented on wearables to support dynamic sharing preferences as noted by [274].

From a more practical standpoint, Epstein et al. [107] considers a value-sensitive design approach [115] to consider whether and how users share step activity. Scholars suggest this type of design as an opportunity to understand privacy and data sharing in Ubiquitous computing [53]. Using this approach, Epstein et al. [107] focuses on methods for transforming fine-grained activity data before sharing. Authors also develop interface designs that provide users with unmodified data, a high-level summary of the data, and the options to delete data prior to sharing. Considering these factors, they develop a new approach to interactively transforming data that attempts to preserve the benefits of sharing while giving people greater control over what they share. To evaluate their approach, authors conducted in-person semi-structured interviews to understand how people respond to fine-grained sharing methods. Findings illustrate that people have concerns about with whom fine-grained data is being shared with. Based on these findings, researchers suggest the importance of interface designs that allow people to share data in a usable way. While this work only explored step data from wearables, authors suggest that sharing other data types may benefit from fine-grained sharing.

In a study that evaluates the potential exposure of users' identity caused by information shared from personal fitness trackers, Aktypi et al. [15], develops an identity exposure tool that models information shared by users and elaborates on how uses may be exposed to unwanted leakage

of personal data from wearables. The tool identifies attributes that users might be expected to share and automatically customizes these attributes based on users' choices and builds a personalized list of inferences and risks, and then filters data and clarifies the risk of exposure based on the data. Results from the qualitative analysis show that users' awareness concerning the risks encountered can be classified as minimal. Furthermore, the authors suggest that by using the interactive tool, users could better identify the risks associated with data exposure from wearables and adopt proposed mitigation techniques to safeguard their privacy [15].

Adopting a user-centered approach to address user's privacy concerns when using wearable technologies, Wagner et al. [345] proposed a privacy awareness framework that assesses and improves privacy aspects for users when using these technologies. In a research study, authors analyzed privacy concerns that arose from collecting data from mobile applications and demonstrated how this framework could be applied for wearables to communicate privacy-related threats and offer solutions to reduce these threats. Authors suggest a systematic consideration of alerting and mitigation options in which can improve user privacy among users of wearables while preserving the functionality of the device and offering control over sensitive from these devices [345].

While many research efforts and solutions have been proposed relating to privacy challenges associated with the usage of wearable technology, topics that focus on these concepts deserve more attention [58] from a user-centered perspective. In the next section, I will discuss privacy controls for wearables and the challenges associated with these controls.

2.2 Privacy Controls and their Challenges

Privacy controls are defined as "settings available within an app or an operating system that allow users to make or revise choices offered in the general privacy policy about the collection of their personally identifiable data" [141]. We know that when privacy controls are flexible and adequately designed, they help users become aware of data practices, alleviate potential privacy-related threats and unwanted disclosures caused by technological systems, and allow users to make informed decisions over their data [297, 327, 332]. However, privacy controls are historically ineffective at affording users control over their personal information [296]. One challenge that designers are faced with is designing controls that are usable and effective for privacy management [296]. Even on large devices, privacy management is complex [157]. Thus, it is not surprising that privacy controls on

wearables have been challenging to design from a user interface perspective [202, 296, 298].

Privacy controls have been challenging to design for wearables because wearables have constrained interaction capabilities. Most wearables have very small visual displays or, in some instances, no visual display at all [265, 298]. For instances where there is no visual display most information handling is decoupled from the device and relegated to an external mobile device or manufacturer's website [265, 298]. Because of the lack of input space and constrained interaction capabilities available on wearables, privacy controls are often decoupled from the wearable device [298]. For example, the Apple Watch uses the Apple health app to organize and manage data. To adjust any permission, a user must have a smartphone, have the app, and have connectivity between the watch and phone. While the app gives a user the option to disable permission, disconnect the app, or entirely delete data, these all must be done proactively or retroactively. The app does not give users any granular options for control.

Furthermore, if a user has concerns about what type of data is being shared, they must set up activity sharing through the app and choose specific friends to ban from receiving future data. For wearables that use the google fit app, users must also manage data sharing via a phone app. Fitbit also requires a phone app for privacy management. Decoupling privacy management from the wearable makes it difficult for people to maintain effective control over personal information on wearables. Consequently, wearers have a difficult time making informed privacy decisions about the data collected about them from their device [265]. Providing usable and effective mechanisms that enable wearers this type of control can be challenging. Despite these challenges, wearables present a feasible on-device method for input [27, 306], even though the input space is limited.

In this dissertation I look to discover interaction mechanisms that can enable usable control over data from wearables. In the next section, I discuss different input modalities that can be used for interaction with wearables.

2.2.1 Input Modalities for Interaction with Wearables

Interacting with wearables requires new types of interactions. Whereas a laptop has a keyboard and mouse, and a smartphone has a touchscreen, wearables may not have any of these user interfaces. Several studies have explored alternative and novel interaction techniques for devices without a traditional graphical user interface [27, 248, 315, 358, 361]. Those techniques include: gaze based interaction for hands-free interaction [109, 312], speech-based interaction for web-browsing

using the Kinect [226], gesture-based interaction for interactive table tops [361], mobile phones [293], large interactive displays [22] and smartwatches [27, 155, 169]. Supplementary studies [16, 58, 183, 334] have also explored alternative input techniques in the IoT domain for wearable technologies. One interaction modality that has been commonly explored in this domain is using gestures as a complementary input modality for wearable devices [27, 199, 270, 306]. Gestural interfaces offer a more natural method of interaction than traditional input devices such as keyboards and mice and promise to have many wide-reaching benefits [27, 222].

In the following section, I discuss prior works that have looked to gestural input as a mode of interaction with a technological system and the methods that are used to come up with a set of interactions.

2.3 Elicitation Studies for Input Interactions

2.3.0.1 Goals of Elicitation Studies

The elicitation method is a popular participatory design technique [164, 303] that is used to understand an individual's preference for providing input to some interactive technology [336, 361]. This method has been applied to the development of user-defined interactions for a wide array of emerging interaction and sensing technologies including single-handed and bimanual gesture interaction on tabletops [361], motion gestures for interaction with mobile devices[293], hand gestures in augmented reality [270], ring gestures [122] interaction with a Kinect for TV web browsing [226], interactive hats [92], gestures for mobile phone motion [293], non-touchscreen gestures for smartwatch interaction [27], and gestures for pen-based interactions [113]. In an elicitation study, participants are provided with the results or effect(s) of performing a task or action, which is termed the *referent*. After receiving (e.g., hearing) the referent, they are asked to produce or "design" an interaction that they feel best matches the result or effect. In addition to collecting elicited interactions, in some cases, think-aloud data, semi-structured interview data, or Likert scale responses to behavioral questions are also collected. The end goal of most elicitation studies is the development of a user-defined set of interactions. Most end-user-defined sets of interactions are analyzed by using quantitative and qualitative metrics.

The primary motivation for elicitation studies over other potential methods is that interaction sets derived using this method result are more learnable and preferred by users [201]. When

comparing user-elicited and expert-elicited interaction sets, Morris et al. discovered that interactions proposed by end-users are not only different from expert-elicited interactions but are indeed favored over the expert elicited sets [228]. In terms of learnability, Nacenta et al. [238] identified that user-defined interactions produced during interaction elicitation studies were more practical and easier to remember than predefined interactions. One possible reason elicitation studies may be better than other methods is that system developers and designers may not share the same conceptual models as the end-users [241]. Therefore, this method may provide interaction design practitioners valuable information during the early design stages, conceivably shaping design decisions and product characteristics for more effective and efficient interaction with a given technology or application [226, 334, 361].

Wobbrock et al. [360] introduced and popularized the user-elicitation method as a unified approach to maximize and empirically evaluated the guessability of symbolic input to an interactive system. In Wobbrock's initial work [360] this approach was applied to increase the guessability of the unistroke EdgeWrite alphabet [362]. In this study, participants were asked to draw an icon representing a command that was classified as the referent, which was originally defined as the results/effects of performing a task or action [218]. The icon participants drew classified as the proposal for the given referent. Through the application of this participatory design technique [164], Wobbrock contends that the learnability of a system can be improved, while guessability can be quantified and compared for an existing character set or toward the design of a new set [360]. The evaluation was facilitated by the computation of the level of agreement, which shows the level of consensus among participants for a given referent [360].

As I've just described, evidence from prior elicitation studies demonstrates that elicitation studies - as an emerging participatory design approach - may result in user-defined interactions that are more memorable and discoverable than to interactions designed by experts. [228, 361]. The outcome of the majority of these types of studies include quantitative and qualitative metrics, and characterization of users' input interaction behavior [344] containing useful information to guide interaction designers toward understanding and developing effective interactions with a given application or interactive system [27, 344]. In the next section, I describe the metrics used in elicitation studies.

2.3.0.2 Metrics / Criteria Used In Elicitation Studies

To identify a non-conflicting gesture set, the most commonly proposed gestures are grouped across participants for each referent by calculating an agreement score. Wobbrock et al.'s [361] level of agreement metric has been applied as the method of quantitative evaluation in several elicitation studies [93, 112, 293, 306, 309, 335, 337]. Level of agreement is used to examine consensus between an individual's interaction preferences using the formula shown in Equation 2.1. This equation 2.1, P_r represents the set of all gestures proposed for referent r and P_i represents groups of similar commands. The agreement rate A_r ranges from $[|P_r|^{-1}, 1]$.

$$A(r) = \sum_{P_i \subseteq P_r} \left(\frac{|P_i|}{|P_r|} \right)^2 \tag{2.1}$$

Beyond level of agreement and agreement rate metrics, additional metrics in elicitation studies include time of thinking (before proposing an interaction)[93, 152], consensus distinct ratio [82, 226], and max-consensus ratio [82, 226]. To assess agreement and identify interactions that are most common among all participants in the study mentioned in Chapter 5, I adopt Morris's [226] metric of consensus (max-consensus and consensus-distinct ratio) as this method accommodates an arbitrary number of interactions proposed per referent [226].

The max-consensus ratio is equal to the percentage of participants that suggest the most commonly proposed interaction for a referent using Equation 5.1, while consensus-distinct metric is the percentage of distinct interactions proposed for a specified referent that achieved a specific consensus threshold among participants [226].

$$Max - Consensus = max \left(\forall_{P_i \subseteq P_r} \left(\frac{|P_i|}{|P_r|} \right) \right) \tag{2.2}$$

2.3.0.3 Legacy Bias as a Limitation of the Elicitation Method and its Remedies

While the elicitation method has proven a useful method for understanding an individual's preference for providing input to some interactive technology, using this method does have its challenges and limitations [294]. During the study's design, these limitations should be acknowledged and addressed to avoid any pitfalls. One substantial limitation with elicitation studies is *legacy bias* [227].

Legacy bias is the phenomenon in which end-users propose interactions based on experience

and familiarity with how interfaces tend to function [42, 227, 228]. This bias could potentially limit the production of interactions that take full advantage of the application domain, form factor, or sensing capabilities of the interactive system. This type of bias could also be associated with the lack of understanding of the fundamental capabilities of the technology in use. Legacy bias is a noted pitfall of prior elicitation studies [27, 309, 361] since it may have limited the potential of that work to develop interactions that take full advantage of the sensing modalities of emerging technologies.

Fortunately, legacy bias can be offset with the strategies proposed by Morris et al. [227]. Those strategies include production, partners, and priming. The production technique requires participants to propose a variable number of interactions for each given referent and has been demonstrated to increase the variety and creativity in output in other domains [227]. The partnering technique suggests recruiting participants in groups rather than individually to leverage ideas in a collaborative effort. The objective of the priming technique is to give the participants an idea of the possibilities of interactions or gestures they might produce. I adopted these techniques in the study mentioned in Chapter 5 to reduce legacy bias. Although legacy bias has been noted as a limitation in prior elicitation studies, Köpsel and Bubalo [176] argue that legacy bias can also have some positive effects. Their work implied that biased interactions have the advantage of being simple, learnable, and more discoverable, resulting in higher agreement scores in such studies. In addition, legacy bias may also be helpful toward introducing new forms of interaction for novel interfaces. [176].

While prior research has explored the potential of alternative interaction modalities with wearable devices that can be done in the air, using one hand, using the head and shoulders or around the device, using gestures [12, 122, 143, 344], these studies focus solely on interactions to execute common navigational tasks. In this dissertation (Chapter 5), I propose using device-independent interactions (e.g., gestures) as an input mechanism to enable usable privacy control over personal information for wearables. More importantly, the decision to elicit any input modality is based on the notion that our exploration of potential interactions should not be constrained to a single device or existing sensors.

2.3.1 Summary of Literature Review.

To ground my work that aims to generate user-defined interaction set for privacy control on wearables, I looked to prior work in wearable privacy and interaction elicitation. Prior work has empirically investigated end-users perceptions, preferences, behaviors and concerns over personal

information collected from wearables [38, 140, 202, 237, 274, 342]. Other work has developed gesture sets for head-mounted devices and wrist-worn devices [27, 169, 248], two of the most common categories of wearables [235].

Based on the literature review, I did not come across any prior work that has joined these separate research streams of wearable privacy and novel interactions to produce usable privacy controls for wearable technologies. Thus, there are still many unanswered questions about interaction design mechanisms that would enable individuals to have usable privacy control over personal information produced by wearables.

Henceforth, my research aims to address these limitations and propose a practical and usable way for users to maintain control over personal information from wearables.

Chapter 3

Study 1: Privacy and Sharing Preferences for Health Information Generated by Wearables

3.1 Introduction

Advancements in mobile and ubiquitous computing have enabled patients to engage in their personal health and wellness. Often this engagement is facilitated by the use of wearable technologies [105]. Wearable form factors such as HMDs, and WWDs have added a new dimension to understanding human behavior as it relates to healthcare [21] and fitness [83, 106, 117, 132] outside of a clinical setting.

Many medical devices can collect, store, and analyze data within a clinical facility (e.g., blood pressure, heart rate, etc.)[49]. Medical professionals can use extra-clinical data (ECD), which is health data generated outside of a medical facility [49], to inform patient treatment [74] and provide actionable insights about quality of health and well-being [96, 225, 317]. Often, ECD can be collected without uncomfortable, or expensive clinical devices [271]. For example, conditions like sleep apnea can be monitored and improved using WWDs [291] where heart rate, breathing, and snoring are captured. ECD from other wearables can assist medical professionals with screening, diagnosing and monitoring depression [367] by using sleep and physical activity data [271]. ECD

from wearables is also useful for individuals interested in systematically tracking and analyzing everyday health related behaviors[46, 320].

While the widespread collection and sharing of ECD from wearables [19] are useful for medical professionals, and those interested in improving health-related outcomes, there are several privacy risks associated with the disclosure of different types of ECD from wearables [15, 118, 140].

Types of Data The types of ECD collected by wearables include steps, activity data, heart rate, stress levels, sleep patterns, and food intake[9, 118, 382]. While participants in prior studies classify categories of ECD like exercise, steps and heart rate as unlikely to threaten their privacy [39, 118, 237, 275], scholars suggest that some categories of ECD (e.g., mood, sleep quality, blood pressure, stress levels) constitute sensitive information [140, 266, 274]. These types of information can serve as a de facto health record [191] identical to the kind of information protected by HIPPA, posing a significant threat to user privacy. This data could be used to impact a wearer's insurance benefits or health premiums, for example. [37, 74, 131, 181, 182, 205, 281, 292]. While there are varying privacy concerns over types of ECD from wearables, any data gathered about an individual's health status is personal[49, 313]. The continuous collection and potential sharing of this ECD from a wearable put the wearer at risk, especially without proper privacy controls available on these devices to handle this information.

Valence of Data In addition to the data type (e.g., heart rate, food intake), data valence influences disclosure decisions [19]. Valence is the affective quality of intrinsic "good"-ness or "bad"-ness of an "event, object, or situation" [116]. For example, positively valenced data (e.g., you met your calorie goal today) would be perceived as intrinsically good, whereas negatively valenced data (e.g., you did not complete your step goal) would be perceived as bad.

In general, people prefer to share positive achievements over negative outcomes [19]. Being able to control how others perceived them might be one reason people choose to manage sharing decisions about data rather than sharing it automatically on social networks[19, 180].

Recipient of data Wearables further exacerbate privacy risk by allowing sensitive data to be disclosed to a variety of potential recipients, potentially without the knowledge of the user about who might receive such data [15, 63]. For example, social features on wearables enable wearers to share data from wearables with health care providers [6],family members and close friends, followers

on social media [133, 145, 239, 254, 256, 318, 325, 381], and employers[64, 99, 131, 202, 234]. While some wearers are comfortable sharing ECD with health care providers, or close family members [118, 275], they are less comfortable sharing ECD with employers, where sharing could leased to unintended consequences [275] or compromise their privacy [37]. For example, researchers found people are concerned their personal information might be used by others they did not intend to share with, and people fear negative impacts on relationships with those who can access their data [275]. There is also concern that inferences made by certain recipient groups (e.g., employers, insurers, creditors, retailers)about data from wearables may cause undesired outcomes that could disqualify a wearer from employment, insurance benefits, and reasonable health premiums [140, 265].

As noted in Chapter 2, the behavioral privacy model identifies content and recipient as potential factors that may influence privacy when used in combination [52]. While empirical evidence suggests that type, valence, and recipient of ECD from a wearable may influence privacy and sharing decisions and related privacy risks, [19, 118, 145, 202, 274, 275] there are no studies that I know of that quantify preference level for those factors or examine them in combination. Leveraging the behavioral privacy model [52], I investigate this topic from a Human-Centered perspective to understand sharing behaviors based on type, recipient and valence of data. I believe examining these factors will inform the design of effective privacy protection schemes for wearables that give users effective and usable control over ECD generated by wearables.

3.2 Background and Significance

We already know the importance of studying privacy and control over data from an electronic medical record(EMR)[50]. However, as the collection and sharing of health information become more pervasive outside of a clinical setting, it is also important to understand privacy and control over ECD collected by wearables. Any health information collected and gathered about an individual should be kept private [49] and used only at the discretion of the producer of the information.

While most commercial wearables collect ECD similar to data collected within a clinical setting (e.g., sleep patterns), such devices are not typically used for treating illness [313]. Because health care providers do not typically use data from wearables for treatment, these devices are not covered by federal privacy laws [37, 313] to treat an illness, such devices are not covered by federal health privacy laws [37, 304, 313]. However, most users do not understand this distinction. People

believe the privacy rules of HIPAA protect "all" types of health information [49]. As the collection and sharing of health information becomes more pervasive outside of a clinical setting, it is essential to understand people's disclosure decisions over ECD collected by wearables. Any health information gathered about an individual should remain private [49] and used only at the producer's discretion.

HIPPA did not expect wearable technologies to pose threats th users privacy [37]. Current regulations either do not entirely protect ECD from wearables or are antiquated and cannot keep up with the increasing legal challenges created by wearables that collect ECD [15, 265]. Although the Federal Trade Commission (FTC) is making efforts toward protecting the privacy of health data [313], there are currently no regulatory guidelines to protect health data, specifically ECD from wearables [149]. Sophisticated classification systems that aggregate ECD from wearables could enable profiling and discrimination based on demographic disparities and medical conditions [184, 224]. Such analysis could impact not only individual consumers but also groups – especially those already at risk – and society at large [224].

While empirical evidence suggests that patients want more control over access to data stored in an (EMR) [50], the literature about ECD data is limited [118]. Key HCI questions that emerge from the expansion of wearables and ECD collection are: What factors influence ECD disclosure decisions from a wearable? Specifically, do the type, the potential recipient, and the valence of data influence disclosure decisions respectively? To answer what factors influence privacy and sharing decisions over ECD from wearables, I designed a study to elicit privacy decisions using a scenario-based experimental design, which used a combination of type, recipient, and data valence as stimuli to explore disclosure decisions. The following section outlines the study's methodology.

3.3 Method

In this portion of the dissertation, we assess privacy preferences for sharing ECD collected via a wearable device. Using a 4 (type) x 4 (recipient) x 2 (valence) within-subjects repeated measures scenario-based experiment we assess adopters(AD's) and potential adopters (PAD's) of wearable technologies preferences for sharing extra-clinical health information collected via a wearable device. Participants in this study completed two questionnaires and a scenario-based experiment that elicited participants sharing preferences over data collected from a wearable.

The study protocol was approved by the Clemson University Institutional Review Board.

3.3.1 Participants

Thirty-two participants were recruited via flyers posted around the Clemson University campus (See Figure 1 in Appendix A). We targeted participants who owned at least one wearable (ADs) or those who had na interest in owning a wearable (PADs). Because we are interested in ECD collection from a wearable, we did not require participants to be current patients or fulfill any specific health criteria. As such, beyond the requirement of being an AD or PAD, there were no other inclusion or exclusion criteria. Upon expressing interest, potential participants were scheduled for the experiment.

3.3.2 Materials

Questionnaires Participants completed a demographic questionnaire that included questions about age, race, employment, and educational background. Additionally, we asked questions to assess participant's technology experience, wearable device ownership, and views on privacy .

Both questionnaires were implemented and administrated via Qualtrics. All questions are reproduced in the Appendix A (See Figures 5-8).

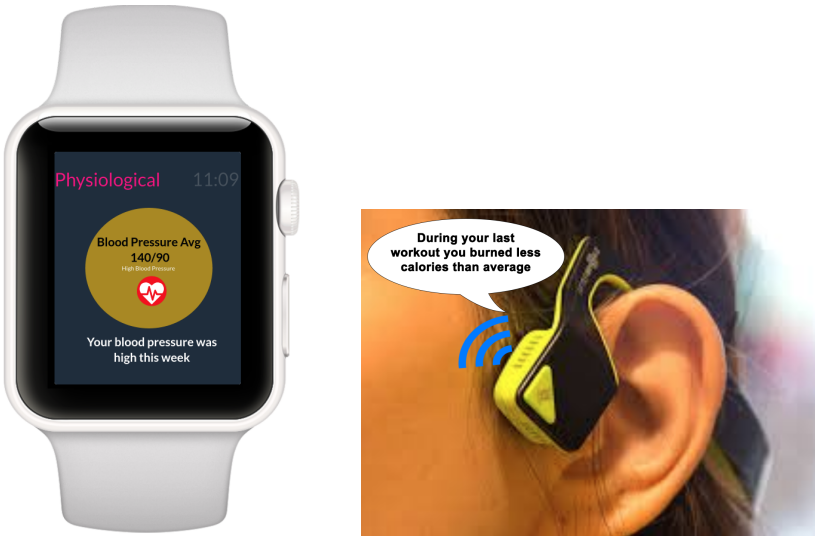
Apparatus Participants received stimuli via two wearable devices: (1)WWD- an Apple Watch Series 2 38mm (see Figure 3.1a) and (2) HMD -a pair of Aftershokz Bluez 2s Open-ear Wireless Bone Conduction Headphones (see Figure 3.1b). Stimuli from the WWD was presented visually, while auditory stimuli were presented via the HMD.

3.3.3 Experimental Design

We used a 4 (type) x 4 (recipient) x 2 (valence) within-subjects repeated measures scenario-based experiment to assess the effects of the independent variables (recipient, type, and valence of data) on the Dependent Variable (sharing preferences). The DV sharing preferences was operationilized as a binary yes/no sharing intention.

3.3.3.1 Predictor Variables

Type of Data We identified four types of ECD to use as stimuli in our experiment(see Table 3.1): activity (e.g., steps, workout summary)[136, 326, 363], sleep (e.g., sleep quality, hours slept)[81, 110,



(a) Scenario presented Via WWD

(b) Scenario presented via HMD

Figure 3.1. Stimuli presented to participants via two wearable devices. Fig. a shows the WWD, and Fig. b shows the HMD

Independent Variable and Levels	Description
Type of Data	
Activity Data	You Met Your Step Goal For Today (+)
	You did not meet your step goal for the day (-)
	During your working you spent over 45 mins in the Fat Burn Zone (+)
	During your last workout you burned less calories than average (-)
Sleep Data	You met your sleep quality goal(+)
	You did not meet your sleep quality goal (-)
	Sleep goal met for the week (+)
	Sleep goal not met for the week (+)
Physiological Data	Stress Levels Indicate you were calm today(+)
	Stress levels indicate you were anxious today (-)
	Your blood pressure was normal this week (+)
	Your blood pressure was high this week (-)
Food Intake Data	Today you met your calorie intake goal (+)
	Today you exceeded your calorie intake goal (-)
	Today you met your healthy eating goal (+)
	Today you did not meet your healthy eating goal (-)
Recipient of Data	
Healthcare Provider	Primary medical professional or doctor
Family and Friends	A spouse, parent, sibling, close friends, and significant other
Employer	Organization you work for who provides income
Broader Social Network	People you may have connected with through social media
	(e.g. Facebook, Linkedin), but do not know personally

Table 3.1. Independent Measures and Description (as provided to recipient)
Note: (+) or (-) indicates valence of scenario. (+) indicates positive valence and (-) indicates negative valence

159], physiological (e.g., blood pressure, stress levels)[269, 281, 319, 359, 363], and food intake data (e.g., healthy eating goals, calorie consumption)[161, 216, 290]. Each type of data was operationalized using two scenarios. Several studies suggest that wearers' privacy concerns vary based on the type of data collected by the device [118, 234, 274, 281]. For example, results from prior studies suggest that people are more willing to share ECD collected from a wearable (e.g., steps calories, and sleep) than their personal traits (e.g., age, gender, height, etc.)[274].

Recipient of Data We investigated four categories of ECD recipients:healthcare providers, broader social network, family and friends, and employers. We chose data recipient as an IV because several studies demonstrate that people make disclosure decisions based on who the information is shared with [51, 63, 64, 70, 133, 180, 239, 254, 274, 275, 318, 325, 357, 381]. People may share ECD with a healthcare provider to help treat or monitor a health-related condition [274, 380], with family members or close friends for accountability [202], with contacts on social media sites for emotional support [133, 180, 234, 239, 254, 318, 325, 381] or even with an employer for insurance discount programs [99], or health promotion campaigns and competitions [64, 131].

Valence of Data We also evaluated sharing preferences related to data valence (e.g., whether data was positive or negative). We include valence as an IV because prior research suggests that self-presentation influences how users make disclosure decions over wearable data [19] Participants from this study desired to only share data that communicated a positive image about their health and fitness [19]. To our knowledge, there is no prior work that has empirically evaluated how valence affects ECD sharing preferences.

3.3.4 Scenario Design

We used a randomized fractional factorial design to create the scenario stimuli for the experiment [135]. Each scenario described an instance where a wearable device collected some ECD about the participant (see Figure 3.2). We randomly assigned each participant to a block of 12 experimental trials (See Table 3.2). The information shown in figure 3.2 was randomized per participant. An example of the 12 scenarios a participant may have saw are shown in table 3.2.

The scenarios presented via the HMD included two of the four categories of data (e.g., activity, food intake), and the scenarios delivered via the WWD included the other two categories

Scenario	Device	Type of Data	Environmental Context	Social Context	Scenario	Recipient of Data
1	HMD	Physiological	at home	alone	Stress Levels Indicate you were anxious today	Employer
2	HMD	Food Intake	at work	alone	Today you exceeded your calorie intake goal	Broader Social Network
3	HMD	Food Intake	at home	with others	Today you met your calorie intake goal	Employer
4	HMD	Food Intake	in public	with others	Today you met your calorie intake goal	Health Care Provider
5	HMD	Physiological	at work	with others	Stress Levels Indicate you were calm today	Broader Social Network
6	HMD	Physiological	in public	alone	Stress Levels Indicate you were anxious today	Family and Friends
7	WWD	Sleep	in public	with others	You did not met your sleep quality goal	Health Care Provider
8	WWD	Activity	at home	alone	You met your step goal for today	Broader Social Network
9	WWD	Activity	at work	with others	You did not meet your step goal for today	Family and Friends
10	WWD	Activity	in public	alone	You met your step goal for today	Health Care Provider
11	WWD	Sleep	at home	with others	You did not met your sleep quality goal	Employer
12	WWD	Sleep	at work	alone	You met your sleep quality goal	Family and Friends

Table 3.2. Experimental Trials Presented to Participants

of ECD (e.g., physiological, sleep). We assigned half of the participants to one of the two scenario descriptions for each level of the factor type of data. For example, half of the participants received the step goal description for the activity data condition, and the other half received the workout summary description. Following the scenario for each experimental trial, we asked participants to report their binary sharing decision for each recipient of data. To prevent carryover effects [307], we used complete counterbalancing, meaning we arranged the experimental trials so that every possible sequence of each IV level was presented to all participants once during the study.

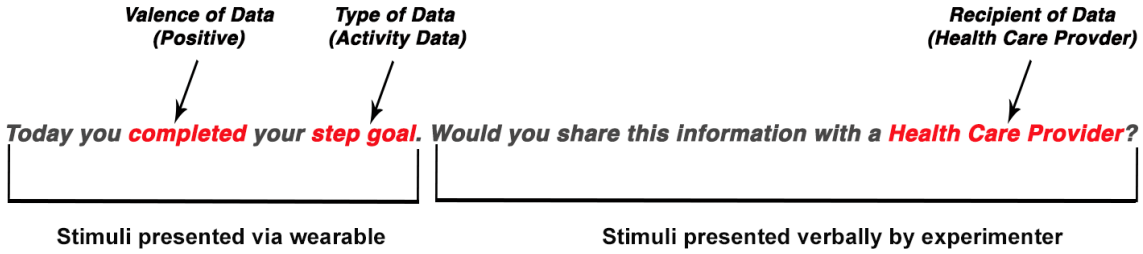


Figure 3.2. An example scenario used as stimuli for the experiment.

3.3.5 Procedure

Before the experiment, participants provided informed consent and completed a questionnaire (See Appendix A Figures 2- 8). Upon arrival, the experimenter reaffirmed consent. Next, the experimenter defined each potential recipient of data to participants, described the scenario

presentation method, and instructed participants to provide a binary response of 'yes' or 'no' for each decision. Participants received the first experimental scenarios via the HMD. After hearing the audio for each scenario, the experimenter asked participants, "Would you be willing to share this information with [recipient of data]?" The recipient factor was randomly drawn from one of the levels of the recipient of data.

Following the completion of six scenarios using the HMD, the procedure was repeated on the six scenarios via the WWD. The only change was that participants received a visual prompt rather than an auditory prompt. After participants completed every scenario, we asked whether they had any questions For participants who owned a wearable, we also interviewed them about their privacy concerns with wearables. Then, participants completed a post-survey questionnaire (See Appendix A Figures 9-12). Following the experiment, participants were remunerated with a $20 gift card. The entire in-person session took approximately 30 minutes and the experimenter sat in the same room as the participant for the entire session.

3.3.5.1 Analysis

To understand the effect of the independent variable (*type, valence, and recipient*) on the dependent variable (sharing preferences) we used a generalized linear mixed-effects (glmer) multilevel regression model with a random intercept to account for repeated measures. We conducted the regression analysis in R [324] using a forward step-wise procedure, adding the strongest remaining IV to the model at each step, and then comparing it against the previous model using ANOVA.

3.4 Results

The following sections report results of descriptive data gathered about participants' demographics and sharing preferences regarding data recipient, type, and valence, and the results from the main regression analysis.

3.4.1 Demographics

Table 3.3 shows participants' demographic characteristics. We excluded data from three participants because they did not meet the inclusion criteria of owning/being interested in adoption a wearable. The final sample size was 29 participants. Just over half of participants from our

	N = 29
Gender	
Male	13 (45%)
Female	16 (55%)
Age	
18-24	19 (66%)
25-34	8 (28%)
35-44	2 (7%)
Education	
High school grad	4 (16%)
Some College	6 (19%)
Four Year College	9 (28%)
Some postgraduate	3 (9%)
Postgrad or Professional	7 (28%)
Ethnicity	
White	19 (66%)
African American	4 (14%)
Asian	5 (17%)
Other	1 (3%)
Technology Knowledge	
Basic	2 (7%)
Intermediate	12 (41%)
Advanced	9 (31%)
Professional	6 (21%)
Wearable Device Ownership	
Potential Adoptors	6 (21%)
Adoptors	23 (79%)
Own any Wearable	23 (79%)
WWD	21 (72%)
HMD	14 (48%)
Both	18 (62%)
Participant Views On Privacy	
Being In control of who can get information about you.	
Very important	14 (48%)
Somewhat important	14 (48%)
Not very important	1 (3%)
Somewhat important	0 (0%)
Being able to share confidential matters with someone you trust	
Very important	24 (21%)
Somewhat important	5 (79%)
Not very important	0 (0%)
Somewhat important	0 (0%)
Controlling what information is collected about you	
Very important	14 (48%)
Somewhat important	14 (48%)
Not very important	1 (3%)
Somewhat important	0 (0%)

Table 3.3. Participant Demographics. Note that for wearable device ownership, the numbers do not sum to 100 because participants can be counted in multiple categories.

sample were women (55%, n=16), while slightly less than half (45%, n=13) were men. Participants ages ranged from 18 to 44, with the majority of participants (66%) between 18 and 24 years old. Participants were highly educated and also tech-savvy, with 66% having at least a four-year college degree or higher and over half (51%) having advanced or professional-level technology knowledge. Seventy-nine percent of participants were ADs, whereas 21% of participants were PADs. We also collected data on participants' views on privacy from three different privacy control perspectives: recipient of information, type of information collected, and sharing confidential information with a trustworthy person. To understand these three perspectives, we chose a questionnaire created by The Pew Research Center that examined Americans attitudes about privacy, security, and surveillance[75]. Similar to findings by Pew, 87% of participants in our study reported that being in control over who can get information about them is at least "important." All participants reported being able to share confidential matters with someone "very important." Ninety-six percent of participants reported controlling what information is collected about them as "important."

As noted previously, nearly half of the participants in our study had advanced or professional-level technology knowledge. Nearly 90% of participants from this group considered "being in control over who can get information about them", as important or very important. All participants with advanced or professional-level technology consider "being able to share confidential maters with someone they trust" as important or very important. Over 90% of participants considered "controlling what information is collected about them" as important or very important.

3.4.2 Would participants share everything with a given recipient?

Descriptive data was compiled to determine whether participants reported they would share *at least something*(e.g., any single data point from the scenarios), *everything*(e.g., all data points from the scenarios), or *none*(e.g., no single data point presented in the scenarios) of the data with a given recipient across the scenarios. Each participant made 12 binary decisions indicating whether they would prefer to share or keep private the information identified in the scenario.

	Something	**Everything**	**Nothing**
Any Recipient	83%	0%	17%
HealthCare Provider	76%	34%	24%
Family and Friends	55%	14%	45%
Employer	31%	0%	69%
Broader Social Network	34%	0%	66%

Table 3.4. Percentage of participants who something, everything, or nothing

Table 3.4 summarizes the percentage of participants who would share any data with a given recipient across the 12 scenarios. We find that 83% of them would share at least something with any given recipient, but none of the participants would be willing to share everything with all of the recipients. Further, 17% of participants would not share at least something with any of the recipients for all scenarios in the condition.

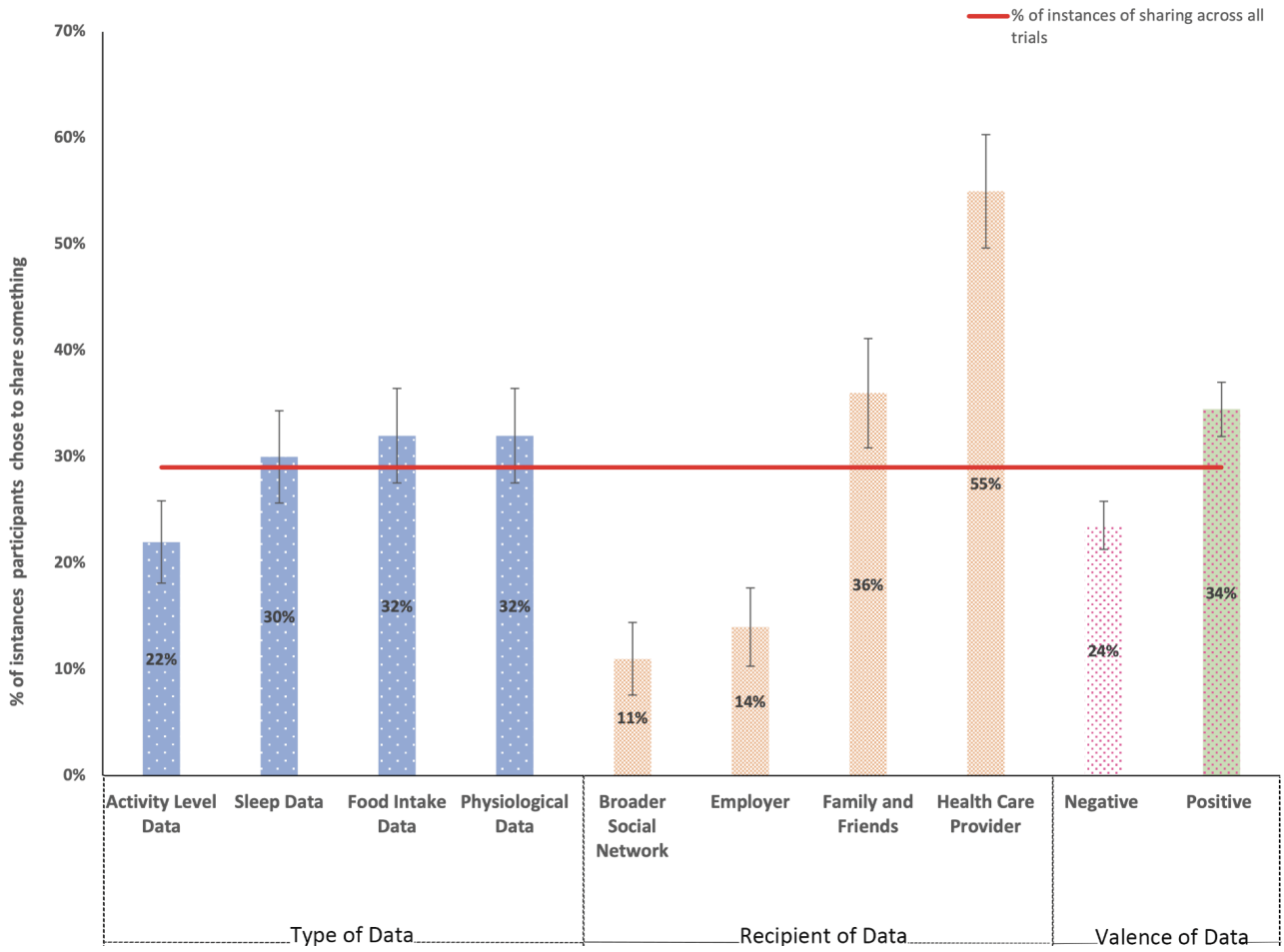


Figure 3.3. An overview of the differences between levels of the IV for the type of data, recipient, and valence categories. **The red bar signifies percentage of instances people would be willing to share at least some type of data (29% indicates overall instances of sharing)

The results reported in Table 3.4 also show that sharing preferences vary per recipient. For example, 34% of participants would share *everything* presented in the healthcare provider scenarios, yet only 14% would be willing to share everything with their family and friends and no participant would share *everything* with an employer or member of their broader social network. While we

see that slightly over one-third of participants would be willing to share everything with a healthcare provider, nearly one-fourth (24%) of participants would not share anything with a healthcare provider.

3.4.3 Instances of Sharing Across Experimental Conditions

3.4.3.1 Instances of sharing across all independent variables

To further understand participant sharing preferences for each IV, we compiled additional descriptive data to determine the percentage of instances across all trials participants chose to disclose their ECD based on the type of data. We also examined the percentage of instances across trials where participants chose to share something with a given recipient of data and the percentage of instances where sharing was contingent on the valence of the data (Figure 3.3). Across all trials, we find that participants are generally least likely to share ECD from a wearable regardless of type, recipient or valence. Figure 3.3 shows that across all trials, participants would share data only 29% of the time. Figure 3.3 also shows that participants slightly differentiate instances of sharing between the types of data. Across all trials, participants are least likely to share activity data in contrast to sleep, food intake, and physiological data. For the recipient of data category, participants most likely share their data with a health care provider and family and friends across all trials and are least likely to share data with an employer and someone from their broader social network. Across all trials, participants are also more likely to share positively valenced data than negatively valenced data.

3.4.3.2 Instances of recipient sharing based on the type of data

Table 3.4 shows the instances of sharing across all participants considering the type of data shared with a given recipient. As we see from the descriptive statistics, participants are generally more likely to share data with their health care provider and family and friends. When we consider health care provider, there is not much difference between the types of data participants would share with this recipient group (See Figure 3.4). We do see that participants were least likely to share activity data compared to the other types of data with a health care provider. When we consider family and friends, participants were more likely to share physiological data with this recipient group in contrast to the other types of data. When considering someone from their broader social network

and employer, participants were overall less willing to share personal information with these recipient groups. Across both broader social network and employer recipient groups, we find that participants were more willing to share food intake data in comparison to the other types of data.

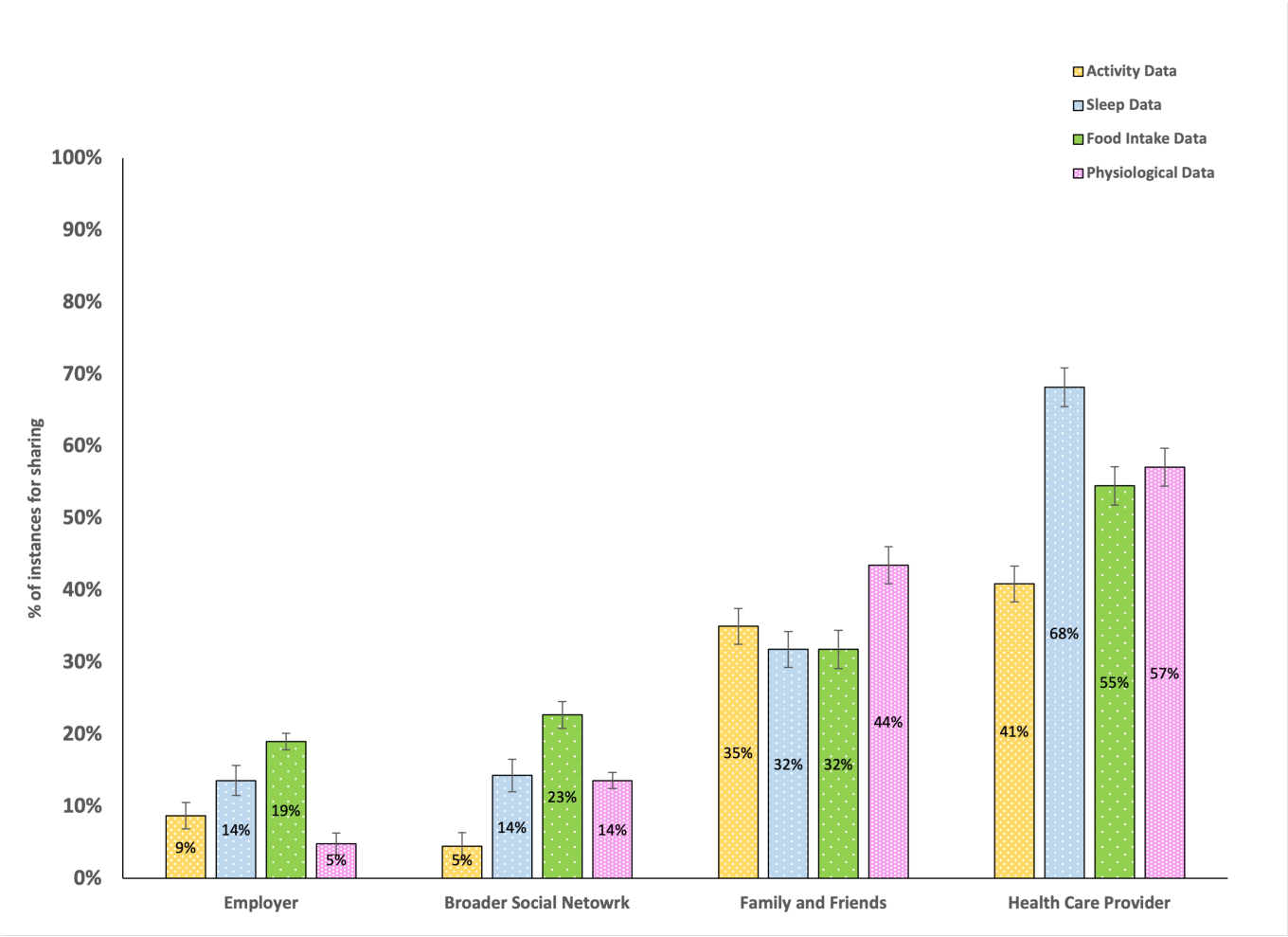


Figure 3.4. An overview of the differences in sharing based on type and recipient of data

3.4.3.3 Instances of sharing based on type and valence of data

Figure 3.5 shows descriptive data for the instances of sharing based on type and valence of data. As the graph shows, participants were least likely to share negative data, and more likely to share positive data across all trials for each type of data. Figure 3.5 also shows there was not much difference in sharing for positively and negatively valenced physiological data across trials. Participants were least likely to share negative activity data in contrast to all the other types of

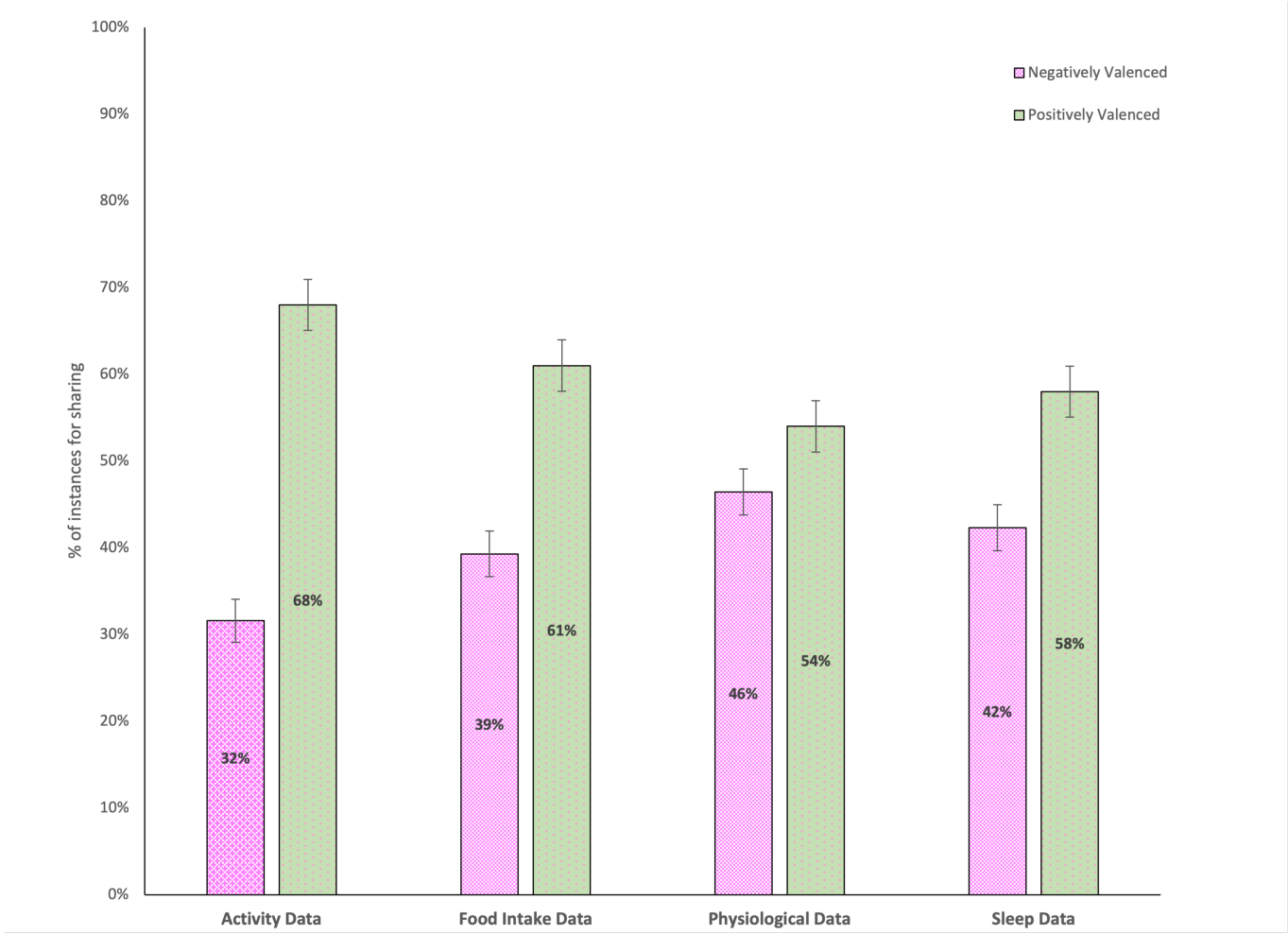


Figure 3.5. An overview of the differences in sharing based on type and valence of data

data.

3.4.3.4 Instances of sharing based on recipient and valence of data

Table 3.6 illustrates differences in sharing for participants across all experimental conditions considering the recipient of data and valence of data. Descriptive data show that participants were generally more likely to share data regardless of valence when the data recipient is a health care provider. For the family and friends recipient group, participants were more willing to share positive data than negative data. Participants were generally least likely to share data with an employer or member of their broader social network regardless of valence. When participants did choose to share with members of these recipient groups, they more likely to share positive data than negative data.

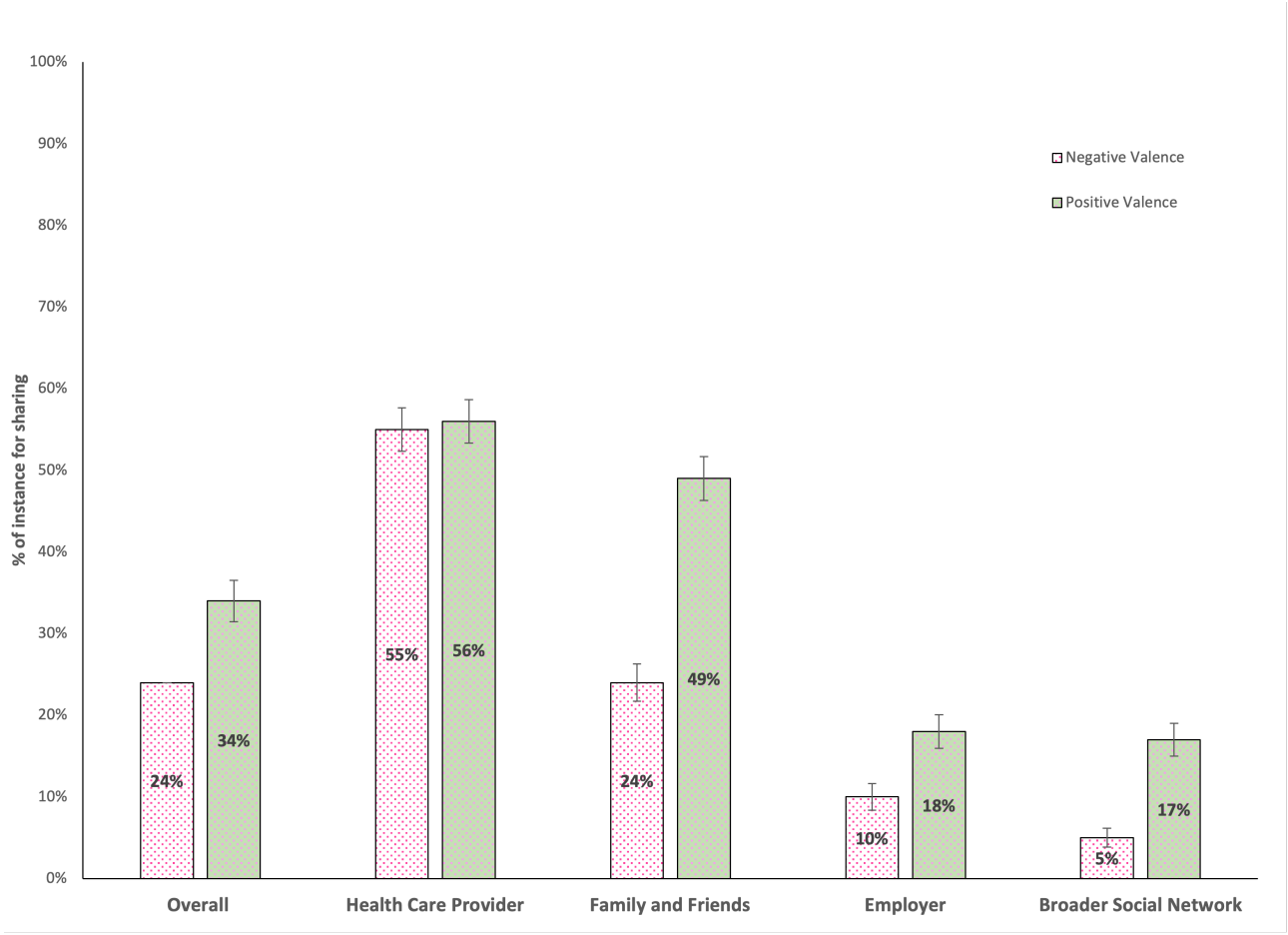


Figure 3.6. An overview of the differences in sharing based on recipient and valence of data

3.4.3.5 Factors that influence privacy disclosure preferences

Table 3.5 shows the effects of the IVs on the share/withhold decision. We find there were no significant interaction effects present at either the two-way [type and recipient (p=0.870), type and valence (p=0.524), or valence and recipient (p=0.657)] or the three-way (p=0.463) type, recipient, and valence) levels. Given the lack of interaction effects, we examine the main effects and find that all IVs had a significant effect, except type (p=0.2872 see Table 3.5).

To understand the effects of each IV on participants' preference for sharing, we calculated the odds ratio for each level of the IV that had a significant main effect. For the IV recipient, the levels of family and friends, and healthcare provider had a significant effect on participants' sharing preferences compared to the baseline recipient broader social network. This result shows that participants are 6.63 times more likely to share ECD with family and friends (p <.001), and

Model	df	Chi.Sq.	p-value
sharing preferences ~(1|pid)			
+type	3	3.77	0.287
+recp	3	69.90	<.001
+valence	1	9.76	<.001
Interactions			
+type:recipient	9	4.57	0.870
+type:valence	3	2.23	0.525
+valence:recipient	3	1.61	0.658
+type:valence:receipient	24	23.97	0.463

Table 3.5. Effect of Sharing on each IV

23.58 times more likely to share ECD with a healthcare provider (p <.001), than with someone from their broader social network. For the IV valence, there was a difference in sharing preferences for the IV valence also. Odds of sharing positively valenced data were 2.63 more likely (p <.001) than odds of sharing negatively valenced data. Figure 3.6 shows an overview of the differences between levels of the IV.

3.5 Discussion

This study considered factors influencing sharing decisions over ECD from a wearable based on the type, recipient, and valence of data. Indeed descriptive statistics show that type, potential recipient, and valence of information influence disclosure decisions, respectively. While our regression analysis did not find a significant main effect on disclosure decisions for type of data, nor an interaction effect between the type of data and recipient of data, we see a significant main effect for the recipient, and valence of data could be considered as type. These results demonstrate that privacy behaviors of ADs and PADs fall within the avoidance category from the behavioral privacy model [52]. This behavior refers to actions that people take to avoid undesired privacy disclosures before they occur [52]. A solution to this behavior is to provide ADs and PADs more granular options over ECD from wearables. Our findings further demonstrate that people desire granular control options over ECD from wearables when they are available, similar to results from early studies investigating the desire for control over information stored in an EMR [50] and Personal medical record (PMR) [65]. The difference is that wearables are a novel class of health technologies that afford health data collection outside of a clinical setting. Wearables are primarily unregulated to protect consumer privacy, limiting privacy protections to the device policy [9]. While ECD from a wearable may im-

prove a person's health, facilitate care, support the management of ongoing conditions, [39], or help a wearer keep track of their health behaviors and status, health data generated by wearables is comprised of sensitive information. This sensitive information can impart itself as an emergent medical record [140] as noted in Chapter 2. These factors present an increasing risk to users (e.g., privacy misclosures [52]), oftentimes without their consent or knowledge [63, 118, 202, 219, 234, 329], These implications demonstrate the need for more granular control options over ECD from wearables to reduce privacy-related threats.

3.5.1 Sharing by recipient

Apart from understanding privacy preferences for ECD generated by wearables, we were also interested in how preferences vary across potential recipients of this information. The primary goal of this work was to understand users' preferences for sharing ECD data with diverse recipients. Our results demonstrate that the potential recipient of the information is the most critical factor influencing participants' choices, with 24 of the 29 willing to share at least something with a given recipient. Moreover, we find that five participants were not willing to share anything with any recipient. Our results illustrate that participants are selective in their sharing preferences, as noted in the privacy behavioral model [52]. We find that none of our participants would share all the data presented from the scenarios with each recipient completely, similar to previous work [50]. This result reveals that AD's and PAD's privacy decisions are dynamic and that flexible and granular controls [118, 274] should be available on emerging wearables that accommodate the wearer's privacy preferences for sharing data with a personalized recipient group. While some level of customized sharing is available for specific types of data on some wearables, personalization choice for recipient is limited [118]. For example, in the Fitbit privacy setting interface, the only options for recipients are "Friends" or "Public." Furthermore, only people who have a Fitbit account can be added as a "Friend." Qualitative results from prior works also show that participants express frustration with the available methods to share data with a healthcare provider [19]. As a result, designers should consider frameworks that allow centralized privacy control [19] over health data from a wearable that is integrated with an EMR to share data with this recipient group if desired. This control should be seamless and should not burden the wearer [118].

We evaluated the results of each data recipient independently because individuals' preferences for sharing with their healthcare provider, family, and friends were significantly different from

sharing with employers and members of a broader social network. This finding is in line with Caine's behavioral privacy model [52] that illustrates how the recipient of data is a factor that may influence privacy decisions, and adjusting this factor may affect privacy.

3.5.1.1 Sharing by Health Care Professional

Compared to other recipients, most participants were more willing to share ECD with a healthcare provider, regardless of the type of data, and 11 participants were willing to share everything if the recipient was a healthcare provider. We know from prior work that people are more comfortable sharing ECD with health care providers because it may help manage personal health goals and result in positive health-related outcomes[19, 65, 202]. Prior works also demonstrate that people are more comfortable sharing ECD with a health care provider because they believe a health care provider will keep their information confidential [274]. While we did not find a significant interaction effect between type and valence from our regression analysis, descriptive statistics (See Table 3.6) show very little difference in sharing positive and negative data with a health care provider. While prior research suggests that self-presentation influences privacy decision [19], we do not see this as a concern for sharing with healthcare providers. While we did not provide any justification to participants why their ECD would be shared with this recipient group, prior studies postulate that a wearer's intention to share ECD with healthcare providers is often associated with an ongoing medical condition. Based on this context, individuals would be comfortable disclosing data to this recipient group[19]. Despite most participants being likely to share information with healthcare providers, seven participants were unwilling to share anything with a healthcare provider. One of these participants reported that they stopped using their wearable device due to a lack of control over their data (P12). This result corroborates the need for more seamless control that is not burdensome to the wearer and gives them the option to share or withhold data from whom they prefer.

3.5.1.2 Sharing with Family and Friends

When we consider family and friends as the recipient of data, participants are willing to share ECD with this group more than with an employer or member of their broader social network. In comparison to healthcare providers, participants were less inclined to share everything with their family and friends (see Table 3.4). While prior research suggests that individuals are most comfortable sharing data with friends as a recipient group [118], authors do not provide examples of

each recipient group, as we did in our procedure. Participants may not have a clear understanding of the differences between groups if examples are not provided. This study also did not explore healthcare providers as potential recipients. Results from our experiment illustrate that only four participants would share everything presented in the scenarios with family and friends. We also find that nearly half (45%) of participants reported they would not share anything with their family and friends. While we did not gather specifics of why participants were less willing to share with family and friends in comparison to a healthcare provider, prior studies suggest that individuals trust their doctor with health data more than their family and friends [275].

In some cases, individuals may feel obligated to share health data with a healthcare provider because of a health-related issue[18], as noted above. We do see from Figure 4 that participants prefer to share positive data over negative data with family and friends. When considering this recipient group, self-presentation may be a determinant that drives minimal sharing of negatively valenced data among participants as evidence from prior work [19].

3.5.1.3 Sharing with an Employer

Our study demonstrates that ADs and PADs are significantly less willing to share PHI with an employer than healthcare providers or family and friends. This result is consistent with previous research that also investigated sharing behaviors with employers [118, 131]. Prior studies demonstrate that individuals have concerns sharing personal information with an employer due to undesirable decisions and inferences that can be made based on the data being shared [65, 116, 131]. For example, qualitative results from [107] reported that participants would not like it if someone from their job had access to data showing they were up late the night before. This information could also be synced with other data to compare sleep quality across employees working on different projects [197], which raises additional privacy concerns about how much information employers should know about their employees' behaviors [118]. Employees may also perceive sharing ECD with an employer as beneficial under certain circumstances (e.g., incentivized health tracking programs) [64]. If there is a situation where people do choose to share data with their employer, granular control options are needed where they can selectively share information with this recipient group and withhold information that may be deemed as more sensitive or private.

3.5.1.4 Sharing with Broader Social Network

While prior research shows that ADs are motivated to share ECD on social media with others who share similar goals[81, 110], our results show that among ADs and PADs, sharing ECD with a member of this group is less likely to occur. Before the experiment, we explicitly define this recipient group to participants as someone they may be connected with through social media but may not know personally. We believe this definition made our participants more cautious about whom this information could be shared and made them less likely to share with this group. Currently, most wearables only offer general categories (e.g., friends and public) as the potential recipient of shared data [275]. While the friends' group could be someone a wearer knows, wearers could be connected to individuals based on activity from boards or challenges they have completed or activity within the app community. For example, one Fitbit community member posted on a message board [1] "I have about 100 friends on my list....and I know 3 of them in my non-digital world." This implies that 97% of the individuals this wearer shares their data with are members of their broader social network (i.e., someone they don't know. As we see from our results, ADs and PADs are significantly less likely to share ECD with a member of their broader social network in comparison to someone they know in a "non-virtual" world. This could be taken as evidence that the term 'friends' is misleading in the sense that a wearer believes they are sharing ECD with someone they are close with, but in reality, their data is shared with someone they do not even know. This could be considered a dark pattern in UX [144]in which the design is used to increase wearer engagement to share more of their ECD, but in reality, this is an undesired behavior. Our results bolster prior research findings that suggest the need for granular privacy control options over ECD from wearables when data is shared within broader social networks [145]. Designers should consider control options for wearables that support granular sharing options when sharing data with members of a broader social network. These options should allow people to modify privacy settings around their needs and goals and understand what types of information is being shared and with whom that information is being shared with, and the option adjust those preferences accordingly [19].

In the context of wearable privacy, previous studies analyzed form factor, type of data collected, type of sensors used to collect data, perceived risk and concerns toward the type of data collected, and potential recipient of data[21, 25, 28, 39, 47]. However, we have not found scientific publications or industrial guidelines that provide adequate support for designers to build

privacy-preserving controls for wearables. Moreover, prior work has not quantified the levels of user preference for the type, recipient, and valence of ECD collected by a wearable. Since no similar models are reported in previous literature, our work is the very first to contribute to quantifying users' preferences for sharing by leveraging the privacy behavior model [52]. Such quantification is valuable to facilitate the implementation of privacy controls for wearables that automate the configuration process for privacy control matching user needs.

3.6 Limitations

While we designed our recruitment methodology to minimize response bias, our participant sample was more educated than the general population [47], and the population of fitness tracker users [343]. This could introduce bias to our sample. While many of the risks associated with the collection and processing of PHI could affect anyone, potential harms are more likely to affect the most vulnerable populations in our society, including those with the least education [224].

The recruitment of a participant sample from a specific geographic location and age range of younger participants may threaten the ecological validity of the study. Therefore, we cannot expect our results to generalize to other populations. While studies have shown that wearables mostly appeal to younger adults, the usage among older adults is rising [368]. Hence, future work should further explore this demographic to understand the extent better and whether the results obtained can be generalized across the entire population.

Similar to prior work[70, 274], our results show that the recipient of data was an important factor in the sharing of health data among participants. Nevertheless, we did not explore any specific circumstances in which the specified recipient would need the participant's personal information and what level of granularity would be most beneficial to the recipient. These factors could further affect the decision to share personal data, further influencing design aspects for privacy-enhanced wearable technologies.

Lastly, while our study could benefit from a larger sample of participants in a naturalistic setting, this work sheds light on understanding ADs and PADs willingness to share PHI from a wearable. We expect these findings to hold broadly for additional types of information generated from a wearable (e.g., location, breathing patterns, motion, etc.) and additional recipients of data (e.g., third parties). General privacy settings for all wearable devices may not be feasible, given the

variety in sharing behaviors among individuals for different types of information and other recipients.

As noted in the results section, participants in our study were highly educated and tech-savvy. This tendency toward the sample having highly educated and tech-savvy people could be due to convenience sampling. This result also could reflect the fact that we targeted adopters and potential adopters of wearable technologies.

3.7 Chapter Conclusion

While our results are not surprising, it is critical to understand that ECD collected on consumer wearables lends itself as an emergent medical record [140], posing significant privacy risks to users if misused.

This scenario-based experiment demonstrates that if people are offered privacy control options over ECD from a wearable, they exhibit granular control preferences over how their data is handled. Our results show that sharing decisions are primarily contingent on the recipient of the information and whether that information is positive or negative. We find that participants are more willing to share ECD with a health care provider or family and friends and are less likely to share this information with their employer and broader social network. We also find that valence did not influence sharing with a healthcare provider. However, participants were more willing to share positively valenced than negatively valenced ECD with other recipients. These results reveal that privacy-enhanced personalized granular controls are needed for wearables to accommodate the wearer's privacy during and beyond the use of the device. The results also suggest that user interface options are needed so users can execute this type of control. This experiment promotes and protects user privacy over ECD from wearables to reduce privacy-related risks and threats that could negatively impact ADs and PADs of wearable technologies. Now that we understand that people have granular control preferences over ECD from a wearable, in the next chapter, I investigate different interface options for wearables that would be more suitable for people to make granular privacy decisions.

Chapter 4

Study 2: An experiment to assess the impact of location of privacy controls and decision timing.

4.1 Introduction

In the previous chapter, I investigated user preferences for privacy and sharing extra-clinical health information generated from a wearable device. Results from this study show that data recipient and valence of data impact privacy and sharing preferences; participants were more willing to share extra-clinical data with healthcare providers and family and friends than with their employer or broader social network. Participants were also less willing to share negatively valenced data (e.g., you did not complete your step goal) than positively valenced data (e.g., you achieved your step goal). Now that we know users have granular sharing preferences over health-related data from a wearable, it is essential to understand what user-interface mechanisms would allow usable, granular data sharing on wearables.

While wearables and mobile devices are paired wirelessly through communication protocols, privacy controls and notice of data practices are decoupled from the wearable (e.g., located on a separate web portal) and not integrated into the user's interaction flow due to system constraints and limited screen space [296]. These constraints make it challenging to design and provide usable

privacy mechanisms for wearables [69, 297]. It may be helpful to decouple certain privacy notices and controls that provide information about data practices (e.g., privacy policy documents) from a wearable due to limited screen space [296]. However, the decoupling of privacy interfaces from wearables poses disadvantages, as well. Being forced to exert privacy control on a separate device (e.g., a mobile phone or web portal) presents several usability challenges. For example, Fitbit requires users to view and manage their Fitbit's privacy options through a web dashboard [177]. In this case, control is separate from the data-collection device. The user cannot make actionable privacy choices when data is produced unless they have immediate access to their mobile phone or computer. If they have access to their phone, it may be a chore to pull out the device every time they adjust their privacy settings.

Instead, users need context-dependent and in-the-moment privacy controls where they can actively manage their privacy when the data is produced [68, 163, 259, 296, 297, 299] directly on the device that is producing the data. In a report on mobile privacy disclosures, the Federal Trade Commission (FTC) recommends that privacy researchers and developers consider designing systems that provide disclosures of a specific data practice (e.g., collection of some health data) at the moment. The FTC also recommends that systems be designed to allow the user to provide affirmative consent before sharing personal information. Researchers believe this approach will enable users to make informed choices over their personal information related to the information collected and the recipient of that information. In a workshop on advertising and privacy disclosure in a digital world, participants noted the importance of in-the-moment privacy disclosures. Also, they pointed out that these types of controls should be clear and understandable [68]. In prior works, timing [33, 103, 129, 163, 258] has been shown to have a significant impact on the effectiveness of privacy notices. Studies have illustrated that displaying untimely notices may result in users ignoring the notice [297]. Patrick and Kenny [259] suggest that technologies that leverage just-in-time privacy disclosures support more appropriate decision-making and control techniques sensitive to human factors constraints.

Furthermore, Kelley et al. [163] found that a privacy display's timing could help users make privacy decisions. Schaub et al. Schaub et al. [297] also note that providing context-specific notices may help users make privacy decisions aligned with their desired level of privacy and reduce perceived threats caused by a lack of contextual control. These findings and recommendations from past research suggest that leveraging both in-the-moment and contextualized control options in the

design of privacy controls for wearable technologies will produce more effective privacy outcomes for adopters and potential adopters of wearable health technologies.

Wearable technologies offer increasing opportunities to enhance privacy control because of the unique set of sensors that are standard on most devices [284]. The same sensors used to detect a range of physical activities (e.g., accelerometers, gyroscopes) give wearables the potential to integrate sharing decisions with privacy interfaces and offer control at the moment. For example, several works have used standard sensors on wearables to sense a myriad of interaction techniques (e.g., tap, swipe, press, handwave, head nod) as a form of input to a wearable [13, 30, 48, 92, 122, 128, 366, 371, 378]. I believe these sensors can be leveraged as an input mechanism for integrated, in-the-moment privacy control for wearables. However, it is essential to consider system interaction opportunities and constraints to develop proper control mechanisms in the context of privacy [296]. It is also important to understand what interface mechanisms would be usable for a user to make these decisions. If enhanced privacy controls are built into a system, but these controls are not perceived as usable or effective by users, it is unlikely they will be adopted. It is also important to understand what interface mechanisms would allow a user to make these decisions. If enhanced privacy controls are built into a system, but these controls are not perceived as usable or effective by users, it is unlikely they will be adopted. Thus, it is important to understand both what features afford greater privacy outcomes and how to design these features to promote a positive user experience. In designing privacy-enhanced controls for wearables, I believe a useful first step is to explore system interface aspects for wearables, as suggested by Schaub et. al [297] and user perceptions of these aspects in order to develop usable and effective privacy controls for these devices.

When thinking about interface mechanisms that would allow proper privacy control, it is important to consider decision timing and location of control. Schaub et al. [297] maps the design space for effective privacy notices and provides a taxonomy of design features for privacy notices and controls within the IoT domain [297]. This design space and taxonomy highlight the relevant design opportunities for privacy notices and controls [297]. As shown in 4.1, the taxonomy identifies four main dimensions, each with multiple options. These dimensions include: timing (when the notice is provided), channel (how the notice is delivered), modality (what interaction mode is used), and control (how choices are provided). This study leverages features of Schaub et al.'s privacy notice design space [297] and adopts specific dimensions from it to create and explore a design space for privacy controls on wearables.

Similar to Schaub et al.[297], I argue that the timing of privacy control dimension (e.g., when a privacy control opportunity is presented) is an crucial design dimension to consider; I call this dimension "decision timing" or the "timing of control" dimension. In this user study, I extracted and evaluated the timing of control dimension by developing an interface that provides the option for privacy control as in-the-moment (just-in-time as defined by [297]) and a privacy control option prior to data collection (similar to at-set-up as defined by [297]). While Schaub et al. consider both channel and control as important design dimensions for privacy notices, I argue that it is important to consider what I call the "location of privacy control" or "location" dimension for privacy controls. Schaub et al. [297] describe a channel of privacy notices as the medium of how notice is delivered, but this dimension does not cover where control is allowed. When thinking about privacy control, we need to think about the location or the device (e.g., wearable vs. online privacy dashboard or mobile phone) the user goes to in order to make a privacy decision.

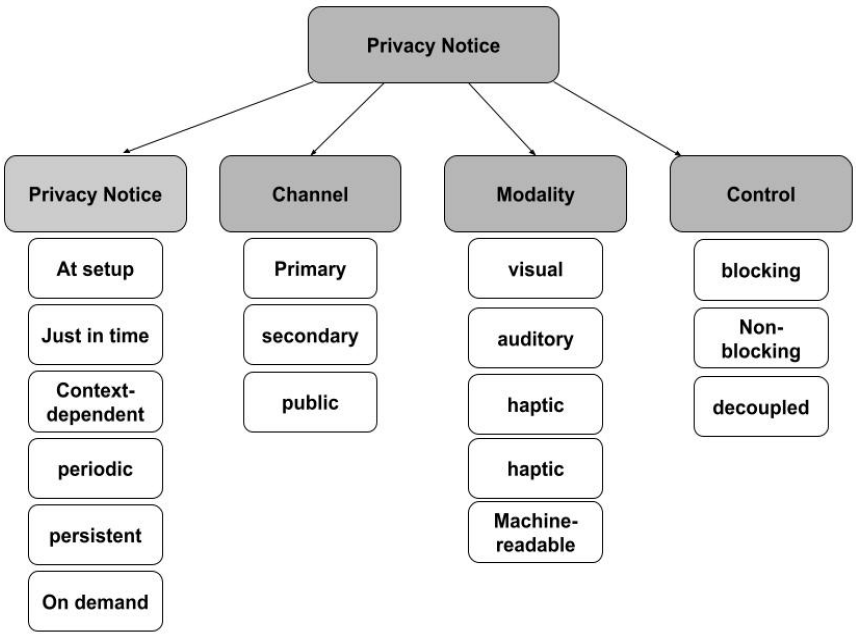


Figure 4.1. The privacy notice design space developed by [297]. This model is defined by four main dimensions:timing, channel,modality, and control.

Additionally, when considering the "control" dimension of privacy notices, Schaub et al. [297] suggests that decoupled notices do not integrate privacy controls into the user's interaction flow, which could be inconvenient to users. Drawing on aspects of both channel and control as

defined by Schaub et al., my proposed "location of control" dimension for privacy controls considers where privacy decisions can be made regarding data collected by wearables (e.g., on the wearable device, on a separated device, etc.) In this work, I explore both decoupled and integrated options for the location of control dimension. Whereas the majority of existing wearable technologies only allow decoupled options for privacy control, an integrated option would be a design where control over data sharing decisions are allowed directly on the wearable device where the data is being collected or processed. While the Apple Watch does have an integrated option for sharing activity data, the only type of data that can be shared is move data, exercise data, and step data. There is not an option to share additional types of data such as sleep data, food intake data, and physiological data (e.g., heart rate). The procedure for setting up sharing preferences is also not very usable. The user can only share data with people in their contacts and this is sorted by last name, meaning users have to scroll through all contacts in order to setup sharing options. Data sharing also has to be done prior to data collection and sharing preferences for sharing activity data is not granular. Users do not have the option to share specific data points with individual recipients.

Regarding Schaub's [297] dimensions of timing and control, the current privacy controls for wearables are limited. For example, many wearable health device manufactures only provide decoupled privacy control options (e.g., privacy control mechanisms, where there is limited control on the actual wearable device [265]). As a result, data-sharing decisions must occur on a separate device (e.g, online privacy dashboard or mobile device) at a time separate from data collection/production. Because this is the only option available on most wearables other than the apple watch, it is unknown whether a user would prefer to control their personal information in-the-moment of data collection/production and directly on their wearable at that moment. For privacy controls to be usable and effective, controls should be actionable and provide meaningful options for users of the given technology [68, 259, 297]. Schaub et al. [297] recommends privacy interfaces that offer integrated control mechanisms and in-the-moment consent management as an improved solution for users [284] as they are easier to use and flow easier into the user interaction without being overly disruptive. Schaub et al. [297] also recommends that once a privacy choice option is considered for development, that notice should be evaluated from an HCI perspective [284]. While these recommendations are helpful for privacy researchers, there are no studies that we know of that have conducted user-centered evaluations to explore these user groups in making privacy decisions on wearables. As a result, we suggest an alternative design space for privacy control on wearables

to accommodate the lack of privacy controls on wearables and interactions that could be used to express privacy decisions.

To recap, past research suggests location of control and decision timing are important dimensions to consider in order to improve privacy interfaces [68, 69, 79, 259, 296, 297]. Additionally, current privacy control designs for wearables are limited, and user evaluation of preferences regarding alternative design options for the location and timing of privacy controls is unknown. Therefore, this research explores the following research question:

Does location of control, timing of control or the combination of the two, impact the user experience for users of wearable technologies?

Through answering this question, this study will build upon Schaub's work [297] by exploring the significance of the location and timing dimensions in the context of the usability of privacy controls for wearables, and it will contribute to understandings of user-centered privacy control design. In the following sections I provide an overview of specific hypotheses I tested to answer this research question.

4.1.1 Hypothesis and Rationale

To explore this research question, I compare four possible privacy control interfaces for a wearable-sharing system: integrated+synchronous(in-the-moment); integrated+asynchronous (a priori); decoupled + synchronous (in-the-moment); and decoupled + asynchronous (a priori). The Integrated+ Synchronous (in-the-moment) condition is where control is exerted directly on a wearable in the moment of privacy disclosure. The Integrated + Asynchronous (a priori) condition is where control is exerted directly on a wearable, but not at the moment of data collection. Control is exerted before data collection. In the Decoupled + Synchronous (in-the-moment) condition, control is exerted on separate mobile device in the moment of data collection. The Decoupled + Asynchronous (a priori) condition is where control is exerted on separate mobile device before the data is collected. I evaluate the four conditions using the following set of metrics: ease of use, perceived privacy control, and perceived oversharing threat. This resulted in a 2 x 2 between-subjects experimental design, which tested the impact of location and timing on these three outcome variables. The rationale for each set of hypotheses and the related metrics is outlined below.

Each set of hypotheses below predicts the impact of location of control, the impact of decision timing, and the impact of their interaction. For each user experience metric (e.g., ease of

use, perceived privacy control, and perceived over-sharing threat), it is predicted that synchronous decision timing will provide a better user experience than asynchronous decision timing (H1a, H2a, H3a). Empirical studies find that the timing of control significantly impact the effectiveness of a privacy notice and may impact a user's ability to act on that privacy notice if the timing is not ideal [10, 35, 104, 129, 163, 259]. For example Balebako et al. investigated whether the time a user sees a privacy notice impacts their recall. Researchers used recall as a proxy of the salience of the notice [34]. Findings show that timing matters for smartphone privacy notices and is a significant predictor of recall. Research also suggests that users make differing decisions at different points in time. These decisions are contingent on contextual factors such as what they are engaged in at that moment and the information provided at that moment [8]. When privacy notices are provided when a data practice is active (e.g., just-in-time), users can make informed choices about their privacy, especially when information is sensitive or unexpected and requires consent [68, 297]. For each metric of user experience, it is also predicted that integrated control will provide a better user experience than decoupled control (H1b, H2b, H3b). Prior work suggests that users prefer to make privacy decisions on the same device where interaction the occurs [252, 299] and this integrated control is a suitable method to deliver privacy control to users [297]. For each metric of user experience, it is also predicted that there is an interaction between the location and timing of control in such that the synchronous, integrated privacy control option will provide the best user experience compared to the other conditions (H1c, H2c, H3c). We see from prior work that these two research streams influence user privacy, but there are no studies that I know of that have joined these research streams together toward the design of effective privacy controls for wearables.

4.1.1.1 Ease of use

The first metric used to test the impact of location, timing, and their interaction is ease of use. Perceived ease of use was chosen as a measure of user experience because we know from the technology acceptance model that a users attitude toward a system may be influenced by the perceived ease of use of the system [85]. Prior work also suggests that perceived ease of use of a system is a determinant on the intention to use the system [87]. Rogers also defines ease of use as the degree to which an individual perceives a new product or service as better than its substitutes [289]. More recent work provides evidence of the significant effect of perceived ease of use on usage intention of a given system [119, 137, 150, 220, 338, 339, 348]. As mentioned previously, studies have

found timing to impact the effectiveness of a privacy notice [10, 35, 104, 129, 163, 259]. If a system is effective, that means it is easy to use.

Thus, the first set of hypotheses tested is:

H1a: *The perceived ease of use will be higher for privacy interfaces with synchronous privacy control compared to privacy interfaces with asynchronous privacy control.*

H1b: *The perceived ease of use will be higher for privacy interfaces with integrated privacy control compared to privacy interfaces with decoupled privacy control.*

H1c: *The impact of location and timing will interact in such a way that the integrated+synchronous condition will have the highest perceived ease of use compared to the other conditions.*

4.1.1.2 Perceived Privacy Control

Perceived privacy control is the second metric used to test the impact of the different privacy control interfaces. Perceived control in the context of privacy is an individual's belief in a certain technology's capacity to allow them to control the release their personal information [369]. The collection, monitoring, and sharing of personal information can lead to a perception of loss of control over disseminating a person's information [210]. Perceived privacy control was chosen as a measure of user experience because past research has noted that perceived control can impact how individuals interact with technological systems [229]. Thus, the second set of hypotheses tested is:

H2a: *The perceived privacy control will be higher for privacy interfaces with synchronous privacy control compared to privacy interfaces with asynchronous privacy control.*

H2b: *The perceived privacy control will be higher for privacy interfaces with integrated privacy control compared to privacy interfaces with decoupled privacy control.*

H2c: *The impact of location and timing will interact in such a way that the integrated+synchronous condition will have the highest perceived privacy control compared to the other conditions*

4.1.1.3 Perceived Over-sharing Threat

The third metric used to test the impact of location, timing, and their interaction is perceived over-sharing threat. Knijnenburg and Kosba define this metric as, "a lack of comfort or confidence regarding the attained level of sharing, which results in a system-specific concern of unwanted data collection or loss of control" [173]. Knijnenburg and Kosba also suggest that granular control options provide a higher level of control, which may possibly decrease perceived over-sharing threat [173].

Thus, I chose this construct to measure user experience. If a wearable privacy interface is easy to use because it offers a more effective means to manage personal information, users will be less worried about breaches to their personal information. Thus, the third set of hypotheses tested is:

H3a: *The perceived over-sharing threat will be higher for privacy interfaces with asynchronous privacy control compared to interfaces with synchronous privacy control.*

H3b: *The perceived over-sharing threat will be higher for privacy interfaces with decoupled privacy control compared to privacy interfaces with integrated privacy control.*

H3c: *There will be a significant interaction effect for timing and location on perceived over-sharing threat.*

4.2 Method

To test the hypotheses, a 2 x 2 between-subjects experiment was designed; the two independent variables are location of privacy control (*integrated, decoupled*) and decision timing (*synchronous, asynchronous*). Participants were randomly assigned to one of four conditions to interact with a wearable privacy interface (See Table 4.1). Participants completed a screener questionnaire to determine eligibility to participate in the study, interacted with a mock-up of a wearable privacy interface, and evaluated the interface in terms of ease of use, perceived privacy control, and perceived privacy threat.

Participants also completed a post questionnaire where I collected quantitative data on their intent to use the interface if it were made available to them I also collected data on participants' privacy consciousness (adopted from Pew [206]) and demographics (including gender, race, and level of education).

The study was approved by the Clemson Institutional Review Board.

4.2.1 Pilot

Prior to running the full experiment on the Prolific crowdsourcing platform, I conducted a pilot study with a group of HCI experts to test any bugs within the prototype. After addressing concerns, we piloted the study on 14 participants from Prolific. Participants in the pilot took an average of 6 minutes and 31 seconds to complete the experiment. Based on the timing to complete the experiment and Prolific's recommended compensation tool, participants were paid $1.60 for

completing the study. The amount of remuneration is equivalent to $14.37 per hour which is well above the federal minimum wage for the U.S, but comparable to some states' minimum wages (e.g., CA's minimum wage is $14/hr).

4.2.2 Power Analysis

After piloting, we conducted a power analysis to determine the desired sample size. Since we wanted to detect between a small and medium effect, we ran an a priori power analysis to determine the needed sample size range (with the alpha set at .05). In order to detect a small effect ($f^2 = .02$) at 80% power for a regression with three predictors (e.g., location, timing, and the interaction term), a sample size of 550 participants was needed. In order to detect a medium effect ($f^2 = .15$) at 80% power for regression with three predictors, a sample size of 77 participants was needed. Based on these numbers and our budget to run the final study, we decided to recruit a total of 305 participants.

4.2.3 Participant Recruitment and Quality Controls

The initial goal was to collect data from 305 participants. After running several iterations of the study, I decided to collect data from an additional 18 participants to distribute participants across conditions equally. We recruited a total of 337 participants (14 pilot and 323 in the complete experiment) through the Prolific sourcing platform. Within the Prolific platform, we used custom prescreening to recruit participants based on the following filters [262]:

- Age
  - Minimum Age: 18, Maximum Age: 100
- Current Country of Residence
  - United States
- First Language (English)
  - English
- Internet enabled products
  - Activity tracker excluding smart watches (e.g. Fitbit, Xiaomi Mi Band, Microsoft band)
  - Smart watch (e.g. Apple watch, Samsung gear, Moto 360, Asus ZenWatch)
- Approval Rating
  - Minimum Approval Rate: 90, Maximum Approval Rate: 100 (inclusive)

We also screened participants within the survey by asking if they owned any of the wearable devices from a list. If they selected they did not own a wearable device, they were redirected to

the end of the survey and thanked for their interest in the study. Because the experiment asked participants to envision using different wearable interfaces based on an online prototype, it was important to recruit people who had actual experience with wearables who would be more able to envision what it would be like to interact with the wearable device in a real-life setting. To ensure high data quality, we included a quality check and an attention check within the experiment [5, 263]. For the quality check, we asked participants whether they would commit to providing thoughtful and honest answers to the questions in the survey. If participants indicated they would provide their best answer, they were included in the sample. For another attention/quality check, we added a question to ensure participants had completed the full interaction with the assigned prototype and that they were paying attention to the instructions. After interacting with the mock-up of the wearable privacy interface, participants were notified they had reached the last screen of the interaction and were advised to select the letter "A" for the next question in the survey. The next question asked them to select the letter seen on the last screen of the prototype interaction; the answer options provided were A, B, C, and "I was not able to make it to the last screen." Only participants who answered "A" were included in the final sample.

Participants for the full experiment (N=323) were randomly assigned into four groups using Qualtrics randomly assigned survey logic branch feature. We paid participants $1.60 for their participation. On average, it took participants 8 minutes and 41 seconds to complete the experiment.

4.2.4 Materials

Questionnaires Prior to the experiment, participants answered questions about their age, knowledge of technology, and wearable device ownership. After interacting with the privacy settings interface, we asked questions about their evaluation of the overall ease of use, perceived privacy control, and perceived privacy threat of the assigned interface. Additionally, we asked participants questions about the likelihood of using the settings interface if it were available to them, what they liked about the method for sharing health data based on the condition they saw, and what would they change about the method for sharing data. Lastly, questions were included to assess participants' views on privacy [206]. We also collected information on participants' gender, race, and education. Both the questionnaires and the full experiment were implemented via Qualtrics. All questions are reproduced in the Appendix B.

Apparatus Participants received the experimental stimuli randomly via one of four mockups of a privacy interface. Mock-ups were designed using the Adobe XD prototyping tool. Prior to interacting with the mock-up, participants were presented with a scenario based on the experimental condition they received. Each scenario described a randomized instance where participants were advised to share step data with a health care provider. Following the scenario, participants continued to interact with their randomly assigned condition via the interface prototype where they could share or withhold their step data. (see Figure 4.2-4.5)

Experimental Condition	Description
Integrated + Synchronous (IS)	operationalized by means of an interface where control is exerted directly on the primary interface at the same time of disclosure.
Integrated + Asynchronous (IA)	operationalized by means of an interface where control is exerted directly on the interface, but the privacy decision is setprior to data collection. Upon collection of data, notice of disclosure is provided based on decision made at set up
Decoupled + Synchronous (DS)	operationalized by means of an interface where control is exerted on a secondary interface. The disclosure decision is exerted at the moment of data collection on the secondary interface
Decoupled +Asynchronous (DA)	operationalized by means of an interface where control is exerted on a secondary interface, but not at the moment data collection. The disclosure decision is exerted at set up, and notice of disclosure decision is shown on primary interface after data is collected

Table 4.1. Description of Each Experimental Condition

4.2.5 Experimental Design

We used a 2 x 2 between-subjects experimental design. The independent variables of location of control (levels: integrated v. decoupled) and timing of control (levels: asynchronous v. synchronous) were operationalized through four interface designs, one for each experimental condition; see Table 4.1. The three dependent variables are overall ease of use, perceived privacy control, and perceived oversharing threat. More details about the scales used to operationalize these constructs can be found in the 4.2.7 section below.

Independent Variables and Levels	Description
Location of Privacy Control	
Integrated	Control is directly on wearable device
Decoupled	Control Separate from wearable (via mobile device)
Timing of Control	
Synchronous	in-the-moment the data is produced
Asynchronous	outside-the-moment the data is produced (prior to data collection)
Dependent Variables	**Description**
System Satisfaction	refers to how satisfied participants are with the user interface [171]
Ease of Use	refers to how simple the interface is understand or use [86, 338]
Perceived Privacy Control	the idea of the privacy interface providing the user control over the personal information generated by the wearable [59, 146, 172]
Perceived Over-sharing Threat	refers to the threat associated with more data being shared than expected via the wearable [171]

Table 4.2. Description of Independent and Dependent Variables

Participants were randomly assigned to one of the four experimental groups (see Table 4.1)

In the IS group, participants interacted with a prototype that mimics a wearable smartwatch (e.g., Apple watch) where they are notified of a completed step goal on the watch interface and asked in that moment if they would share that information with their health care provider (see Figure 4.2).

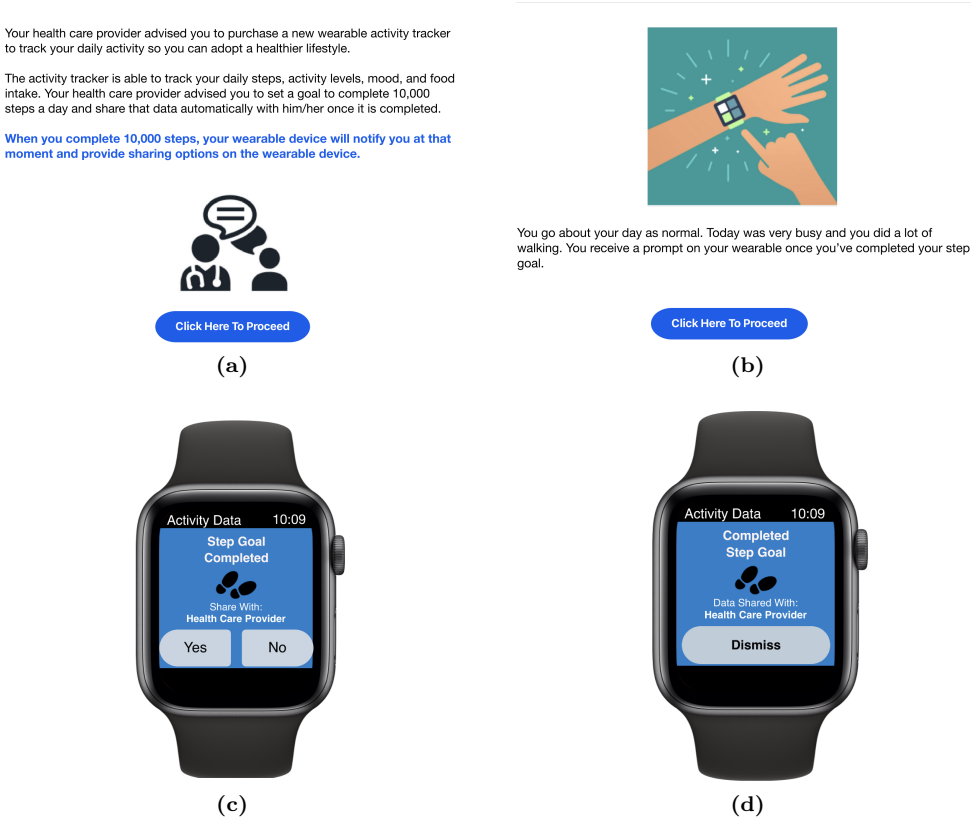


Figure 4.2. Stimuli presented to participants via mock-up for the Integrated Synchronous Condition

Participants interacted with a similar prototype in the IA group, except they were instructed to set up their step goal sharing preferences before the time of data collection (see Figure 4.3).

In the DS group, participants were notified of the completion of a step goal, but they were instructed that they needed to make their privacy decision on a separate mobile device. Instead of making their decision on the watch interface, they were asked to imagine taking their phone out of their pocket. There was a 5-second delay to simulate the process of removing a phone from the pocket. Once this simulation was completed, participants were asked to make their privacy decision using the mobile device interface instead of the wearable (see Figure 4.4).

In the DA condition, participants were prompted on the mock-up of the mobile device interface to open the mobile app to set up their privacy preferences for that day. Using the mobile

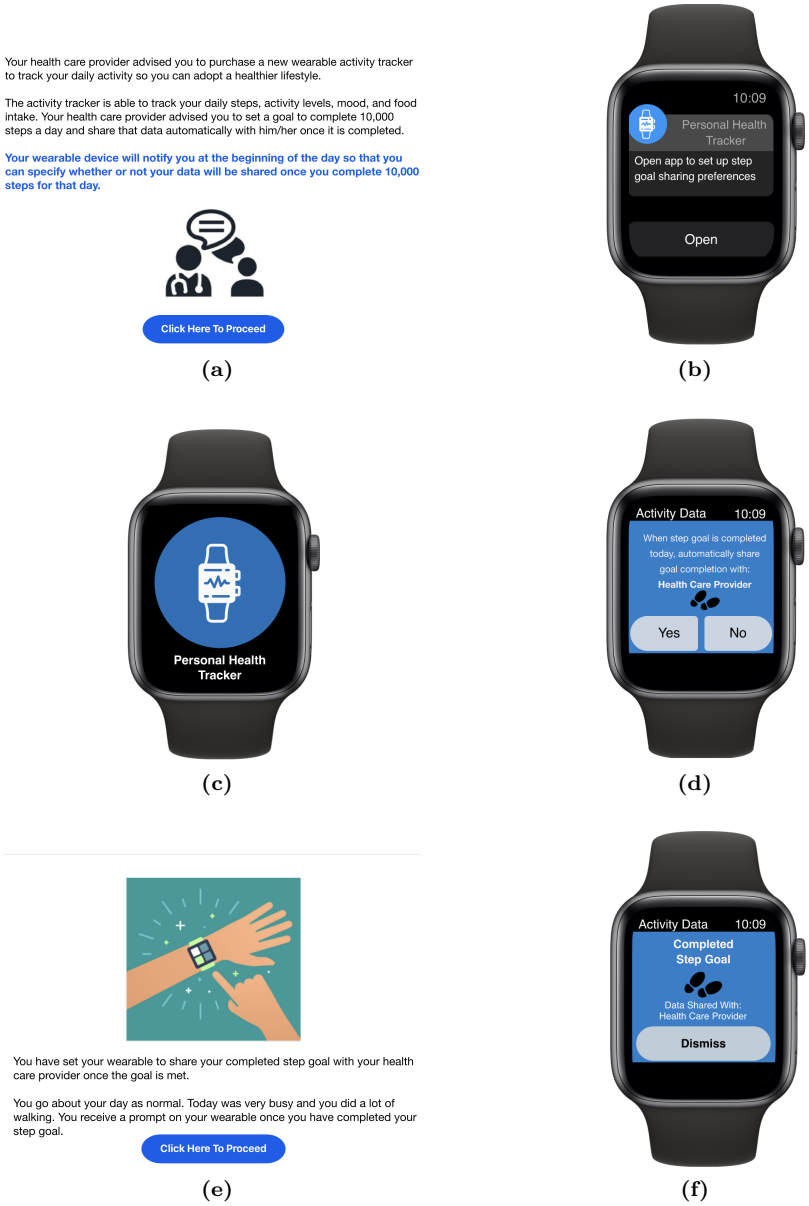


Figure 4.3. Stimuli presented to participants via mock-up for the Integrated Asynchronous Condition.

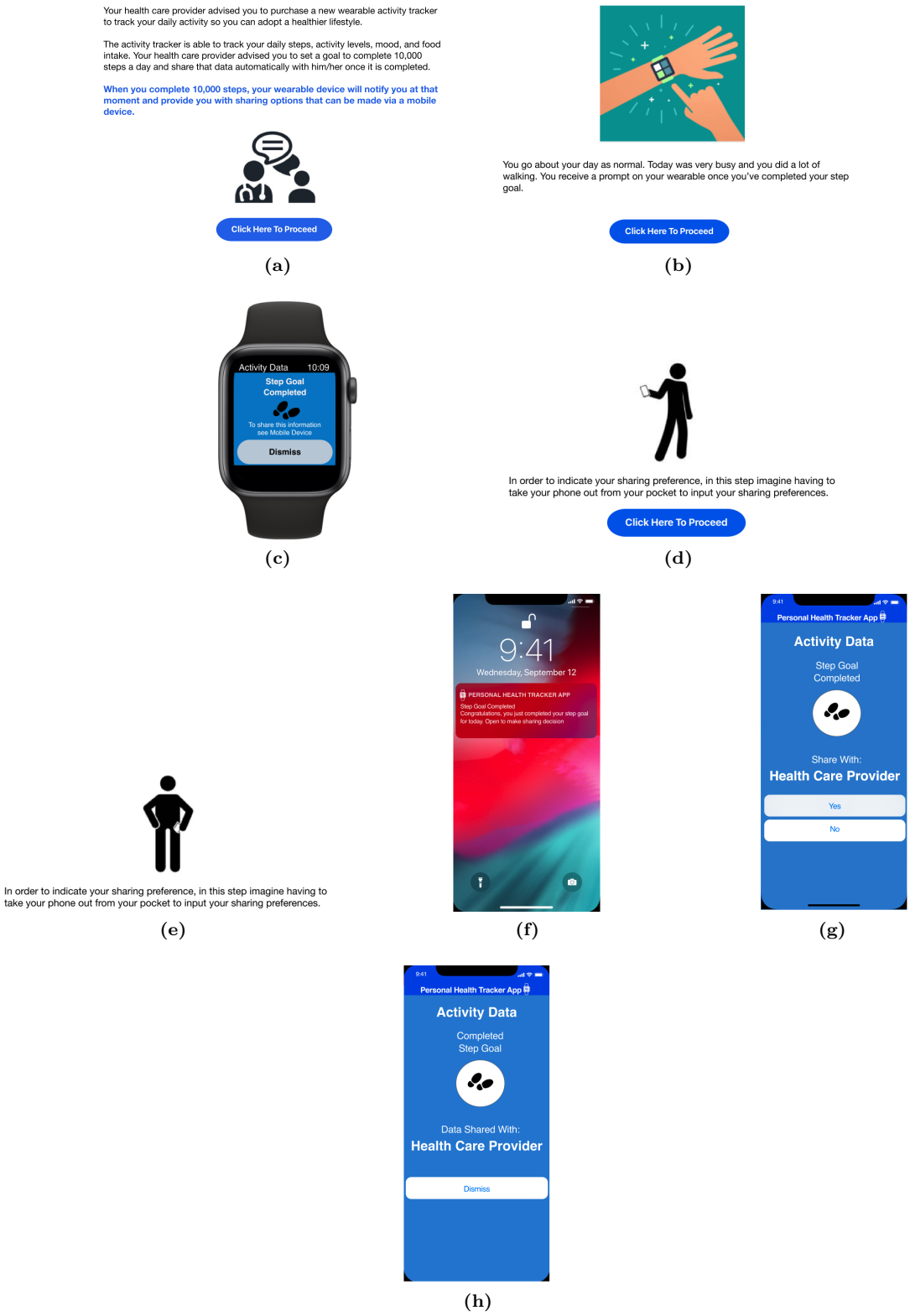


Figure 4.4. Stimuli presented to participants via mock-up for the Decoupled Synchronous Condition.

device interface, they made their privacy decision prior to data collection (see Figure 4.5).

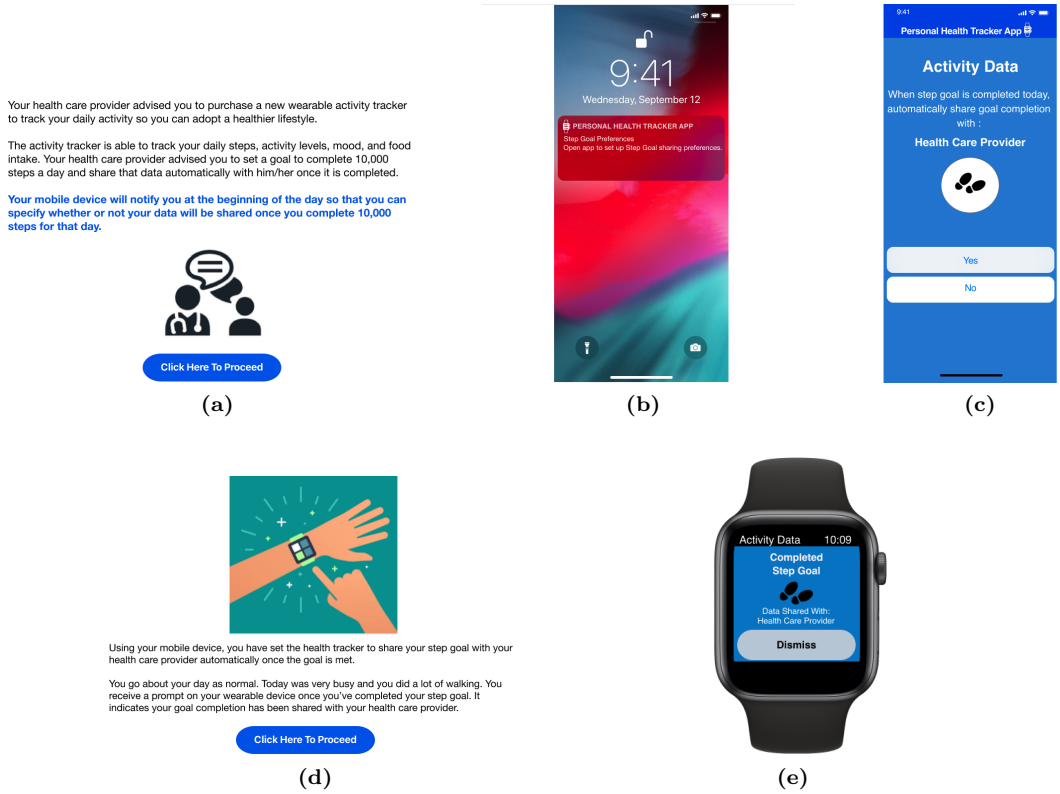


Figure 4.5. Stimuli presented to participants via mock-up for the Decoupled Asynchronous Condition.

4.2.6 Scenario Design

In all four conditions, participants are presented with the same scenario (See image a in Figures 4.2-4.5): their health care provider has asked them to use a wearable and share their step activity. We held the type of data and recipient of data constant for each scenario, using a positive-neutral framing. Based on prior work, step data is considered a neutral data point that does not present much of a privacy risk [131, 170, 234, 281]. Also, as identified in the previous chapter, people are generally more willing to share data with their healthcare provider. The scenario was designed to be neutral and non-threatening, so users would focus more on their perceptions of the settings interface versus a potentially risky data-sharing scenario. We adopted a wizard of oz approach to simulate how the interface for each condition would perform in a real-world scenario. As noted in prior works, simulating the functionality of a mock-up or a prototype allows researchers to

explore and evaluate designs to test certain elements a design and improve them before investing the considerable time, effort, and money in implementing the system [98]. We also had to take certain precautions due to the current COVID-19 pandemic and could not run the experiment in person with participants. We decided to conduct an unmoderated online controlled experiment to reach a larger and more diverse group of less WEIRD (White, Educated, Industrialized, Rich, Democratic) participants [148, 154, 175, 286] in comparison to laboratory experiments. Using this approach, participants can take part in experiments anywhere without having to take time to travel to a lab to participate in a research experiment [154]. In addition to increasing participant reach, running studies online cuts down on time, effort, and resources needed to recruit participants [17, 154]. We simulated a privacy sharing interface for all four conditions. While we did not collect the participants' preferences for sharing (e.g., whether they chose to share or not share their step data), the participants were presented with additional confirmations based on their preferences for sharing to simulate a working interface that provides appropriate feedback.

Construct	Item	Loadings
Perceived Ease of Use [86, 338] Ave= 0.754 Sq. (AVE) = 0.863	1.Using this privacy interface would be easy for me.	0.774
	2. I find it easy to get this settings interface to do what I want it to do.	0.796
	3. I find the privacy interface easy to use	0.806
	4.My interaction with the settings interface was clear and understandable.	0.821
	5.I find the settings interface easy to use.	0.573
Perceived Privacy Control [59, 146, 172] Ave= 0.5038 Sq. (AVE) = 0.709	1. The settings interface restricted me from my preferred choice of how to share my data.	0.523
	2. I had limited control over my personal information using the settings interface.	0.700
	3. Using the settings interface, I believed I had control over my personal information collected by the wearable.	0.461
	4. Compared to how I normally configure my sharing preferences for a wearable, the settings interface was very limited.	0.433
	5. I would like to have more control over the settings interface.	0.402
Perceived Over-sharing Threat [171] Ave= 0.742 Sq. (AVE) = 0.861	1.Using the settings interface, I believe too much of my data will be shared.	0.825
	2. I am comfortable with the amount of data that could be shared using the settings interface.	0.735
	3. Using the settings interface, I believe I am not disclosing too much of my personal information to anyone.	0.638
	4.I am afraid that using the settings interface, I will share my data too freely.	0.788
	5. Using the settings interface, I feel my settings would be spot on; I would not be disclosing too much to anyone.	0.724

Table 4.3. Constructs used to measure overall user experience

4.2.7 Measurements

After interacting with the selected interface, participants completed a post-survey.

4.2.7.1 Measure For Dependent Variables

The post-survey asked participants to rate the following based on their interaction with the privacy interface: overall ease of use, perceived privacy control, and perceived over-sharing threat.

These constructs were measured using [59, 86, 146, 171, 172, 338] scales. These are 7-point Likert scales, measured from 1 ('Strongly disagree') to 7 ('Strongly agree'). The items for these scales can be found in Table 4.3.

4.2.7.2 Measures for Demographic and Contextual Variables

Participants' reported intentions to use the assigned interface in the future was measured with the following question:

- *On a scale of 1-10, how likely would you be to use the settings interface you interacted with if it were available to you?*

Participants views on privacy were measured using a 5-point Likert scale [206] using the following questions:

- Privacy means different things to different people today. In thinking about all of your daily interactions-both online and offline-please tell us how important each of the following are to you:
  - Being in control of who can get information about you
  - Being able to share confidential matters with someone you trust
  - Not having someone watch or listen to you without your permission
  - Controlling what information is collected about you
  - Being able to have times when you are completely alone, away from anyone else
  - Having individuals in social/work situations not ask you things that are highly personal
  - Being able to go around in public without always being identified
  - . Not being monitored at work
  - Not being disturbed at home

Participants' demographic information (e.g., age, race, and education) was also collected using questions from Pew [55].

4.2.8 Procedure and Analysis

Within the Prolific platform, participants were presented with a description of what they would do in the study (See Appendix B Figure 13). The description indicated that their role would

be to take part in a survey and interact with a mock-up of a wearable device and provide answers regarding their experience with the interface. They were told it would take approximately 10 minutes to complete the study. Once they clicked the study link, they were directed to Qualtrics where the experiment was hosted. They were asked to input their profile ID at the beginning of the study and provided with an informed consent briefing of the study.

After providing informed consent, participants were provided with three screener questions that asked their age, knowledge of technology and wearable device ownership. If participants indicated they were under 18, or did not own a wearable device, or did not commit to providing their best answers, they were not allowed to participate in the study. The instructions informed participants they would be presented with a scenario and an interactive mock-up of a wearable device. We informed participants that they would be presented with a method (one of the 4 randomized conditions) for sharing health information collected from a wrist-worn health-tracking device (similar to a FitBit or Apple Watch). We also informed participants they would move through each part of the scenario by either clicking a "Next" button or interacting with a device mock-up (e.g., clicking on a notification or button on the device). We also asked participants to imagine they own a wearable device and use it daily. We advised them to pay attention to how the sharing options were presented to them, as they would be asked questions about their experience of that method. Next, participants completed the post-survey questions and were redirected back to Prolific. We reviewed each survey for quality and paid participants for participation.

To test the research hypotheses, a set of linear regressions with interaction terms were used. The exploratory data was analyzed using linear regression, also. Descriptive statistics and regression plots were generated for each regression model to ensure the data met the assumptions of regression; adjustments were made to address any violated assumptions.

4.3 Quality Checks for construct measures

To examine the quality of the individual measures used to measure overall experience with the provided interface, Confirmatory Factor Analysis (CFAs) was performed on all scales. Cronbach's α were also obtained to confirm the scales met conventional standards of reliability. The results from these quality checks are described below.

4.4 Reliability and validity check for each construct to measure user experience

Prior to the experiment, reliability and construct validity measures were obtained for each DV to see how well the items for the overall experience held together as a whole. The perceived ease of use (Cronbach's $\alpha = 0.86$), perceived privacy control(Cronbach's $\alpha = 0.78$), and perceived oversharing threat(Cronbach's $\alpha = 0.90$) constructs had had high reliability. CFA was also performed to estimate the validity of the scales. A saturated model comprised of all the items in the scales was created for each scale. The model had a decent fit as indicated by the fit indices. The CFI and TLI values were 0.965 and 0.960 respectively. The RMSEA was 0.071 [CI(0.064,0.078),p<0.001]. R-square values and Average Variance Extracted (and its square roots) for all of these constructs are mentioned in Table 4.3.

	N = 296
Gender	
Male	168 (55%)
Female	133(43%)
Other	18(1.3%)
Age	
18-24	61 (21%)
25-34	133(45%)
35-44	71 (24%)
45-64	71 (24%)
65+	3 (1%)
Education	
High incomplete or less	2 (1%)
High school grad	20 (7%)
Some College	71 (24%)
Four Year College	110 (37%)
Some postgraduate	22 (7%)
Postgrad or Professional	70 (24%)
Race/Ethnicity	
White	218 (74%)
African American	27 (9%)
Asian	37 (13%)
Other	12 (4%)
Technology Knowledge	
Basic	10 (3%)
Intermediate	121 (41%)
Advanced	133 (45%)
Professional	32 (11%)

Table 4.4. Participant Demographics

4.5 Results

Data for 23 participants were not included in the final analysis because they either failed the attention check question (n = 18) or reported they were unable to make it to the last screen of the interface prototype (n = 5). Participants who were not included in the final analysis because they failed attention check questions indicated that the letter on the last screen of the interaction scenario was something other than the letter “A", as specified in the interface prototype. The five participants who indicated they could not make it to the last screen stated they were unsure why they did not make it to the last screen. We double-checked the prototype to ensure all bugs were removed. We did not find any bugs in our investigation, so we believe it was a technical issue related to their internet connection that did not allow them to get through the full prototype. Additionally, four outliers were removed in the data cleaning process because they were four or more standard deviations outside of the mean. These outliers also influenced the normal distribution of overall ease of use. As a result, the final sample size was 296 participants (IS:73, IA:75 DA:71, DS:77). A post-hoc sensitivity analysis reveals the final sample is adequately powered ($\beta = .80$) to detect between a small and medium effect ($f^2 = .037$) for a regression with three predictors. This number is approaching the lower bound of a small effect as defined by Cohen ($f^2 = .02$) [66]. The participant demographics can be found in Table 4.4. The descriptive data for the dependent variables is listed in Table 4.6.

Dependent Variables	Integrated+Synchronous (N=75)		Integrated+Asynchronous (N=73)		Decoupled+Synchronous (N=77)		Decoupled+Asynchronous (N=71)	
	Mean	SD	Mean	SD	Mean	SD	Mean	SD
Perceived Ease of Use	6.46	0.52	6.40	0.61	6.27	0.63	6.26	0.64
Perceived Privacy Control	4.70	1.03	4.52	1.10	4.30	1.17	4.51	1.09
Perceived Oversharing Threat	2.91	1.16	3.12	1.19	3.14	1.26	2.98	1.16

Table 4.5. Mean and Standard Deviation for all constructs used to measure overall user experience per condition

4.5.1 Hypothesis Testing

Linear regression was used to test if the location of control and timing of control predicted participants’ ratings of ease of use, perceived over-sharing threat and perceived privacy control. In each model, we tested the main effects of location of control and timing of control and the interactions between them. We conducted the regression analyses in R [324] using the “lm” function from the “lme4” package with default parameters.

	Dependent variable:		
	EaseofU	PCtrl	Pthreat
	(1)	(2)	(3)
Location	-0.165^{**}	-0.194	0.039
	(0.070)	(0.128)	(0.139)
Timing	-0.027	-0.186	0.176
	(0.070)	(0.128)	(0.139)
Location:Timing	0.091	0.001	-0.048
	(0.140)	(0.256)	(0.279)
Constant	6.354^{***}	4.514^{***}	3.037^{***}
	(0.035)	(0.064)	(0.070)
Observations	296	296	296
R^2	0.020	0.015	0.006
Adj R^2	0.010	0.005	-0.004
RSE (df = 292)	0.603	1.099	1.198
F Statistic (df = 3; 292)	2.029**	1.508**	0.577**
Note:			*p<0.1; **p<0.05; ***p<0.01

Table 4.6. Regression results from hypothesis testing.

Table 4.6 presents the regression results and shows the effects of the IVs on each dependent variable. For ease of use (model 1), the regression results indicate that timing and the interaction effect between the location of control and timing of control are not significant predictors. We do find a main effect for location, which significantly predicted ease of use *(B = 0.165, $p < 0.05$)*. Although model 1 was significant, the R^2 value was low only explaining 2% of the variance in ease of use *($R^2 = 0.020$; $F\ (3, 292) = 2.029$, $p < 0.05$)*, which is a small effect according to Cohen [66]. For models 2 and 3, none of the independent variables had a significant impact on perceived privacy control or perceived over-sharing threat. The findings from models 1 through 3 do not support the research hypotheses H1a,c; H2a,b,c; or H3a,b,c. The results from model 1 do provide support for H1b, though.

H1b was supported in that location had a significant effect on the overall ease of use *($p < .05$)*. Additionally, as hypothesized, a post-hoc independent t-test revealed that individuals who received the integrated conditions reported higher ease of use for the settings interfaces than those who received the decoupled conditions. The t-test results show that the 148 participants who received the integrated condition demonstrated significantly higher mean scores for overall ease of use *($M = 6.44$, $SD = 0.55$)* compared to the 148 participants who received the decoupled condition *($M = 6.27$, $SD = 0.63$; $t(290) = 2.36$, $p = 0.01$)*.

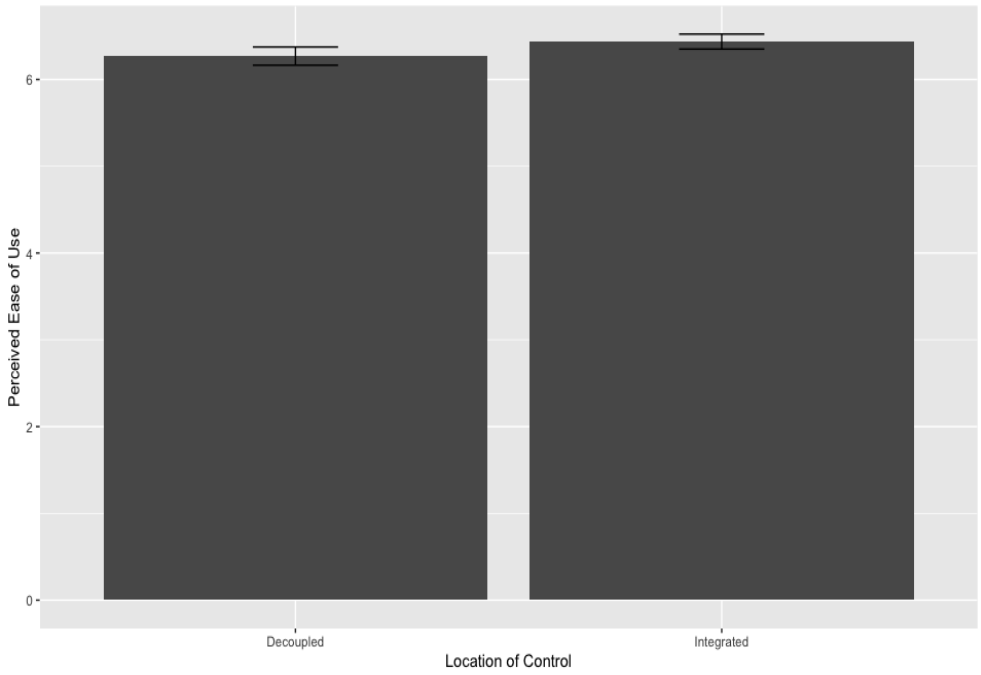


Figure 4.6. Overall Ease of Use for Decoupled Versus Integrated Interfaces

4.5.2 Post-Hoc Exploratory Analysis

A series of prior studies illustrate that privacy concerns affect behavioral intentions like intent to adopt and use technology [167, 273, 308, 370] As noted in section 4.2.7.2, we asked participants to report their intentions to use the assigned interface in the future if it were available. While there was not much difference in the scores for intentions to use the provided interface, we do see from our descriptive statistics that participants in the decoupled + asynchronous condition gave the highest intention-to-adopt ratings (M = 7.76, SD = 1.98; see table 4.8 for full results). To further explore insights related to the overarching research question, we performed post-hoc hierarchical regressions to investigate the predictors of participants' intent to use the assigned settings interface if it were available to them. Hierarchical regressions were run to examine how much unique explained variance each predictor adds to the model. Since *location* of control had a significant effect on overall ease of use, it was entered in the first step of the regression. Next, each predictor was entered separately to examine its unique impact starting with *timing*, then *ease of use*,then *perceived privacy control*, then *perceived oversharing threat.*

The full results from the hierarchical regressions can be found in Table 4.7. The results from

	Dependent variable:				
	Likelihood of Adoption				
	(1)	(2)	(3)	(4)	(5)
Location	−0.068	−0.050	0.152	0.222	0.114
	(0.249)	(0.247)	(0.234)	(0.223)	(0.207)
Timing		−0.656***	−0.623***	−0.523**	−0.478**
		(0.247)	(0.232)	(0.222)	(0.205)
Ease of Use			1.233***	0.979***	0.662***
			(0.193)	(0.190)	(0.181)
Perceived Ctrl				0.575***	0.134
				(0.104)	(0.114)
Perceived Threat					−0.771***
					(0.108)
Constant	7.331***	7.336***	−0.496	−1.482	4.868***
	(0.125)	(0.123)	(1.233)	(1.189)	(1.414)
Obs	296	296	296	296	296
R^2	0.0002	0.024	0.143	0.224	0.340
Adj R^2	-0.003	0.017	0.134	0.214	0.329
R^2 Δ		0.0235**	0.1223***	0.0947***	0.1490***
RSE	2.145	2.124	1.993	1.899	1.755
F Stat	F(1,294) = 0.0730	F(2,293) = 3.569***	F(3,292) = 16.272***	F(4,291) = 21.054***	F(5, 290) = 29.886***
Note:					*p<0.1; **p<0.05; ***p<0.01

Table 4.7. Hierarchical Regression Analysis Results for Predictors of Likelihood to Adopt

model 2 show that timing of control significantly predicts intent to use the settings interfaces; the asynchronous interface predicts higher likelihood of adoption *(B = -0.66, p < .01)*; see Figure 4.7. Adding timing of control to the model explained an additional 2 percent of the variance in likelihood to adopt *(R^2 Δ = .02, p < .05)*. Results from model 3 show that the perceived ease of use positively predicts likelihood of adoption *(B = 1.23, p < .01)*, explaining an additional 12% of the variance in likelihood to adopt *(R^2 Δ = .12, p < .05)*. Results from model 4 show that perceived control positively predicts adoption likelihood *(B = .58, p < .01)* and explains an additional 9% of the variance *(R^2 Δ = .09, p < .05)*. (Note that perceived control becomes a non-significant predictor once perceived threat is added in model 5). Results from model 5 show that perceived over-sharing threat negatively predicts adoption likelihood *(B = -0.77, p < .01)* and explains an additional 15% of the variance *(R^2 Δ = .15, p < .05)*. Additionally, the overall model with all 5 predictors explains 34% of the variance in intent to use, which is a large effect *(R^2 = 0.34; F (5, 290) = 29.886, p < .001)* according to Cohen [66].

Interface Condition	Mean	SD
Integrated+Synchronous (N=75)	7.59	1.80
Integrated+Asynchronous (N=73)	7.15	1.98
Decoupled+Synchronous (N=77)	6.82	2.59
Decoupled+Asynchronous (N=71)	7.76	1.98

Table 4.8. Mean and Standard Deviation for Likelihood of adoption for each interface condition

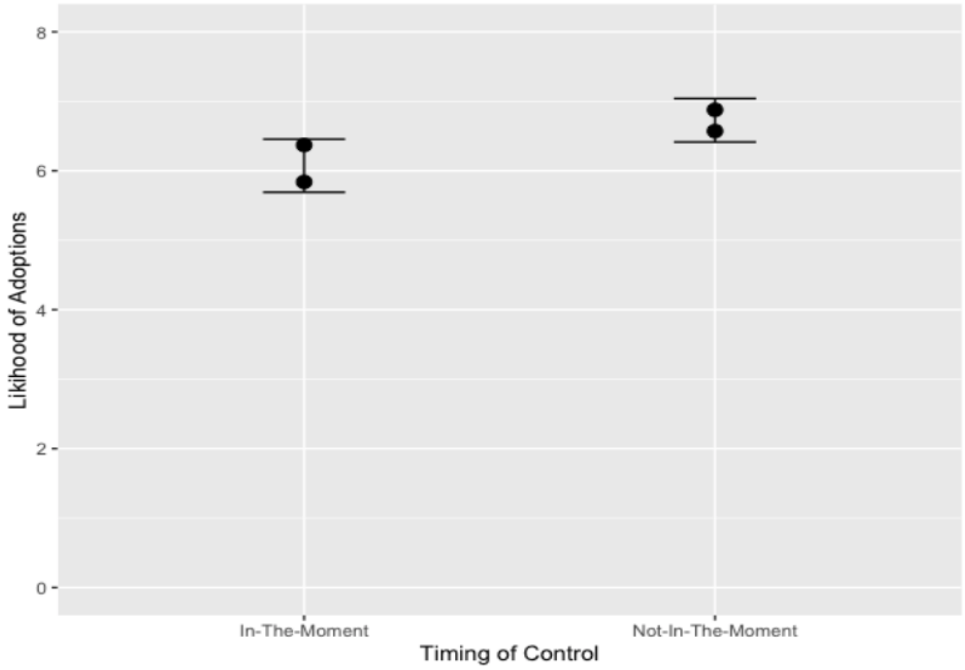


Figure 4.7. Overall Ease of Use for Decoupled Versus Integrated Interfaces

4.6 Discussion

We know from the previous chapter that adopters and potential adopters of wearable health technologies desire more granular control over data from their wearable device. When designing privacy-enhanced solutions for wearable technologies, it is essential to understand what interface mechanisms would provide users with adequate control over their personal information. As noted by the FTC, providing proper privacy interface mechanisms in the context of IoT can be challenging, especially for wearables due to the lack of displays and user interfaces [69]. Researchers need to explore alternative privacy interfaces that minimize privacy risks to users. I believe the first step in doing so is to examine how location and timing impact overall ease of use, perceived privacy control, and perceived over-sharing threat.

In the context of privacy control for IoT devices, previous studies have noted that for privacy controls to be usable and effective, controls should be actionable and provide meaningful control options to users [68, 259, 297]. However, there are no studies that we know of that have evaluated timing and location of control in combination to provide users with ways to manage their privacy actively. While Schaub et al. has mapped the design space for effective privacy notices [297]

by providing a taxonomy of design features for privacy notices and control within the IoT domain (See Figure 4.1), this study is the first to evaluate user interfaces based on location and timing for privacy control for wearables in terms of their ease of use, perceived control, and perceived over-sharing threat. In the following sections, we discuss the implications of our results and discuss the broader implications of our results to design privacy-enhanced solutions for wearables.

4.6.1 Location of Control Predicts Overall Ease of use

While we did not find a significant main effect for timing or a significant interaction effect for location and timing, we found that location of control somewhat influences overall ease of use, with the integrated privacy control interfaces predicting higher ease of use scores (supporting H1b). While we do see a statistically significant impact on the ease of use for location of control, the R^2 value for the model was low, only explaining 2% of the variance. The low R^2 value could be because this was a simulated experiment and overall ease of use was high for all conditions regardless of the interface (as shown in Table 4.5). In general, the findings do support Schaub's suggestion that an improved solution for designing privacy-enhanced interfaces for wearables could be to design privacy interfaces that offer integrated control mechanisms [297]. The mean ease of use scores for the integrated conditions were between 6 and 7, indicating that most participants either "agreed" or "strongly agreed" that the interfaces were easy to use (see Table 4.5).

Users are increasingly making decisions about accepting and adopting information technologies [338], and it is important to understand the factors which influence these decisions. Although the mean ease of use scores were high for each condition in this study, we believe if there were a situation where people interacted with these interfaces in the wild over a more extended period of time, there would be larger differences between the ease of use scores for each condition. In particular, when privacy controls are decoupled from the user's interaction flow, this may present a degree of difficulty that could be inconvenient to users and may also make them less willing to use these controls. Currently, the only options present for privacy control on wearables are decoupled except for the Apple watch. The results from this study suggest that integrating privacy control directly on the wearable could result in an easy-to-use interface, according to users' evaluations. Future research should investigate whether users have differing preferences for integrated versus decoupled privacy controls when regularly interacting with these interfaces for an extended amount of time. In the next section, I will discuss the implications for the non-supported hypotheses.

4.6.2 Implications of Non-Supported Hypotheses

Although H1b was supported, the data from this study did not support the remaining research hypotheses. With the exception of H1b, location, timing, and the interaction between the two did not significantly impact the reported ease of use, perceived privacy control, or perceived over-sharing threat. This does not necessarily mean that these variables are not important to consider when attempting to improve privacy outcomes for users; the results suggest that these variables did not impact the users' overall user experience regarding the interfaces in this simulated experiment. One implication of this is that none of these interface options present unique barriers to user experience itself (except that decoupled control options may provide lesser ease of use than integrated options).

In addition to results from the previous chapter, prior literature suggests that users do have granular preferences for sharing data from a wearable [118, 274]. We also know that when users have more granular options for privacy sharing, there is more potential to mitigate privacy violations [50, 107, 118]. Therefore, the non-significant results provide some positive implications for designing interfaces that protect user privacy that should be further explored by interface designers and privacy researchers. If the user experience is positive and relatively stable across different interface options for location and timing of privacy control (as observed in this study), this means designers can focus on creating interfaces that promote the most positive privacy outcomes without worrying about compromising user experience. Thus, we recommend designers and researchers attend to the model proposed in Figure 4.8. Building upon work from Schaub et al. [300], this model outlines a design space for privacy controls for wearable technologies; this model points to the available opportunities for privacy controls on wearable technologies that need to be understood and explored by both researchers and designers.

4.6.3 Perceptions Impact Intention To Use

In a post-hoc analysis, we examined which interface conditions and related evaluations of those conditions predicted intent to use. We found that timing of control, perceived ease of use for the interface, and perceived privacy threat from the interface predicted intent to use (See Table 4.7). This suggests that, when deciding whether to adopt a settings interface, people care about the decision timing options, whether the system is easy to use, and whether there is a perceived

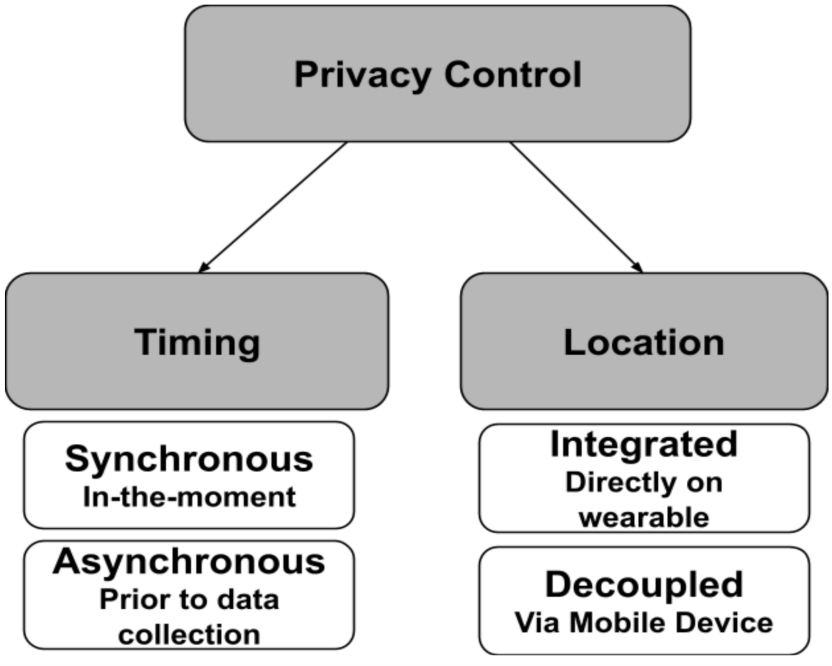


Figure 4.8. Proposed Design Space For Privacy Control on Wearable Technologies

over-sharing threat. We were surprised to see that timing of control impacted likelihood of adoption (with not-in-the moment or asynchronous options leading to more likelihood of adoption compared to in-the-moment/synchronous options) as this variable did not have a significant effect on any of the other variables we explored. It is possible that people are more familiar with the asynchronous control option because it is already on existing devices, explaining their higher reported likelihood to adopt asynchronous interfaces. The result that timing of control impacts intent to use privacy interfaces further supports the model with modified dimensions (See Figure 4.8) and suggest that this design space is something we need to attend to.

The findings also show that perceived oversharing threat explains an additional 15% of the variance for intent to use, which is a medium effect. This result suggests that designers must attend to people's perceived oversharing threat of a privacy interface when making design decisions. Additionally, the full model, which included timing, ease of use, and perceived threat, had an R^2 of .34, which is a large effect according to Cohen [66]. This suggests that it is important to account for all three of these factors together when trying to understand the likelihood of adoption for privacy interfaces. The post-hoc analyses also show that perceived privacy control is not a significant predictor of intent to use when accounting for perceived threat; it is possible that there

is a mediation or confounding effect occurring. We know from prior work [33, 68, 103, 129, 163, 258] that granular control options would be more effective and beneficial to reduce privacy related risk. In other words, proper privacy controls can help mitigate privacy threats. Future work should further explore the relationships between users' perceptions of privacy control, privacy threat, and the related likelihood of technology adoption.

4.7 Limitations

While we can draw valuable insights from our results, there are several limitations that we must acknowledge. While we are able to access a broad subject population in order to gain generalizability while staying safe during the 2020 COVID-19 pandemic, our study is limited is that we had lack of control over many of the experimental conditions. There is also a lack of ecological validity to the study, in that we simulated a mock-up of a privacy interface, and participants did not interact with a real wearable. While we were careful to make our prototype as intuitive as possible and clearly operationalize the differences for each condition, participants may not have felt they were interacting with an actual phone or wearable and saw the experiment as an interaction with something on their computer screen. This could be the reason all the ease of use ratings were fairly high and stable across conditions. We would also expect the effect to be larger if participants used an actual wearable device and phone combination.

The experiment was also very short. On average, it took participants 7-10 minutes to complete the study. This means that it participants only interacted with the prototype for 1-2 minutes. This may be the reason we did not see a significant effect of timing. In our initial planning for this study we discussed having two sessions that were separated in time by a week or so. Due to the COVID-19 pandemic we were limited in our study design and decided to simulate the study using crowd-sourced participants instead of conducting the study in the wild. Using our original approach would have allowed us to get at timing variable more appropriately, which may have allowed us to see the timing effect emerge. In future work, we will implement our privacy interfaces in a real-world setting where participants can interact with the device over an extended period of time. This will allow us to further evaluate what privacy interfaces users would prefer when interacting with a wearable that is really collecting and potentially sharing information with others.

While we did see a significant effect on the location of control, we simulated the study due to

the COVID-19 pandemic. We expect the effect to be stronger if participants used the actual wearable device and phone in combination. Overall, we believe if this study would have been conducted in the wild over an extended period of time, there is good reason to believe we would see a significant effect for both timing and location. Future research should test the impact of location and timing in an in-the-wild, longitudinal experiment.

We also ran a between-subjects experiment where participants were not exposed to all the conditions. We chose to do a between-subjects experiment to minimize fatigue effects. Furthermore, while we found valence as a significant impact on sharing preferences from study 1, in this study we used a positive neutral scenario and did not explore valence of data in this study. In this study we explored a positive neutral framing and that was done intentionally to make the scenario as neutral as possible to focus as much we could on the settings interface themselves, which may have caused the non-significant result. More specifically, the perceived oversharing threat construct could be affected by the sensitivity of the information. In this study, we explored a positive, neutral framing, which was done intentionally to make the scenario as neutral as possible to focus as much we could on the settings interface themselves. In a future study, we think it would be useful to explore if the sensitivity of the information would change the sharing decision and perceived oversharing threat. In future studies, we can look at this in a more negative or sensitive way to see if this alters user perception over privacy control and over-sharing threat. One thing we can learn from the neutral scenario is that it is unlikely to see a significant feeling of oversharing threat. Still, if there is a difference in perceived oversharing threat within these settings options in a positive, neutral scenario, it would be interesting to see that the settings themselves affect the perceived sharing threat in a very neutral positive scenario. In a volatile scenario, it would make more sense to see differences.

4.8 Chapter Conclusion

In this chapter, I investigated the impact of location of privacy control and decision timing on three aspects of user experience for wearables. Findings reveal that location of control influences overall ease of use; participants prefer to have privacy controls that are integrated on a wearable device. Results also highlight that timing of control, ease of use, and perceived-oversharing threat influence behavioral intention to use the system if it were available. In the next chapter, I explore

the potential of integrated interaction techniques that could possibly afford users in-the-moment privacy control for wearables.

Chapter 5

Study 3: User-Defined Interactions for Integrated and and In-the-Moment Privacy Control on Wearable Devices

5.1 Introduction

From the last study, I learned that location of control influenced ease of use when interacting with wearables, suggesting that users may prefer to have privacy controls that are integrated on their wearable. While there was not much contrast in the differences between the interfaces, we know that for most wearables, decoupled and not-in-the moment controls are already available on most wearables. Prior works also suggest that integrated control mechanisms could be an improved solution for users [297]. Thus, in this study, I explore the design space for integrated controls where privacy decisions can be made directly on the wearable with user-defined interactions as an alternative design option. We know from prior works [26, 241, 277, 361] that user-defined gesture sets are more complete than those defined exclusively by experts.

Wearables collect sensor data, and behavioral information [372], posing significant privacy

risks to wearers [139]. Developers and designers need to provide practical and effective ways for wearers to manage their privacy while using wearable technologies [266, 298].

A minimum step in enhancing a wearer's privacy is to inform them about what type of data is collected. A further step is to enable control over what information is collected and whether and with whom that information is shared [296, 354]. However, even on devices with large user interfaces (e.g., desktop computers, laptops, tablets, and smartphones), providing people with usable privacy choice mechanisms is challenging [296, 298, 355]. The difficulty of providing privacy controls on wearables, which have tiny user interfaces in comparison to laptops or smartphones, is exacerbated because of the limited input space [27, 233, 267, 296] and constrained interaction capabilities on such devices [298]. To be worn continuously, wearables must be small, lightweight, and comfortable [234], requirements that are currently in conflict with the large user interface needed for existing privacy control interfaces.

Instead of putting privacy controls on wearables, designers have relegated privacy controls to a paired computer or smartphone, which offer a larger user interface. For example, Fitbit requires users to manage privacy options of the wearable via its paired app [177]. However, we see the decoupling of privacy interfaces from wearables as a missed opportunity.

Wearable technologies afford new and exciting opportunities for privacy controls. Wearables, unlike many non-wearable technologies, are available to the user at the time data is collected, *Integrated and In-the-Moment*. When heart rate while exercising is captured via a wearable, the wearer is in the environment where they are exercising. This unique feature of wearables means that users do not have to make privacy decisions in advance, based on assumptions that may turn out to be incorrect. Instead, users can make privacy decisions while steeped in the nuance and context of that individual privacy decision because the wearable device is available at that moment.

Many traditional user interfaces for privacy settings are meant to be set up in advance, "checked," or updated from time to time. For example, Facebook recently released an updated "Privacy Checkup tool" [2], which allows users to review who can see their profile information and posts. This type of privacy user interface is not designed to be accessed Integrated and In-the-Moment. Rather, it is designed to be used during an a priori session dedicated to making privacy choices in advance of data collection and sharing. Making privacy decisions before a person knows what data is collected presents difficulties for users [34, 69, 174, 259] and results in privacy concerns, unanticipated sharing, and regrets about what is shared [140, 257, 310, 347].

The opportunity we identify is that wearables have the potential to couple sharing decisions with privacy interfaces to offer Integrated and In-the-Moment privacy control. However, a challenge is that we do not yet know what user interface mechanisms for Integrated and In-the-Moment privacy control are usable. We meet this challenge by identifying a set of user-defined interactions that can provide Integrated and In-the-Moment privacy controls on wearables. This work also guides researchers toward a more informed understanding of how we can use human-centered techniques to design interfaces that expand the privacy options available to users.

5.1.0.1 Research Questions

While the complexity of privacy management is quite nuanced, and managing privacy on miniaturized devices like wearables is challenging, a holistic understanding of how an individual manages their privacy Integrated and In-the-Moment requires context-specific studies. As a first step, we explore how contextualizing privacy decisions into a users' interaction flow can be useful for more effective privacy control. In an experiment that simulates realistic privacy decision tasks, we seek to answer the following research questions:

- What interactions do users propose to communicate privacy decisions about data from a wearable?
- Does social context (e.g., whether people are alone, in the presence of others or in a situation where they need to be discreet) affect the type of interactions people propose to communicate privacy decisions?
- Are there differences in the types of interactions people propose for situations requiring privacy (e.g., when they are around others, but need to be discreet) vs. situations that require less privacy?

5.1.1 A Focus on Device-Independent Interactions

A primary goal of this work is to find a set of interactions that will not only work across many devices but can also guide the development of new devices. Indeed, we agree with the human-centered design school of thought that suggests that user needs should lead to the creation of new technologies, rather than a technology-centered approach where technologies are first created, then,

hopefully, find a user need to satisfy. To that end, we designed our study and contributions to be device-independent. We chose NOT to have participants interact with a prototype we developed and suggest interactions for that single prototype. Instead, we offered participants the opportunity to generate interactions without constraining them to our prototype's placement on the body or sensors. This study design choice means that the set of interactions we identify can be used to guide the development of privacy controls to enhance existing wearables and potential wearables that are not yet designed.

5.1.2 Contextualizing Privacy Decisions Allows Surprising Complexity from Binary Choices

Privacy decisions are notoriously complex, as we discuss extensively in the related work section on privacy theories. However, we discovered that once we *contextualize* complex decisions Integrated and In-the-Moment, these complex questions can be answered with a simple, binary choice: *share* vs. *withhold*. Other variables related to privacy, such as the type of data and the potential recipient, can be embedded in a question asked to participants Integrated and In-the-Moment. For example, a wearable device with audio output capability (e.g., via an earphone) can identify the content of interest by producing the following audio:"Your stress levels were high today." Then, the wearable can ask, "Would you like to share this information with your healthcare provider?" This identifies the potential recipient and prompts the wearer to respond. The user then needs only respond with a *share* or *withhold* decision, in the context of the moment, with all the complexity that being in that moment entails.

Contextualizing privacy decisions affords expression of privacy decisions in an explicit, actionable way [266, 296]. While Schaub and colleagues focused on privacy notices in their piece, *Designing Effective Privacy Notices* [296], many of the same principles apply to privacy choice interfaces. Privacy choice interfaces should provide relevant, actionable, and understandable information in the transactional context [296]. Providing information and a decision interface in the transactional context can help "users incorporate privacy considerations into their privacy decision making" [296]. Decisions made in context also require less interpretation by the user [296]. Notably, these notices and decisions in context can be incorporated into the user's interaction flow without being overly disruptive [296]. Furthermore, we can use the decisions made over time to generate preference

models that would reduce the need for people to be asked about their privacy preferences over time.

In this study, 32 participants saw or heard a scenario describing a transactional context via a head-mounted device or wrist-worn device. Next, they received a description of data collected by a wearable (e.g., sleep goal met, failed to meet step goal). Then, participants responded with one of two options, *share* or *withhold*, to express their sharing choice. We then asked participants to demonstrate an interaction that they would use to execute their binary sharing preference in that context. One way we contextualize privacy decisions in this work is by embedding social context in the scenario. We diverge from Nissenbaum's notion of "social context". In the theory of privacy as contextual integrity (CI), Nissenbaum identifies all "context" as "social context." Social context, she says, is "not formally constructed but, discoverable as natural constituents of social life. As theorized in sociology, social theory, and social philosophy, they have been assigned various labels, including, social domains, social spheres, fields, or institutions." In this paper, we use social context to indicate a much narrower concept: whether people are alone, in the presence of others, or trying to be discreet.

5.1.3 Overview

In this chapter, I describe results from an open-ended elicitation study [27, 361], where we elicit intuitive interactions from end-users that imply binary sharing preferences of some data collected by a wearable (e.g., activity data) with a given recipient (e.g.,social network) across three social contexts: *alone*, *in the presence of others*, and *discreet*.

Building on the participatory nature of prior end-user elicitation studies, which primarily investigate gesture-based interactions for a specific device [27, 112, 226, 228, 361], we adapted this method in two ways. First, we expanded our investigation to include all potential *interactions* (e.g., speech), rather than just *gestures*. Second, we took a *device-agnostic* approach that informs our understanding of the types of interactions users produce exclusive of any specific device. It is critical for the Ubicomp community to have a clear understanding of what types of interactions for privacy control on wearables are intuitive to users.

To that end, the overall goal of this study is to identify a user-defined set of privacy control interactions that feel natural and intuitive. The interaction set can inform design decisions and fabrication of future wearable technologies that enhance the privacy of wearables.

The primary contributions of this work are five-fold:

- A qualitative and quantitative analysis of user-defined,device-independent input interactions for wearables that enable usable Integrated and In-the-Moment privacy control.
- A set of 20 user-defined interactions that allow users to imply sharing preferences about information collected by a wearable.
- An exploration of how interactions vary based on social context.
- Establish a taxonomy of interactions for Integrated and In-the-Moment privacy control over data from wearables.
- Using the taxonomy, we analyze the physical properties of interactions produced, including interaction modalities.
- Implications for incorporating Integrated and In-the-Moment interactions to enable privacy control into existing and novel wearables.

Using Caine's privacy behavioral model [52] in study 1, I focused on participants' decision to share or withhold information from a wearable using binary decisions in my experimental design. Binary decisions, combined with auditory or visual prompts about the *content* and *recipient* provide a rich, nuanced space for privacy decision making. Furthermore, the key innovation and benefit is that these decisions are naturally contextualized, Integrated and In-the-Moment, with all the nuance and context that the moment affords. In the next section, I discuss the methods used to explore what interactions users chose to express these binary decisions.

5.2 Method

We conducted an open-ended interaction elicitation study [226, 361] with 32 participants. Elicitation studies can inform natural, simple to perform, and easy-to-recall interactions [27, 112, 226, 228, 361]. Building on the participatory nature of these studies, we used this method to identify a set of user-centered interactions to enable in-the-moment privacy decisions. The within-subjects scenario-based experimental design asked participants to design corresponding interactions that could be used to execute the binary response of either *share* or *withhold* some type of data with a given set of recipients.

Prior work has established that elicitation studies are widely used in HCI to successfully inform the design of a gesture set for a given interactive technology. A gesture is a movement of part of the body to express an idea, or meaning [45, 218]. In our work, because we are interested

in identifying a device-independent set of interactions, we are not limited to only *gestures* as input. Instead, we are interested in all interactions that could be used to provide input to a wearable device. Interaction concerns two entities (e.g., an input device or technology and the end-user) that determine each other's behavior over time [153]. A gesture is a subset of, or a modality of, an interaction. However, gestures are not the only form of input that can be provided to a system. Another form of input that can be provided to a system, for example, is speaking or touching a device. In our work, we do not want to exclude such non-gestures but instead prefer to collect these as part of a possible interaction set. Therefore, while we adopt the *elicitation* method, we extend the method to include all proposed input elicited from participants. Thus, we re-characterize the method as *interaction elicitation* rather than *gesture elicitation*.

The entire study was approved by the IRB.

5.2.1 Participants

We recruited 32 participants (18 female, 14 male) using flyers posted around the campus of a large U.S. southeastern university. Flyers briefly described the study, noting that it would include a one-hour study, noted the remuneration amount (a $20 gift card), and included an email address where participants could indicate their interest. After expressing interest, potential participants were scheduled for a study session. Other than expressing interest, there were no inclusion or exclusion criteria about who could participate in the study.

Participants' ages ranged from 18 to 35 years old with 63% age 18-24, 31% age 25-34, and 6% aged 35-44. Forty-two percent of participants reported having intermediate technical expertise, while 32% reported having advanced technical expertise. Fifty-nine percent of participants reported that they currently own a wearable device.

5.2.2 Referents

The primary referents we used in this study are *share* and *withhold*. Prior elicitation studies describe referents as operations that are executed as commands, and the result or response to execute that command would be a gesture or an interaction [361]. Each referent was placed in a scenario that provided the social context, type of information, and potential recipient. We describe this in the following section below.

Study Demographics		
Gender	Male	14 (44%)
	Female	18 (56%)
Age	18-24	19 (63%)
	25-34	11 (31%)
	35-44	2 (6%)
Education	High School Grad	5 (16%)
	Some College	6 (19%)
	Four Year College	9 (28%)
	Some postgraduate	3 (9%)
	Postgrad or Professional	9 (28%)
Ethnicity	White	19 (59%)
	African-American	7 (22%)
	Asian	5 (16%)
	Other	1 (3%)
Technology Knowledge	Basic	2 (7%)
	Intermediate	13 (42%)
	Advanced	10 (32%)
	Professional	6 (19%)
Wearable Device Ownership	Own Wearable	19 (59%)
	Wrist-worn device	17 (53%)
	Head-mounted device	10 (31%)
	Both	8 (25%)

Table 5.1. Demographics of Study Participants

5.2.3 Scenario Design

We designed scenarios to address the nuances of privacy management and the kind of decisions people make about whether or not to share data collected from wearable devices.

Each scenario asked participants to consider multiple privacy-related variables resulting in a binary answer of either *share* or *withhold* (See section 3.3.4). Based on their binary choice, participants provided an interaction to express that choice. The interaction participants provided serves as the dependent variable.

The independent variable of interest for this study is *social context*, which contained three levels: *alone*, *in the presence of others*, and *discreet*.

In the *alone* condition, the scenario described a situation where the participant was by themselves, whereas in the *in the presence of others* condition the scenario described a situation where the participant was around other people. In the *discreet* condition we asked participants to design an interaction they would use if they wanted to respond in a discreet or private way without drawing attention to themselves. Within the scenario we also manipulated the type of data

collected (e.g., “step count goal”) and the potential recipient of the data (e.g., “family and friends”) to simulate a realistic privacy decision making task.

5.2.4 Setting and Apparatus

We conducted the study in a lab to maintain control over variables such as the social context, to ensure all participants experience was similar, and so that we could record the session for analysis.

We used two wearable devices - one head-mounted device and one wrist-worn device - to present prompts to participants (see Figure 5.1). The wrist-worn device was an Apple Watch which produced visual prompts and the head-mounted device was a pair of bone conduction headphone which produced auditory prompts. Neither of these devices were intended to sense or recognize any input (e.g., gestures, speaking) by the users.

(a) Scenario presented via wrist-worn device.

(b) Scenario presented via head-mounted device

Figure 5.1. Stimuli Used in Interaction Elicitation

5.2.5 Procedure

5.2.5.1 Pre-Experiment Phase

Upon expressing interest, participants were provided details about the study and information about informed consent. After providing informed consent, participants completed a 23-item questionnaire. The survey instrument was implemented in Qualtrics (www.qualtrics.com). Qualtrics is an online survey platform used to create, distribute, collect, and analyze survey data. The questionnaire contained four sections: six demographic questions including age, race, educational background, and marital status, one question about knowledge of technology, one internet usage frequency question, one social network usage frequency question, and two questions about wearable device ownership. Additionally, we collected participants' views on privacy and surveillance in everyday life via a second single item questionnaire [206]. Once participants completed the pre-experiment questionnaire, they were assigned a randomly generated number ranging from 1-32. This number was used as a participant identification number and was subsequently used to assign each participant to a scenario set (which varied social and environmental context, for example).

5.2.5.2 Consent and Instructions

Upon arrival to the lab, participants were greeted and seated across from the experimenter. Prior to beginning the interaction elicitation exercise, we reaffirmed participants' consent. Next, the experimenter provided participants with an overview of the wearable devices which served as method of presentation of the experimental stimuli (described in section 5.2.4;see Figure 5.1). Following the explanation of the wearable devices, we reminded participants about the purpose of the study and then described their role. We told participants that they would hear a scenario from the experimenter and then receive either an auditory (e.g., on a head-mounted device) or visual prompt (e.g., on wrist-worn device) depending on which wearable they had on at the time. Upon receiving the prompt, they would propose an interaction that would indicate whether they wanted to *share* or *withhold* information given that scenario.

Furthermore, similar to work by [27, 361]) we sought to remove the gulf of execution [245] between participants' current understanding of how wearable technologies detect input by informing participants that absolutely any interaction they proposed would be recognized by the device and would be appropriate in the context of this experiment. We did this to avoid having existing gestural

user interfaces on wearable devices constrain or influence user behavior as participants designed their preferred method of input.

5.2.5.3 Training to Reduce Legacy Bias

Next, we conducted a short training exercise to ensure participants understood the concept using some part of their body to express an action or feeling, be it verbal or non-verbal [45, 215] to reduce legacy bias.

As we described in section 2.3.0.3 in the literature review, legacy bias a primary concern in end-user elicitation studies is *legacy bias* [227]. To increase the novelty of interactions among participants while reducing legacy bias, we adopted the priming and production technique proposed by Morris et al. [227]. For the priming technique, we asked participants to show us how they would respond to a given scenario using some part of their body. Using the production technique, participants could propose up to 12 different interactions based on their sharing preference if they wished.

The first training example we provided to participants was *"Imagine that you are at your favorite sports team game and they score a touchdown. Show me how you would respond at that moment"* Participants responded by performing a fist pump or clapping to communicate their excitement. The next training example we provided to participants was to *"Imagine you are driving and someone cuts you off in traffic. Show us how you would respond to the driver who cuts you off to communicate your frustration."* Some participants responded by showing the middle finger, while others threw their hands up to imply frustration. The results of the training indicated participants understood the task.

5.2.5.4 Experimental Phase

Following the training exercise, we began the experiment. First, we described a scenario and asked participants to imagine themselves in that scenario. Next, participants received a prompt from one of the two devices they were wearing. When the prompt originated from the head-mounted device, participants received an auditory prompt (e.g., a voice via the bone conduction headphones said *"stress levels indicate you were calm today."*). When the prompt originated on the wrist-worn device, participants received a visual prompt (e.g., a text image on the Apple Watch showed *"stress levels indicate you were calm today.")*. See Figure 5.1 for an example of both types of prompt.

After receiving the prompt, participants first indicated their preference, then produced an interaction to either *share* or *withhold* the data identified from the recipient in the scenario. Scenarios were randomly assigned to originate from either the wrist-worn device or the head-mounted device, half of the scenarios originating from each. We instructed participants to think aloud as they performed the interaction and repeat the interaction once so that we could be sure we captured it and all its components as the participant intended. As expected, participants' responses across scenarios.

5.2.5.5 Post-Experiment Questionnaire and Debrief

Following the elicitation exercise, we asked participants if they had any questions or comments about the study. After making note of participant comments, they were then provided with post-study questionnaire.

5.2.5.6 Participant Remuneration

Each experimental session was video recorded with a single participant and took approximately 30 minutes. At the conclusion of the study, participants were remunerated with a $20 Amazon gift card for roughly one hour of total participation.

5.2.6 Data Analysis and Coding

The study produced three types of data: questionnaire responses, video clips of interactions, and transcriptions of the audio from the think-aloud portion of the study. For the participants who owned any wearable device, we also asked them about whether they had privacy concerns about their wearable. We summarized questionnaire data quantitatively and used qualitative coding to analyze the video clips of the interactions. To analyze the video clips, three researchers viewed each video clip and classified each interaction along the following dimensions: part of the body used to perform interaction and modality of interaction.

Similar to previous elicitation studies [58, 92, 270], we grouped interactions that were similar rather than identical. For example, swiping up with an index finger, was considered equivalent to swiping up with two or three fingers. We separated interactions according to the relative direction (e.g., swipe left, swipe right) and if participants did a single tap or double tap, and these were different when participants indicated their binary sharing preferences.

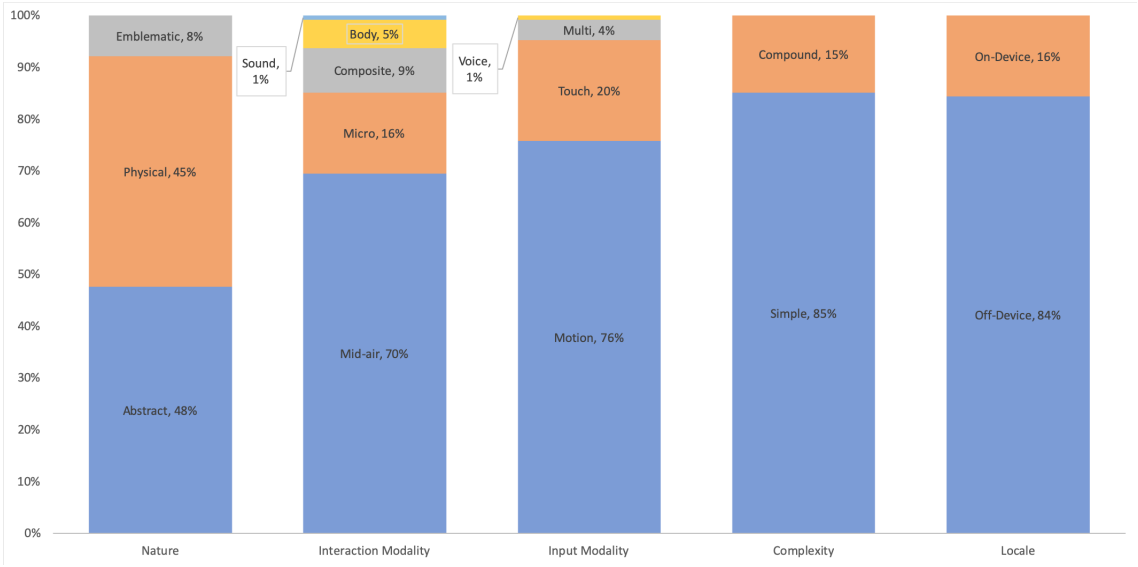


Figure 5.2. Proportion of interactions from each dimension of the taxonomy.

5.3 Results

The results from this study include an The results from this study include an interaction taxonomy for Integrated and In-the-Moment privacy control on wearables, agreement scores for referents and social context, a user-defined consensus set of device-independent interactions, along with criteria that were used to develop this set.

5.3.1 Descriptive Information about Data from Elicitation Study

Participants proposed a total of 129 unique interactions across 460 trials. A trial consists of participants receiving a prompt via a scenario, then providing an interaction suggestion. In some instances, the same interaction was produced by a single participant multiple times. In other instances, multiple participants produced the same interaction.

5.3.2 Taxonomy of Interactions For Integrated and In-the-Moment-Privacy Control on Wearables.

To better understand our participants' input interaction proposals for Integrated and In-the-Moment privacy control, we develop a taxonomy that organizes characteristics of the interactions hierarchically. Several studies (e.g., [27, 27, 92, 293, 335, 361] analyze characteristics of proposed

interactions by classifying the interactions into categories, referred to as taxonomies. Taxonomies assist researchers in gaining insights about the mental model of users [162] and provide guidance to interaction designers to help them better understand what types of interactions are most appropriate for a given referent. For example, Wobbrock et al.'s proposed taxonomy for surface gestures [361], Ruiz et al.'s proposed taxonomy of motion gestures for mobile interaction [293], Shimon et al.'s taxonomy for non-touchscreen gestures for smartwatches [27], Piumsomboon et al. taxonomy for gestures in augmented reality taxonomy [270] and Dingler et al.'s. proposed taxonomy of gestures across device types for reading control [94]. In this study, we considered the most appropriate dimensions of analysis from those taxonomies to serve as a basis for our taxonomy. No prior work we are aware of has established a taxonomy of interactions for Integrated and In-the-Moment privacy control over data from wearables.

Interaction Mapping		
Nature	Emblematic	Interaction conveys a particular meaning expressed by movements of the body widely recognized within a specific culture.
	Physical	Interaction physically acts upon an external physical surface, part of the body, or the interface of the wearable device.
	Abstract	Mapping is binary
Interaction Modality	Micro	A single-handed small interaction that can be performed quickly without interrupting primary task at hand [29, 56, 207, 233]
	Mid-air	Refers to touchless interactions performed freely in 3D space with one or multiple parts of the human body using non-intrusive sensors [22, 344]
	Composite	A single channel of input where the interaction combines two or more unimodal interactions (e.g. Tap + swipe) to develop a more high-level interaction [73]
	Sound-based	Refers to any interaction that is recognized by a sensor based on the sound.
	Multimodal	Refers to any interaction that used a combination of either speech, pen, touch,hand gestures, eye gaze, and head and body movements [250]
	Body-based	Refers to any interaction that directly involves movements of the body without the use of a device. For example, a head nod, head shake or foot are interactions that are performed without directly touching a wearable device
Input Modality	Touch-based	Refers to the user providing direct input through touch to the device that can be recognized.
	Motion	Some form of motion is recognized by the device to detect interaction
	Multi	A combination of the previously listed modalities of input
Physical Characteristics		
Complexity	Simple	Consists of a single interaction
	Compound	Interaction can be decomposed into simple interactions
Locale	On-Device	Interaction occurs directly on the interface of the device
	Off-Device	Interaction occurs off the device (e.g. mid-air)

Table 5.2. Taxonomy of interactions for Integrated and In-the-Moment privacy decisions for wearables based on 128 unique interactions collected interactions from 460 trials

Similar to Ruiz et al. [293] and Shimon et al. [27] we classified interactions across two high-level dimensions - *interaction mapping* and *physical characteristics*. While these works classify the first dimension as *gesture mapping*, we classify it as *interaction mapping*, as some of the

inputs that participants proposed extended beyond the modality of gestures (e.g., touch, speech) and were therefore outside the scope of solely gestural interaction. Interaction mapping describes how interactions are mapped to situational conditions by participants, and they were divided into nature, interaction modality, and *input modality* categories. Physical characteristics describe the characteristics of the interactions themselves and include the *part of body* used to perform the interaction and the *complexity* of the interaction. The full interaction taxonomy is listed in Table 5.2. The nature dimension is at the highest level within the *interaction mapping* dimension. Similar to other elicitation studies that utilized this dimension for their proposed taxonomy, this dimension defines the relationship between the interaction to physical objects (e.g., wearable devices, surfaces, or nearby platforms) or the intended task and how they relate to each other. The nature dimension is divided into *emblematic*,*physical* and *abstract* categories. *Emblematic interactions* are classified as interactions that impart a specific meaning expressed by movements of the body that are widely recognized within a specific culture [18, 196, 212]. For example, in the western culture, thumbs up usually signify approval. *Physical interactions* are classified as interactions that physically act upon an external physical surface, part of the body, or the interface of the wearable device. For example, double tapping on the screen of the device or tapping the hand to activate input for a wearable worn on the wrist. *Abstract interactions* are classified as interactions that were arbitrary, as these interactions did not fit into the aforementioned categories.

The *interaction modality* dimension refers to the form of input that a human provides to a system for some desired outcome. Interactions from this dimension are divided into *micro*,*mid-air*,*composite*, and *mutlimodal interactions*. *Micro interactions* are classified as small one-handed interactions (e.g. tap, press) that can be completed quickly without interrupting primary task at hand [29, 56, 207]. Mid-air interactions are classified as interactions that involve touchless manipulations based on sensor modalities of body movements and gestures [344]. Composite interactions involve a combination of two or more interactions decomposed into one interaction. Multimodal interactions are classified as interactions that use a combination of other input modalities [250].

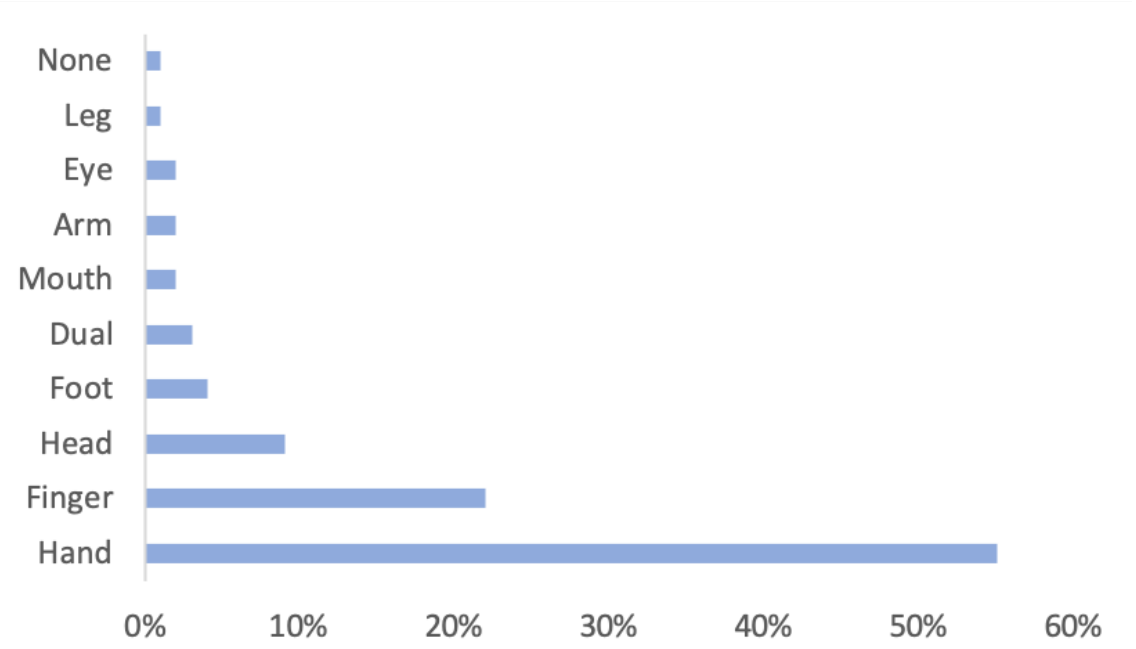


Figure 5.3. Proportions of interactions involving each part of the body.

5.3.3 Findings from Classification

5.3.3.1 Taxonomic Breakdown of Interactions From of Data

Figure 6.6 illustrates the breakdown of the 129 unique interactions collected across 460 trials during the study using our taxonomy. Within the five dimension taxonomy, the most common characteristics of the interactions proposed by participants were *simple, off-device,motion-based, mid-air interactions.*

In the *nature* dimension interactions were mostly *abstract (48%)*, and *physical (45%)*. The interactions chosen to propose *share* and*withhold* were mostly abstract in nature. In the *interaction modality* dimension, most of the interactions were mid-air interactions. As far as input modality, most interactions were motion based, simple and performed off the device.

5.3.3.2 Use of Body Parts

Figure 5.3 shows the use of body parts participants chose to use for their interactions. Single hand interactions were the most preferred, followed by interactions using one or more fingers.

Hand interactions were commonly performed in the form of movements such as air swipe, wave of hand, shaking of the hand. There were no distinctive interactions for the share or withhold

referent that was used with strictly the hand, but we did notice more distinctive interactions that used the finger for the share referent. Across both referents, there were an overall diverse set of interactions using the hand. Finger interactions commonly featured one or more fingers to tap, wave, swipe, or press to express sharing preferences. Some participants used interactions using the head as emblematic interactions to express preferences for sharing by either performing a head nod or head shake to express preferences for sharing.

5.3.4 Criteria For Developing A User-Defined Set

We chose the following metrics as criteria to generate a user-defined set of interactions that enable Integrated and In-the-Moment privacy control for wearables:

- The medium to highest agreement scores across all interactions considering referent (*share* vs. *withhold*), and social context (*alone* vs. *in the presence of others* vs. *discreet*)
- The individual frequency of unique occurrences of interactions considering referent (threshold >= 5)
- Interactions that had a symmetrical match.

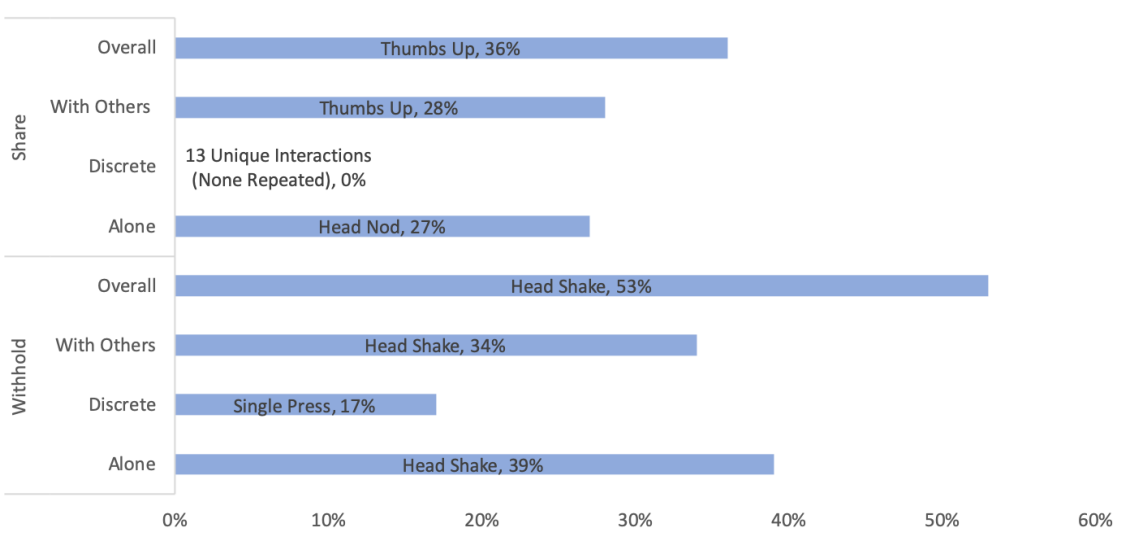


Figure 5.4. Highest Max-Consensus Ratio for the referents and included social contexts used during the interaction elicitation exercise. Interactions that had the highest consensus are shown in the Figure. Agreement rates of less than 10%, between 10% and 30%, and between 30% and 50% are considered low, moderate, and high agreement respectively [335]. *Note: The referent *share* while in the presence of others;discreet, had no max-consensus as none of the 13 interactions were repeated.

5.3.5 Comparison of Interactions Elicited to Criteria

Table 5.3 lists all interactions that met at least one criteria. In the table, each interaction elicited is organized by corresponding referent and social context (in the first two columns). Then, in the rightmost three columns, there is an indication of whether the interaction met each criterion. For example, we see that the interaction *head nod* met all three criteria for the referent *share* in the social context *in the presence of others*. We also see that the interaction column for the social context *discreet* is blank. This is because participants proposed 13 unique interactions, none of which met any criteria.

In the following sections, we provide detailed results for each criterion, starting with consensus, then moving on to frequency of unique occurrence, and symmetric match.

5.3.6 Consensus Among Interactions

First, we organize the consensus results at the interaction level by referent (*share* vs. *withhold*) and social context (*alone vs. in the presence of others vs. discreet*). We show both the max-consensus and consensus distinct ratio in Table 5.4 which separates results by the referent and context.

5.3.6.1 Formulating Agreement

To assess agreement and identify interactions that are most common among all participants, we use Morris's [226] metric of consensus (max-consensus and consensus-distinct ratio). Max-consensus is a calculation of the percentage of participants suggesting the most common interaction produced for a given referent See Equation 5.1, where P_r is the set of proposed interactions for the referent r, and P_i is the subset of identical gestures from P_r.

$$Max - Consensus = max\left(\forall_{P_i \subseteq P_r}\left(\frac{|P_i|}{|P_r|}\right)\right) \tag{5.1}$$

Previous interaction elicitation studies (e.g.,[27, 56, 58, 92, 293, 335, 365]) use either Wobbrock et al.'s [361] level of agreement metric or Vatavu and Wobbrock's Agreement rate metric [336] to assess the degree of consensus among participants. This concept of agreement developed for use in studies where participants were presented with a targeted number of tasks (referents), broken up into a targeted number of categories and asked to propose an interaction that would be appropriate

Referent	Social Context	Interaction	Frequency	Max Consensus	Symmetric Match
Share	in the presence of others	Head Nod	*	*	*
		Swipe Up		*	*
		Thumbs Up	*	*	*
	Discreet	Blink once			*
		Double Foot Tap			*
		Head Tilt Right			*
		Single Nod			*
		Single Tap Device			*
		Thumbs Up			*
	Alone	Head Nod	*	*	*
		Swipe Up	*	*	*
		Double Tap Device	*	*	*
		Thumbs Up	*	*	*
Withhold	in the presence of others	Air Swipe Left		*	*
		Cut it out		*	
		Double Tap Device	*	*	*
		Ear Tug		*	
		Finger Wave		*	
		Flick Wrist Once		*	
		Hand Wave	*	*	
		Head Shake	*	*	*
		Head Tilt Left		*	*
		Single Tap Device	*	*	*
	Discreet	Head Shake		*	*
		Single press		*	*
		Double Tap Device			*
		Finger Swipe Left			*
		Grab Wrist Turn Upward			*
		Hand Wave to the Left			*
		Head Raise Up			*
		Head Tilt Left			*
		Left Shoulder Shrug			*
		Single Nose Tap			*
		Single Nod			*
		Single Tap Device			*
		Thumbs Down			*
		Turn Head to the Right			*
		Turn Wrist Down			*
		Double Wrist Flip			*
	Alone	Hand Wave		*	
		Head Shake		*	*
		Hand Shake		*	
		Turn Wrist Once		*	*
		Speak "No"	*	*	*

Table 5.3. Table showing all interactions that met at least one criterion. Interactions are organized by corresponding referent and social context along with an indication of whether the interaction met each of the three criterion. Interactions that meet a given criterion are marked with an *
NOTE: Frequency is the individual frequency of unique occurrence with a minimum of five and max consensus is medium or high only.

for the specified task. In these studies, referents were presented to participants via the experimenter, or through some type of software. After being presented with the referent, participants are asked to immediately propose a input interaction that would activate the given task. In some cases participants were asked to propose multiple interactions per referent and choose the one they preferred the most. Additionally, in some studies (e.g. [92, 112] participants are asked to suggest interactions for a specific task under a specific conditions (e.g. sitting, standing, hands preoccupied). [56, 92].

Referent and Social Context	Interaction With Highest Consensus	Max-Consensus	Consensus-Distinct Ratio
Share (overall)	Thumbs Up	36%	0.472
in the presence of others	Thumbs Up	28%	0.566
Discreet	13 Unique Interactions (None repeated)	**0%**	1.000
Alone	Head Nod	27%	0.596
Withhold (overall)	Head Shake	53%	**0.291**
in the presence of others	Head Shake	34%	0.360
Discreet	Single Press	17%	0.651
Alone	Head Shake	43%	0.389

Table 5.4. The referent and social context along with the interactions participants produced with the highest consensus. The overall max-consensus and consensus-distinct ratios are shown for each referent and included context. The highest scoring referent(s)/context(s) for each metric are shaded in grey, whereas the lowest scores are indicated in **bold**.

In our study however, like Morris [226], we used a repeated measures design where participants could propose a variable number of interactions per referent, under different social contexts making Morris's method more appropriate for our analysis than Wobbrock et al's. Table 5.4 displays the results for both the the max-consensus and consensus-distinct ratios for each referent along with the social contexts.

5.3.6.2 Consensus Considering Referent and Social Context

Across both referents (*share* and *withhold*) and social context (*alone*, *in the presence of others*, and *discreet*), the max-consensus metric ranged from 0.00 (low agreement, *max-consensus* <0.10) to 0.53 (high agreement, 0.30 < *max-consensus* < 0.50) while the consensus-distinct ratio ranged from .291 to 1.000. Furthermore, across both referents and social context, we find that the mean max-consensus was 30% and mean consensus-distinct ratio was .475 (using a consensus threshold of two).

As displayed in Figure 5.4 and Table 5.4, excluding social context, the *thumbs up* interaction had the highest max-consensus for the referent *share*, while the *head shake* interaction had the highest max-consensus for the referent *withhold*. Considering social context *while in the presence of others*,

for the referent *share*, *thumbs up* also had the highest max-consensus among interactions. Similarly, for the referent *withhold*, in the social context *in the presence of others*, the *head shake* interaction had the highest consensus among interactions. Additionally, for the referent *withhold* for both the social contexts *in the presence of others* and *alone*, the *head shake* interaction also had the highest consensus among interactions. For the referent *share* in the *alone* condition the interaction with the highest consensus was *head nod*. We did not find consensus for the referent *share* in the *discreet* condition. Participants in this condition produced 13 unique interactions.

For the referent *withhold* in the *discreet* condition the interaction *single press* achieved a moderately low consensus of 17% in comparison to the other scores, but surprisingly high consensus-distinct ratio. Looking at the interactions with the highest consensus here provides a unique non-conflicting set of interactions for both referents (*share/withhold*) along with social contexts. To further extend our interaction vocabulary, we will now examine interactions with medium to high consensus for the given referent, including social context.

Referent	Social Context	Interaction	Max-Consensus
Share	in the presence of others	Head Nod	20%
		Swipe Up	12%
		Thumbs Up	28%
	Discreet	-	
	Alone	Head Nod	27%
		Swipe Up	18%
		Thumbs Up	23%
		Double Tap	18%
Withhold	in the presence of others	Head Shake*	34%**
		Single Tap Device	19%
		Hand Wave	16%
		Double Tap Device	16%
	Discreet	Single Press*	17%
		Head Shake	13%
	Alone	Head Shake*	43%**
		Speak "No"	18%
		Hand Wave	18%
		Turn Wrist	14%
		Shake Hand	11%

Table 5.5. Interactions with medium and high max-consensus. Interactions with high max consensus (>0.30) are marked with an *.
Note: None of the interactions from the *share; discreet* condition achieved high or medium max-consensus.

5.3.6.3 Interactions With Medium to High Consensus

The next metric we examined was interactions with medium or high consensus. We considered interactions that had medium ($0.10 < \textit{Max-Consensus} < 0.30$) to high ($\textit{Max-Consensus} > 0.30$) consensus for the given referent, including social context. As shown in Table 5.5 there are multiple interactions with medium to high max-consensus for all referents including social context, except for

share; discreet. No interactions in the *share; discreet* referent condition achieved even medium max-consensus. Also notable is that the interaction *double tap device* achieved medium max-consensus in both the *share; alone* and *withhold; in the presence of others* referent conditions and is therefore conflicted. Other interactions were repeated within referent condition not considering context (e.g., *thumbs up* in the *share* condition) but no others were conflicted in that they occurred in both *share* and *withhold*.

5.3.6.4 Interactions Produced by at Least Five Participants (Individual Frequency).

The next metric we will discuss is the individual frequency of unique occurrences of interactions considering referents (see Table 5.6). Table 5.6 shows all proposed interactions that have consensus threshold of five or more for referents *share* and *withhold*. A consensus threshold of five means that at least five participants proposed the same interaction.

Referent	Social Context	Interaction	# of unique participants who proposed interaction (N=32)	total # of times interaction proposed across all trials (N=460)	% of participants who proposed interaction
Share	in the presence of others	Thumbs Up	7	9	28%
		Head Nod	5	6	20%
	Discreet	-			
	Alone	Head Nod	6	7	27%
		Thumbs Up	5	5	23%
		Double Tap Device	4	4	18%
		Swipe Up	4	6	18%
Withhold	in the presence of others	Head Shake	11	15	34%
		Single Tap Device	6	6	19%
		Double Tap Device	5	7	16%
		Hand Wave	5	7	16%
	Discreet	Single Press	6	6	20%
		Head Shake	4	4	13%
	Alone	Head Shake	12	17	39%
		Hand Wave	5	5	16%
		Speak "No"	5	8	16%

Table 5.6. Frequency of interactions produced by participants during the interaction elicitation. Only interactions that met the threshold of five are included. No interactions in the *share; discreet* referent condition met the threshold of five.

As Table 5.6 shows there are multiple interactions that meet the threshold of five for both referents across all social contexts, except for the *share; discreet* referent condition. No interactions in the *share; discreet* referent condition reached the threshold of five. Also notable is that the interaction *double tap* met the threshold for both *share; alone* and *withhold; in the presence of others* and is therefore conflicted. Other interactions were repeated within referent condition not considering social context (e.g., *thumbs up* in the *share* condition for both *in the presence of others* and *alone*) but no others were conflicted in that they occurred in both *share* and *withhold*.

Table 5.6 also shows the total number of times each interaction that met the threshold of five was proposed across all 460 trials. A higher number indicates 1) that more participants proposed the interaction and/or 2) one or more participants repeated the same interaction across multiple trials. For example, we see that 12 participants uniquely proposed *head shake* in the *withhold; alone* referent condition, but that it was repeated 17 times across all trials. On the other hand, while six participants uniquely proposed *single tap device* in the *withhold; in the presence of others* referent condition, none of the six repeated the interaction.

5.3.6.5 Interactions With a Symmetrical Match

A symmetrical match is defined as an interaction that is made up of similar components of its match but produces an opposite affect. All interactions with a symmetrical match are shown in Table 5.3 and are marked with a * in the "symmetric match" column. An example of an interaction with a symmetrical match is *head nod* for the referent *share; alone*. The symmetric match for this interaction would be *head shake*, for the contextual referent *withhold; alone.*. We noted interactions with a symmetrical match, even if that interaction was not produced by participants in our study. For example, for the referent *withhold; alone* participants proposed the interaction *speak "no"*. However, no participants proposed its symmetrical match, *speak "yes"*, in any condition. Because *speak "no"* has a symmetrical match, we considered *speak "no"* to have a symmetrical match, and therefore marked it with an * to Table 5.3.

We then evaluated these 12 interactions to see if there was a symmetrical match for each (e.g. t*humbs up / thumbs down).* Of the 12 total interactions six had a symmetrical match (*thumbs up / thumbs down, head nod / head shake, double tap, single tap*).

We wanted to have a balanced set of interactions for each referent, so we decided to select an interaction that had a symmetric match for each of the remaining interactions. Therefore, we removed the *shake hand* interaction because this interaction did not have a symmetric match. For the *hand wave* interaction for the referent *withhold* participants did not specify the direction. To make this interaction reversible, we assigned *hand wave* to the left for the referent withhold, and *hand wave* to the right for the referent share.

This process resulted in the following interactions: Share = *double press, hand wave right, speak "yes", swipe up, turn wrist twice* ; Withhold = *single press, hand wave left, speak "no", swipe down, turn wrist once.*

5.4 Discussion

Individuals need to be able to communicate their sharing and privacy preferences to wearable devices and even more important that they can do this Integrated and In-the-Moment for effective and usable control [296]. In this section we introduce a set of interactions that will enable Integrated and In-the-Moment privacy control on wearable devices. Then, we discuss the broader implications of our results for the design of device-independent interactions.

5.4.1 A User-Defined Consensus Set

The set of interactions we identify for Integrated and In-the-Moment privacy control on wearable devices is graphically presented in a Venn diagram (Figure 5.5). This set combines agreement (max consensus) findings, frequency of unique occurrence, and interactions with a symmetrical match to create a consensus set. To generate this set, we took all interactions that met two or more of the criteria (as shown in Table 5.3) and added interactions that had symmetric matches for the opposing contextual referent condition. This resulted in a set of 20 interactions as shown in Figure 5.5.

The Venn diagram in Figure 5.5 shows a clear, logical relationship between the three social contexts (alone, in the presence of others, and discreet) and the interaction(s) that met our criteria for each context. The diagram shows interactions that are exclusive to each social context (e.g., *press single/double* only appear in the *discreet* condition), as well those that satisfy multiple social contexts (e.g., *head nod/shake* is at the intersection of all three social context conditions).

Each interaction shown in Figure 5.5 has a symmetrical match for the opposing command beside it. The leftmost interaction shown in the symmetrical pair satisfies the referent *share*, and the rightmost interaction for the pair satisfies the referent *withhold*. For example, in the circle labeled *discreet* the leftmost interaction is *press single*, corresponding to *withhold* and the rightmost interaction is *press double* corresponding to *share*. The venn diagram also clearly shows that only a single interaction pair met our criteria for the *discreet* condition.

For the interactions *speak* and *turn wrist*, we only include a single image of the interaction but describe the symmetrical pair below the image. While the *speak* interaction for the referent *share* did not meet our first two criteria, it was a symmetrical match for its opposite command for the referent *withhold*, which met our specified criteria.

Similarly, the *turn wrist once* interaction met our criteria for *withhold* in the *alone* condition, so we added its symmetric match *turn wrist twice* for the referent *share*. While we did find some promising discreet interactions (e.g. *blink once*, *tap foot*) proposed by participants, we only found one interaction in the discreet condition (*press single/double*) that met our criteria.

Speak, *swipe*, and *turn wrist* are the only interactions that met the criteria for the alone condition. Furthermore, *head tilt*, *swipe on device*, and *finger air swipe* only met the criteria in the *in the presence of others* condition.

The remaining interactions in the Venn diagram met the criteria for both the *in the presence of others* and *alone* conditions. Those interactions are *thumbs up/down*, *double/single tap*, *hand wave right/left*.

5.4.2 Implications

In this section, we describe the implications of this work including the need for discreet interactions, the promise of symmetrical interactions and hardware and software needs.

5.4.2.1 A Need for Discreet Interactions

We found notable differences in the types of interactions people produced for situations requiring privacy vs. those that need less privacy. Notably, participants did not propose any sound-based interactions or multimodal interactions when instructed to be discreet. Sound-based interactions – or at least speaking words out loud – may not be suitable for situations when people need to be discreet in the presence of others (e.g. during a meeting) since other people are likely able to hear spoken words [78]. Speaking as a modality of interaction may distract others and may not be suitable in specific social contexts. On the other hand, when people do not need to be discreet (e.g., in public alone), word-based sound interactions may be suitable.

Participants also did not propose multimodal interactions when asked to be discreet in the presence of others. Multimodal interactions use a combination of inputs (e.g., speech, touch, visual). In most instances, those types of interactions involve two or more parts of the body [328] and therefore may be more likely to be noticeable by an observer [57, 288]. We were surprised that over half of the interactions produced in the discreet condition were mid-air, and just under a third were micro-interactions. However, among these mid-air and micro-interactions, participants were deliberate in creating private interactions that were subtle and therefore may not be easily deemed

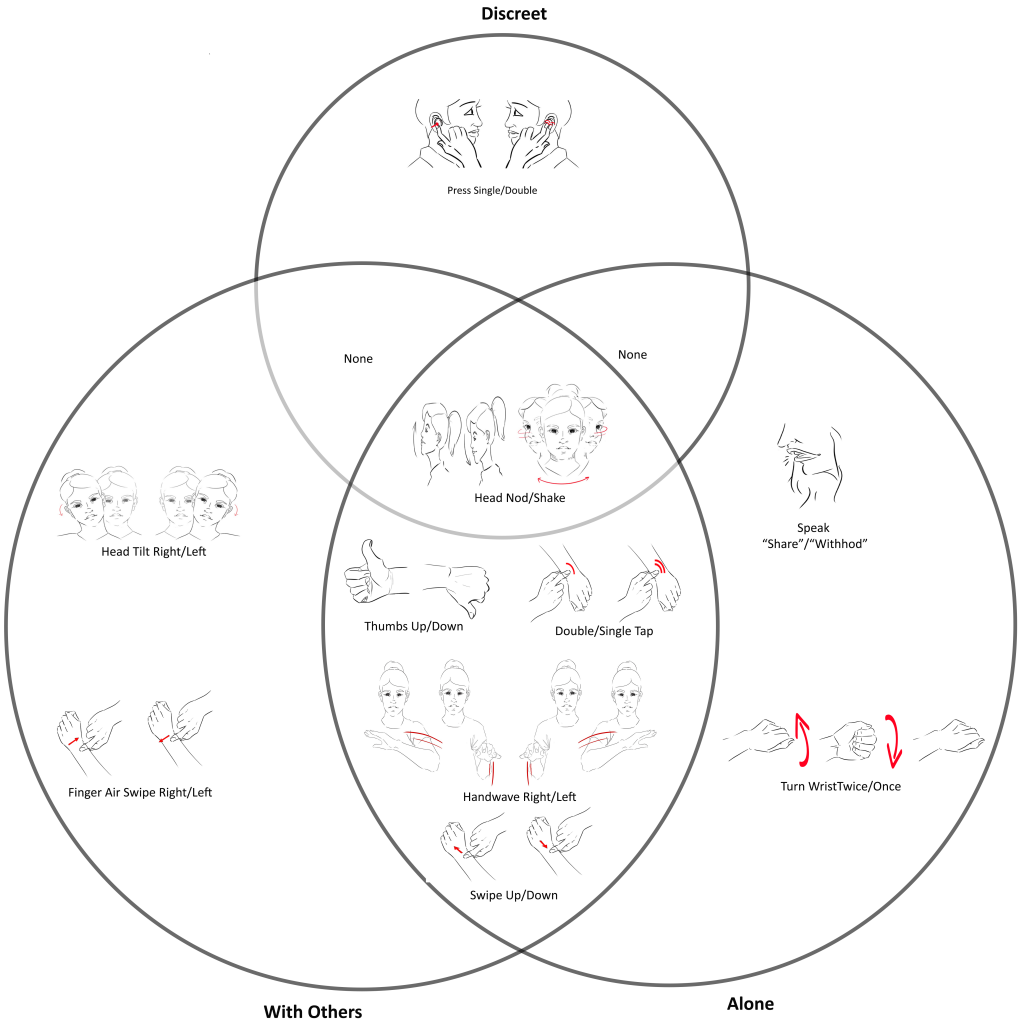


Figure 5.5. The user-defined set of interactions across social context. The leftmost interaction in the symmetrical pair satisfies the referent *share*, and the rightmost interaction of the pair satisfies the referent *withhold*.

as an interaction with a wearable by observers. For example, one participant proposed to cough in their hand, while another proposed to hold their hand by the leg and clench their fist, followed by tapping their leg twice.

While prior work has begun to explore subtle interactions that are based on implicit movements that are generally considered socially acceptable or unnoticeable [25, 36, 76, 295], it is important to further explore what types of subtle interactions are discoverable, memorable, and easy to learn [228, 361]. To support Mark Weiser's vision for Ubiquitous computing – in which technology is embedded into the background to enhance interaction [352] – it is vital for designers to build interfaces that enable users to communicate privately with a device even in the presence of others [25, 288].

We identified two sets of interactions that are uniquely suited for instances when a user wants to communicate discreetly with a wearable device. Those interactions are: *head nod* (share) and its symmetrical match *head shake* (withhold) and *double press* (share) and its symmetrical match *single press* (withhold). As shown in table 5.3, we see the *head shake* and *single press* interaction had the highest agreement metrics among participants. We also see that these two interactions had a symmetric match (e.g., head nod and double press). Based on these criteria, we chose these interactions as suitable for when people need to interact without their wearable without being noticed. Notably, within the discreet condition, we were not able to identify an interaction for the referent *share* that satisfied the agreement metrics. However, there was a very low consensus for the withhold referent for both *head shake* and *single tap*, so we used the symmetrical match for these interactions.

5.4.2.2 Little Consensus in the Discreet Condition

In the discreet condition, for the referent *withhold*, one interaction – *single press* – achieved medium consensus. However, for the referent *share*, in the discreet condition, participants all proposed different interactions. Therefore, we did not find any interactions with even a medium max-consensus. Not surprisingly, the consensus distinct ratio was high. The high consensus distinct ratio shows that there is diversity among the interactions proposed. The diversity among interactions generated in the discreet condition could be because people do not have a commonly agreed-upon vocabulary of interactions to use in situations requiring discretion, in part because these are, by definition, performed in private and therefore not observed. Alternatively, this result could demon-

strate freedom from social pressure in private situations. People may not feel pressured to use socially acceptable interactions. The pressure to use socially acceptable interactions may constrain the space of possible interactions performed in front of others. People may feel free to use a larger, more diverse set of interactions with no such constraint.

One obvious takeaway from this result is that discreet interactions should be based on movements that do not disrupt individuals in the immediate environment [75]. Furthermore, these types of interactions should be - at minimum - socially acceptable [58], or even undetectable or invisible [58, 75, 204, 287] in social contexts where privacy is a concern. If an observer sees a wearer performing an obvious interaction (e.g., thumbs up), they may realize that they are interacting with a wearable when the wearer wishes to remain discreet.

If interactions are designed to be private, they should not be seen or observed by bystanders. If the interaction is unnoticeable to bystanders, the bystander will not learn when a wearer is interacting with a wearable.

5.4.2.3 Symmetrical Interactions

We discovered that several of the interactions that met our first two criteria, frequency and max-consensus, have a symmetrical match for opposite commands. For example, *head nod* met both the high frequency and max-consensus criteria and has *head shake* as a symmetrical match.

An important factor in the success of interaction sets is whether the interactions can be easily learned and remembered [200, 238]. Symmetry in interactions increases learnability [32, 166]

5.4.2.4 Hardware and Software

We designed our study to be device agnostic. That means our results can inform user interactions that can be implemented on existing wearables and new wearables that have yet to be invented. For example, ubicomp researchers are already designing wearables that could, in the near future, be in the form factor of earrings that track heart rate [126], a wearable earpiece that detects eating behavior [43], clothing that monitors physiology [223, 251], shoes that track walking patterns, [375], contact lenses that monitor physiological information within the eye to provide non-invasive medical diagnostics [253, 374], and telemetry devices that can be implanted, ingested or injected [62, 90, 138, 192, 203]. Because we used a device-agnostic approach, the results from our study can inform the development of new software and hardware to enable user interaction for each of these

emerging form factors.

Many of the interactions we identified can be sensed with hardware already available on existing commodity devices. For example, some head-mounted devices and wrist-worn devices can sense presses. Other head-mounted devices can detect taps using microphone sensors [371]. Microphone sensors in commodity wearables (e.g., Apple Watch, Samsung Galaxy, Apple Air Pods, Samsung Galaxy Buds) also allow voice-based interactions using hot-words such as, "Hey Siri". Other wearables can detect taps (e.g., Air Pods) and a limited range of mid-air gestures using integrated motion sensors (e.g., accelerometer and gyroscopes) [48]. For example, Wen et al. demonstrated the feasibility of using motion sensors on the Samsung Galaxy Gear to detect fine-grained gestures like a hand wave. While most commodity head-mounted devices have integrated motion sensors, very few have software processing capabilities to detect head-based interactions. We only know of one, the Tic Pods Pro 2 that uses integrated motion sensors for head nod and head shake interactions. Because these sensors are able to sense the range of motion of a user to identify direction, speed, and orientation of the movement [13, 230, 366] and are cost-effective in terms of energy consumption and dollars, they should be able to sense many of the interactions we identify (e.g., thumbs up, thumbs down, head nod, head shake). A notable implication of our findings are that a subset of the interactions for privacy control we identify may be implemented on existing commodity wearables without hardware changes.

On the other hand, many of the interactions we identified will require hardware that is not currently in most commodity wearables. For example, few commodity wearables contain emerging miniature radar sensors [195] that perform non-vision- based sensing such as electronic field sensing and radio frequency sensing to detect mid-air interactions like finger air swipe right and left. While these types of sensors are not widely available, a demo from the 2016 Google I/O conference [189] showed how the miniature radar sensor could be used to detect air gestures in a Wear OS smartwatch to control the interface. Gong et al. [128] also demonstrated how implementing an array of proximity sensors on a wrist-worn device can be used for interactions that require full wrist motion like the *turn wrist once* interaction from our recommended set. Gong and colleagues also explored the use of a skin-contact piezo sensor. This type of sensor was used as a dedicated delimeter sensor to detect the start and end of interaction (e.g., finger pinch). The addition of the piezo sensor also led to significant power conservation, as it allowed the motion sensors only to be turned on when the finger pinch was detected. This approach could prove promising to detect interactions we identify in this

chapter.

5.4.2.5 Sensor Placement

All of the interactions included in our recommended set, except three pairs (i.e., *head nod/shake*, *head tilt left/right*, and *speaking*), involved the users' hands. This indicates that there is a rich interaction space for wrist-worn devices to implement privacy controls. Tapping a device is already available as interaction on many wrist-worn devices (e.g., Apple Watch). On the other hand, emerging wearable sensors that utilize contact-based inductive sensing (e.g., Tessutivo [127]) and piezo-electric sensors [24, 128] could be used to improve detection of tap interactions on new wearables that extend the input space on wrist-worn devices beyond the device itself (e.g., to the skin surrounding the wrist [302]). For wearables that are not already located on the wrist or near the hands, designers should consider adding sensors that are able to detect hand-based interactions through the use of classification algorithms no matter the location of the wearable with respect to the body. Such approaches have shown initial success through a real-time system that leverages the microphone in commodity wireless earbuds to detect tapping and sliding gestures near the face and ears [371]. Harrison et al. [20] developed a novel interactive on-body system using a ceiling-mounted infrared camera that can track a myriad of arm and hand gestures. Cooaco et al. also introduced a low-power 3D sensor for short-range gestural control of a head-mounted device through the use of the hand. These sensors provide low-power time of flight sensing for 3D hand-motion tracking using an RGB image-based vision computer algorithm [67].

Many interactions we identified also involve the head. For these interactions, designers should consider including inertial sensors (e.g., accelerometers) and nine-axis attitude sensors [30] that detect interactions such as a *head nod* or a *head tilt*, as well as sensors (e.g., piezo-electric) that can detect near- or on-head touch-based interactions. Furthermore, similar to our recommendation about sensing hand-based interaction no matter the location of the wearable, designers should consider including sensors that are able to detect head-based interactions no matter the location of the sensor on the body (similar to the notion of body-are networks) [151].

Finally, one pair of interactions we identified involved sound. In contrast, voice-based interfaces are common on some home-based devices (e.g., Amazon Echo, Google Home, and Apple Home), smartphones, and some wrist-worn devices. There are not many wearable devices that support voice-based interactions. Our results suggest that designers should consider adding voice-based

user interface capabilities to wearable devices so users can use their voice to manage privacy on wearables.

5.4.2.6 The Power of Integrated and In-the-Moment Binary Privacy Controls

Now that we have discovered a set of interactions that have the potential to allow people to express complex, nuanced privacy decisions on wearable devices, with limited space for user interfaces is an important development for privacy in ubiquitous computing. Privacy concerns in ubiquitous computing go back to the dawn of the field, with Weiser, noting that privacy was one of the key issues yet to be solved in his vision of the future [351].

The simplicity of Integrated and In-the-Moment binary privacy controls has important implications for many other ubiquitous computing systems where privacy control remains challenging to implement effectively. For example, the approach we introduce in this chapter could be applied to smartphones. Smartphones could occasionally check in with users to see whether they wanted to share location data with all the apps and services that were currently collecting it. Machine learning, or human-centered approaches, could use data generated from these check-ups to learn about what kinds of data people wanted to share with which recipients under what conditions, all with users only being asked to provide binary responses.

5.5 Limitation and Future Work

One difference between our study and many other gesture elicitation studies is the narrow referent set (*share* and *withhold*). In most prior elicitation studies, a set of referents about an available system is provided to participants. The majority of these studies follow Wobbrock et al.'s [360] protocol where participants are presented with multiple referents (actions or tasks) that represent basic functions (e.g., for a TV turn on/off, next/previous channel, volume up/down/mute), or generic functions (e.g., select single choice, select multiple-choice, select a date). Participants are then asked to suggest a gesture to execute that specific task. In a recent systematic review of 216 gesture elicitation studies [340], authors note the average number of referents from these studies was 20, with a wide variance (SD=5.23). The large variance indicates that the number of referents varies from few (N=1) [278] to many (N=70) [364].

Unlike most published work on gesture elicitation, we prioritized the context of the potential

interaction because context is essential for privacy. Therefore, we let participants choose the referent (share/withhold) based on the context provided by the independent variable (e.g., health care provider, family, and friends, etc.). Because we chose to prioritize context over the execution of an action or task for a primary function, we did not follow the most frequently reported metric "level of agreement" [361]. Instead, we considered several metrics (e.g., max-consensus, individual frequency of interaction, and interactions with a symmetrical match) to identify a user-defined consensus set. It's possible that the small referent set may limit our interaction set. We could hypothesize that increasing the number and variety of referents beyond just share/withhold could produce different interactions. However, this initial study was only concerned with examining interactions for binary sharing preferences, allowing us to propose a consensus set of usable and private user-defined interactions to express Integrated and In-the-Moment preferences. This study could serve for further experiments that look at more explicit contexts. We could also explore how participants would respond to a notification informing them that some data is being collected and how they would handle this accordingly.

Another notable difference in our work in contrast to many elicitation studies is that we did not elicit a subjective assessment of the proposed interactions. As a result, some of the interactions from our set may not be a users' favorite or the most suitable [61]. We did not elicit a subjective assessment of the interactions participants proposed because of the narrow referent set. In some cases, participants suggested the same interaction for the referent *share* and the same for the referent *withhold*. We believe it would not have been methodologically sound to have participants rate their interaction if this was the case. In future work, it may be useful to conduct a follow-up choice-based elicitation study [60, 93] and show a separate group of participants the interactions from our recommended user-defined set and require them to subjectively evaluate each interaction based on the referent *share* or *withhold*. This process would allow us to narrow down our referent set using an additional metric.

Lastly, participant selection in elicitation exercises is a concern that should also be considered [213]. The results from all elicitation studies are dependent on the participants in the study. Whether the results generalize to other domains, groups of people, or cultures remains open. For example, we see that most of the interactions that participants proposed are emblematic in nature (See Table 5.2). Would these emblematic interactions be recognized across other cultures? While this is worth exploring, we did not have the resources to travel around the country to examine gesture preferences

among more diverse cultures. Furthermore, the participants in our study mainly consisted of younger people living in the U.S. who have intermediate technology experience and who own or previously owned a wearable device. This was by design since these are the most likely users of wearable technologies [368], and thus those who may most immediately require Integrated and In-the-Moment privacy control. While the results may not fully generalize to larger populations of potential adopters of wearable technologies [368], our data does reflect the experiences of the general U.S. population of individuals who own wearables [214]. Nevertheless, we hope additional studies will be conducted to generalize our results from a cross-cultural aspect further.

Given the diversity of wearable technologies, this interaction elicitation study only scratches the surface of the opportunities to provide individuals with control over personal information from a wearable. However, our methods and results can be tailored to inform various interactions that allow users to express privacy decisions Integrated and In-the-Moment.

5.6 Conclusion

Using an interaction elicitation study with a group of 32-participants who produced 460 mid-air, micro, sound-based, multimodal, and composite interactions, we identified a set of user-defined, device-independent interactions for privacy control on wearables. We found differences in the types of interactions people produced for situations requiring discretion vs. those that require less discretion, such as when people are alone. This set of interactions may be helpful to researchers who wish to study privacy preferences on wearables and developers wanting to build interfaces that enable Integrated and In-the-Moment privacy control on wearables.

Chapter 6

Study 4: Invisible Input for Invisible Devices

6.1 Introduction

One of the most salient aspects of IoT Devices like wearables is their invisibility. As noted in Chapter 5, there is a need for discreet interactions for wearables. As Marc Weiser pointed out in his earlier work, these technologies are not invisible to the eye but hidden in terms of context and use [350]. As these technologies continue to proliferate, there is an ongoing need to enhance the human experience with wearables by developing new modes of interaction. New methods of interaction that are not only seamless but invisible where users can provide input and receive output more subtly or invisibly without being observed or disrupting others nearby [25].

While we were able to develop a user-defined set of interactions for privacy control on wearables in Chapter 5, we sought to further explore the noticeability of some of the interactions we collected from this study to develop a set of interactions that could be used in situations where a user desires to be discreet while in the presence of others. This study explores a set of user-defined interactions that could be adopted for use on wearables that allow a wearer to provide input to a wearable without being observed or disrupting social interaction when around others [25, 261]. We consider real-life scenarios in which a user may need to be discrete in their interaction with a wearable and explore which input mechanisms allow a user to do so. If an individual is in public,

either with friends at dinner or in a meeting at work, and wants to interact with their device in a way that is hidden or unobservable from the perspective of others [272] - how could they do that? Indeed, speaking to the device would draw attention to themselves, just as taking time to physically input the information to the device directly would draw their attention away. What if the wearer could provide input to their wearable without letting their interaction interrupt others around them? This is the problem we face, and we attempt to address it by evaluating various gestures on their discreteness. A subtle approach to user interaction ensures more privacy and discretion to users [231].

Subtle interactions for wearable technologies have historically focused on actions that require reduced cognitive loads for users so the interaction with the device can be completed without observers noticing them [25]. For example, Jing et al. introduced a finger ring-shaped input device to detect subtle interactions [160] using inertial sensors as a hands-free input method. However, this study focused on technical evaluations of interactions with an input device. Motionless gestures sensed through electromyographic (EMG) signals have also been shown to allow subtle or discreet input to a wearable device when fastened on the upper arm, in a mobile context [77]. In this study, observers watched a video recording of these gestures and found it challenging to identify if an input to the wearable device took place [77]. This study also evaluated the usability of these gestures. Despite the promising results of this work, the results are limited because they involve assessing the usability and subtlety of interactions or gestures that were not sourced from users. In addition, these interactions consisted of only those that are detectable by EMG signals. Researchers should consider how this method can be levered for use on any wearable technology regardless of its form factor.

Principles of magic have also been adopted to improve the subtlety of interactions with devices and have succeeded in creating interactions that remain discreet or inconspicuous to an observers' eyes [25]. While the results of this work seem promising, this work also suffers from the limitation of neglecting human factors as a source of interaction, and researchers only factored in humans as a tool to evaluate subtlety and leveraged magic as means to design illusory and discreet interactions.

One study that used a participatory design approach to collect subtle interactions was Kim et al.'s study on M. Gesture. In this study, researchers ran an elicitation study based on a formative study that looked to understand how users perceived and define interactions with mobile devices.

Results from the elicitation study show that most of the gestures collected were subtle; however, researchers did not further explore their gesture set with additional participants to determine the subtlety of the proposed interactions.

While prior works have explored subtle interactions that are based on movements that are not consciously recognized and are generally considered socially acceptable or unnoticeable [25, 76, 295], it is critical that members of the HCI community further explore what types of subtle interactions would be appropriate for emerging technologies like wearables. Many wearable technologies require interaction between the user and the device[101]. Drawing from this school of thought, we choose to evaluate the subtlety of a pool of inputs interactions from Chapter 5.

The goal of this study is to extract some of the interactions that were elicited in Chapter 5 and evaluate how noticeable/unobservable these interactions are based on evaluation from another set of participants. To accomplish this goal, we conducted a study where we recruited a group of participants from Amazon Mechanical Turk to evaluate if the interaction they saw in a video was indeed an action and if that action was deemed as interaction with some technology. In this study, We seek to answer the following RQs.

Given a set of user-defined interactions:

- Which interactions proposed under a discreet social context are perceived as: an action, an interaction with some technology, invisible to the naked eye, and deemed as subtle when viewed by a second group of participants?

Building from existing privacy literature, research on wearable devices and mobile communication needs, this work makes the following contributions.

- An evaluation of the subtlety of a set of user-defined interactions that could be used with any wearable device.
- A set of interactions that are subtle enough that could be used by any wearable device
- A set of interactions that would be appropriate for use with invisible wearable devices.

In the next section, we discuss the methods used to answer our proposed RQs.

6.2 Methods

The objective of this experiment was to determine the noticeability of interactions and degree of subtlety based on a video of an actor performing the interactions we gathered during from

the study in Chapter 5. The meet our objective, we evaluated the observability of 49 of the 129 interactions we collected in the study from chapter 5, in addition to one interaction where the actor is not doing anything (which is used as control)which resulted in a total of N=50 interactions.

To extract a subset of interactions from the 129 collected in chapter 5, two researchers evaluated the list of interactions based on social context (e.g., alone, while in the presence of others, with others while private), as well as areas of the body used to perform the interactions and classified the interactions based on personal judgments of similarity for each social context. After this evaluation, the researchers selected a final list of sufficiently different interactions for each social context, which resulted in 36 interactions from the "in the presence of others while private" social context, 11 interactions from the "in the presence of others" social context, and one interaction from the "alone" social context. All of the interactions include at least two or more interactions from the following areas of the body: *head, torso, arms, fingers, leg, and foot.*

After formulating this list of interactions, the primary investigator and an independent rater categorized each interaction as either subtle or obvious and had two additional raters review all the interactions and provide a binary rating for each interaction as subtle or obvious to establish inter-rater reliability. This resulted in interactions across three categories: 15 obvious interactions, 34 subtle interactions, and one no interaction at all (See Table 6.1).

To evaluate the interactions in terms of their subtlety, we conducted a study on Amazon's Mechanical Turk(MTurk), where we had participants attempt to identify if an action in the video took place and if that action was an interaction with some form of technology from several video clips. The content of each video clip belonged to one of three broad categories, namely, 'Video Clips With Subtle Interactions', 'Video Clips with Obvious', and 'Video Clips with No Interactions at all.' Each participant viewed 5 randomized blocks of interactions. Using the qualtrics randomization feature, interactions were randomly sorted in different orders within each block, where in four of the blocks participants saw seven subtle interactions, 3 obvious interactions, two interactions where participants did not move (which we classify as control), and two attention check videos that displayed as a glitch to ensure participants were paying attention. In the remaining block, participants were shown six subtle interactions, three obvious and the same control and glitch videos as mentioned previously. Each block of interactions were counterbalanced across five groups of 15 participants.

The entire study was IRB approved. Additionally, informed consent was obtained at the beginning of the each study and the pilot.

Interaction	Category
Adjust Sleeve	Subtle
Arm Rub	Subtle
Blink Eye	Subtle
Chest Pound	Subtle
Circular Head Nod	Subtle
Cough	Subtle
Cover Mouth	Subtle
Cross Leg	Subtle
Ear Tug	Subtle
Eyebrow Swipe	Subtle
Finger Cascade	Subtle
Finger Wave	Subtle
Foot Scratch	Subtle
Foot Tap	Subtle
Hand behind back	Subtle
Hand in pocket	Subtle
Hand Squeeze	Subtle
Head Nod	Subtle
Head Tilt	Subtle
Leg Pat	Subtle
LegRub	Subtle
Money Gesture	Subtle
Neck Roll	Subtle
Nose Tap	Subtle
Rub Behind Ear	Subtle
Single Head Nod	Subtle
Single Shoulder Shrug	Subtle
Speak	Subtle
Strech	Subtle
Swipe Across Body	Subtle
Teeth Click	Subtle
Thigh Scratch	Subtle
Touch Behind Ear	Subtle
Turn Wrist Down	Subtle
Double Tap Ear	Obvious
Double Tap Wrist	Obvious
Finger Pinch	Obvious
Fist Swipe	Obvious
Grab wrist, make fist, twist hand	Obvious
Hand Side Knock	Obvious
Hand Swipe Forward Twice	Obvious
Knock	Obvious
Two Finger Palm Tap by Leg	Obvious
ShakeWrist	Obvious
Finger Swipe Forward	Obvious
Swipe on wrist	Obvious
Temple Swipe Backward	Obvious
Wrist Twist	Obvious
Ziplips	Obvious
Control	No Interaction at all

Table 6.1. Researcher Classification of Interactions

6.2.1 Pilot Testing

We conducted two rounds of pilot testing to validate, refine and assess the reliability of our survey instrument. The first round of piloting was with 25 participants (13 males, 11 females, 1 undisclosed) aged between 25 and 55. Using a between-subjects design, five groups of participants were randomly assigned to one of five groups of videos of an actor performing interactions. Four groups of interactions consisted of seven videos of subtle interactions, three videos of obvious interactions, and two videos where the actor did not move, which we classify as control. Additionally,

two attention check videos displayed as a glitch to ensure participants were paying attention. The last group of interactions consisted of videos of six subtle interactions, three obvious interactions, two control, and two glitch videos. After reviewing the video, participants were asked to indicate if there was an issue with the video, and if so, to describe the issue; provide a binary response of 'yes' or 'no' to if the person in the video took any action and rate their confidence of the response on a 7-point Likert scale (completely unconfident - completely confident); provide a binary response of 'yes' or 'no' to if the person in the video interacted with any technology/devices and rate their confidence of that response on a 7-point Likert scale (completely unconfident - completely confident). For interactions where participants indicated there was an interaction with technology, they were asked to indicate which part of the body was used to perform the interaction based on an image of a body map and provide an open response to describe what they observed and what kind of technology the person in the video was interacting with. It took each participant 30 minutes on average to complete the pilot, and they were paid $5.00 for participation. Based on the results from this pilot were able to reclassify interactions into categories such as *very subtle, subtle, obvious, and very obvious* based on these results (See Table 6.2).

We looked at what percentage of participants considered a particular interaction as interaction with technology and their confidence score to classify interactions. To classify very subtle interactions, we looked to those where none of the participants indicated these as interactions with technology. They were very confident in their response (M =6.44, SD =0.53). Interactions classified as subtle were those where only 20% of participants indicated an interaction occurred with technology. Interactions classified as *obvious* were those where 40% of participants indicated an interaction with technology took place, and interactions classified as *very obvious* were those where 50% or more of participants indicated an interaction with technology occurred.

We find differences in the interactions we classified as subtle/obvious compared to the interactions that were reclassified as subtle/obvious in participant evaluation (See Table 6.2. For example, 10 of the interactions we initially classified as subtle were reclassified as obvious or very obvious based on participant evaluations, while 7 of the interactions were originally classified as subtle or very subtle.

The next round of piloting was with 13 participants (8 Females, 5 Males) aged between 25 and 55 years old. In this pilot, we employed a within-subjects design where each participant was shown all interactions. Instead of asking participants to provide a binary response of 'yes' or

Interactions	Category
Double Tap Ear**	Subtle
Ear Tug	Subtle
Finger Cascade	Subtle
Finger Pinch**	Subtle
Foot Scratch	Subtle
Foot Tap	Subtle
Hand Squeeze	Subtle
Leg Pat	Subtle
Leg Rub	Subtle
Nose Tap	Subtle
Single Shoulder Shrug	Subtle
Swipe Across Body	Subtle
Swipe on wrist**	Subtle
Temple Swipe Backward**	Subtle
Thigh Scratch	Subtle
Touch Behind Ear	Subtle
Turn Wrist Down	Subtle
Arm Rub	Very Subtle
Blink	Very Subtle
Circular Head Nod	Very Subtle
Cough	Very Subtle
Cover Mouth	Very Subtle
Cross Leg	Very Subtle
Fist Swipe**	Very Subtle
Money Gesture	Very Subtle
Neck Roll	Very Subtle
Shake Wrist**	Very Subtle
Single Head Nod	Very Subtle
Stretch	Very Subtle
teeth click	Very Subtle
Zip Lips**	Very Subtle
Adjust Sleeve *	Obvious
Chest Pound*	Obvious
Eyebrow Swipe*	Obvious
Finger Wave *	Obvious
Hand Behind Back*	Obvious
Hand In Pocket*	Obvious
Hand Side Knock	Obvious
Hand Swipe Forward	Obvious
Head Nod*	Obvious
Head Tilt*	Obvious
Two Finger Palm Tap by Leg	Obvious
Double Wrist Tap	Very Obvious
Grab wrist, make fist, twist hand	Very Obvious
Knock	Very Obvious
Rub Behind Ear*	Very Obvious
Speak	Very Obvious
Finger Swipe Forward	Very Obvious
Wrist Twist	Very Obvious
No Action	Control

Table 6.2. Reclassification of Interactions From Pilot Testing. Note: Interactions with a * were originally classified as subte. Interactions with a ** were originally classified as obvious

'no' to if the person in the video took any action, and if the person in the video interacted with technology and/or devices, we asked them to provide their response based on a 7-point Likert scale from 1-Strongly agree-7 Strongly Disagree. Following the perceived action and perceived interaction questions, participants were still asked to rate the confidence of their response on a 7-point Likert scale (completely unconfident - completely confident). For the perceived interaction with technology question, if participants answered on the higher-end of the scale (5-7) they were asked follow-up questions at the end of the experiment to indicate which part of the body was used to perform the

interaction based on an image of a body map and provide an open response to describe what they observed and what kind of technology was used. It took participants approximately 90 minutes on average to complete the pilot, and we compensated them $15.00 for their participation. At the end of the experiment, we also asked participants two questions about the fairness of the compensation and their experience completing the experiment.

We excluded data from two participants as we suspected bots based on the results. This resulted in a total of 11 participants. We used the data from the pilot to determine the number of participants we would need for the full study and how much we would compensate participants for their participation in the study.

6.2.2 Participants

6.2.2.1 Sample Size

To determine the number of participants needed for the experiment, we conducted a power analysis based on data from the pilot. The power analysis revealed that we would need 56 participants to find an effect at the 0.85 power level.[194]

We used the same recruitment strategy as we did in the pilot by recruiting participants via MTurk. To ensure the data quality, we set restrictions to only include MTurk workers with a high reputation (above 95% approval ratings) and with the number of approved HITs approved greater than 1000 [264]. The HIT for the full experiment was advertised at a rate of $ 11.00 USD, and participation was voluntary.

To account for complete counterbalancing across all conditions, we recruited a final sample of 60 participants (37 Females, 23 Male). Seven percent ranged in age from 18 to 24; forty-two percent ranged from 25 to 34; twenty-five percent ranged from 35 to 44; eighteen percent ranged from 45 to 54; eight percent were 55+. Thirty-seven percent of participants reported having intermediate knowledge of technology, while forty-two percent reported having advanced technical expertise. Surprisingly, eighty-three percent of participants reported owning a wearable device.

	N = 296
Gender	
Male	23 (38%)
Female	37(62%)
Age	
18-24	4 (7%)
25-34	25(42%)
35-44	15 (25%)
45-54	11 (18%)
55+	5 (8%)
Education	
High incomplete or less	2 (3%)
High school grad	6 (10%)
Some College	17 (28%)
Four Year College	26 (43%)
Some postgraduate	2 (3%)
Postgrad or Professional	7 (12%)
Ethnicity	
White	39 (65%)
African American	12 (20%)
Asian	5 (8%)
Native Hawaiian or Pacific Islander	1 (2%)
Other	1 (2%)
Technology Knowledge	
Basic	6 (10%)
Intermediate	22 (37%)
Advanced	25 (42%)
Professional	7 (12%)
Wearable Device Ownership	
Own Wearable	50 (83%)
Did not own wearable	10 (53%)
Did not own wearable, but interested in using one	3 (30%)

Table 6.3. Participant Demographics

6.2.3 Experimental Design

6.2.3.1 Independent Variables

Because our study focused on evaluating the subtlety of interactions with a wearable device, the recorded video clips (N=50) of an actor performing an action formed the independent variable. The videos included 15 obvious interactions, 34 subtle interactions, and 1 video where the actor did not moved. We used the data from pilot testing to create classifications for each type of interaction performed in the video clips. Those interactions feel into four categories: 'Very Subtle (N=14)', 'Subtle (N=17)','Obvious (N=11)', 'Very Obvious (N=7)' and 'Control (N=1)'. The control was a video of an actor not doing anything. These categories formed the levels for the independent

variable.

6.2.4 Dependent Variables

To evaluate the perceived noticeability of and action and perceived interaction with technology of what participants saw in the video clips, we measured identification of an action on a 7-point Likert scale (1 Strongly Disagree to 7 Strongly Agree); confidence of the response on a 7-point Likert scale (1-Completely Unconfident to 7-Completely Confident); identification of an action with technology on a 7-point Likert scale (1-Strongly Disagree to 7-Strongly Agree) and confidence of that response on a 7-point Likert scale (1-Completely Unconfident to 7-Completely confident). These factors formulated the dependent variable in our study.

6.2.5 Procedure

The full experiment was identical to the second-round pilot testing, with a larger sample size. Participants accessed our experiment via a website hosted by Qualtrics via the link posted on MTurk. After providing informed consent, participants answered six demographic and one knowledge of technology question. In addition, we collected participants' views on privacy and surveillance in everyday life via a single-item questionnaire [206]. After completing the pre-survey, participants were redirected to a web page explaining the task that they had to perform for the study. They saw four training video clips, which were identical to the experimental trials, except, if they responded incorrectly, we provided additional information (e.g., please review the video and try again). Two of the training clips showed participants examples of actions, one clip demonstrated the actor not doing anything, which served as the control, and one showed participants to the glitch clip. Once the participants completed the training successfully, they could begin the task of identifying whether an interaction took place in each of the video clips they were shown.

Each participant viewed a total of 69 video clips across five blocks wherein four of the blocks they saw seven interactions that were either subtle and/or very subtle, three interactions that were obvious and/or very obvious, two interactions where the actor did not move, and two attention check videos that displayed as a glitch to ensure participants were paying attention. In the remaining blocks, participants saw six videos of either subtle and/or very subtle interactions, three obvious and/or very obvious interactions, and the same control and glitch video as mentioned

previously. To account for order effects, we used a standard 5 x 5 orthogonal Latin square for complete counterbalancing. There were a total of five counterbalanced batches, where we assigned 15 participants to the first two batches and 10 participants to the remaining three batches.

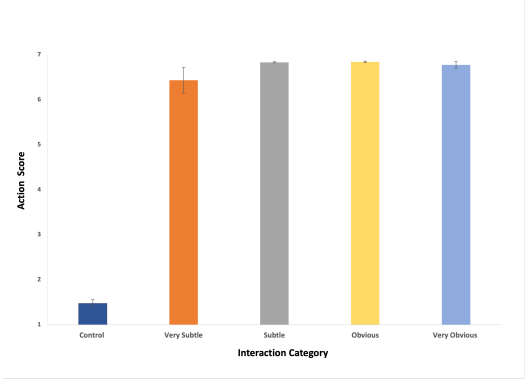
After viewing all 69 clips, participants were redirected to a block where they were shown videos where they indicated that the actor interacted with some form of interactive technology. For each video they were asked to identify which part of the body the interaction primarily involved, describe the interaction they observed, and indicate what type of interactive technology the person in the video interacted with. In the final block, participants were asked to complete two questions about compensation and their experience in completing the experiment. The first question ask them to rate the fairness of the tasks on a 7-point Likert scale (Strongly Disagree- Strongly agree) and provide a qualitative response based on their answer. Most participants believe that the compensation was fair for the amount of time spent completing the task.

6.3 Results

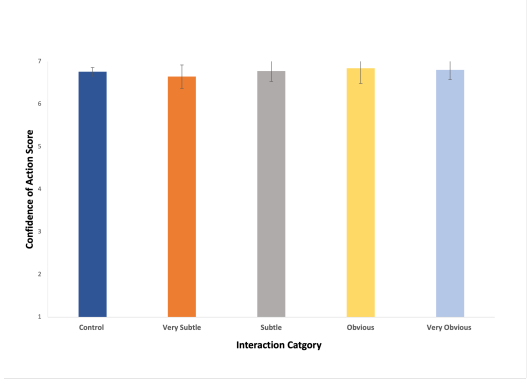
6.3.1 Overall means for action, confidence of action, interaction and confidence of interaction

Four measures were captured to analyze how noticeable/unobservable videos of an actor performing a set of input interactions collected from the experiment mentioned in Chapter 5: *if an action took place, the confidence of that response, if that action was an interaction with some wearable technology, and the confidence of that response.* Each participant provided their response to the questionnaire on a 7-point Likert scale. Figure 6.1 shows the mean action score and confidence of response, and Figure 6.2 shows the mean interaction score and confidence of that response for the five categories of interactions. For the *control* category when the actor did not do anything, we can see that the overall sample believed an action did not take place ($M= 1.48$, $SE = 0.08$) and participants were confident in their response ($M= 6.76$, $SE = 0.01$). For interactions classified as *very subtle* ($M= 6.43$, $SE = 0.28$), *subtle* ($M= 6.83$, $SE = 0.01$),*obvious* ($M= 6.84$, $SE = 0.01$), and *very obvious* ($M= 6.77$, $SE = 0.07$), we see that the sample of participants believe an action took place and were mostly confident in their response.

In terms of an interaction with technology, for the control condition (See Figure 6.2), par-

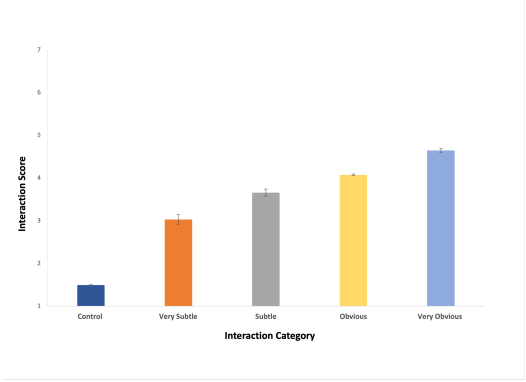


(a) Mean Action Score.

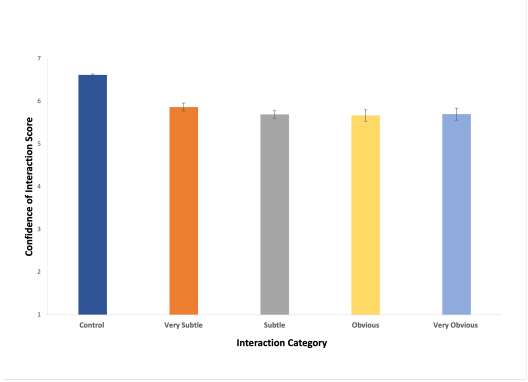


(b) Confidence of Action Response

Figure 6.1. Mean Action and Confidence of Response Across All Categories



(a) Mean Interaction Score.



(b) Confidence of Interaction Response

Figure 6.2. Mean Interaction and Confidence of Response Across All Categories

ticipants did not believe an interaction with technology took place (*M= 1.49, SE = 0.10*), and were mostly confident in their response (*M= 6.62, SE = 0.02*). For interactions we categorized as *very subtle*, we can see that the overall sample of participants did not believe what they saw in the video clip was an interaction with technology (*M= 3.03, SE =0.27*), and were very confident in their response (*M= 5.87, SE = 0.09*). For the interactions we classified as *subtle* participants were not very sure if an interaction with technology took place a (*M= 3.66, SE = 0.24*) and were moderately confident in their response (*M= 5.69, SE = 0.08*). The result was nearly the same for the interactions we classified as obvious (*M= 4.08, SE = 0.36*) and the confidence rating was fairly high (*M= 5.67, SE = 0.13*). For interactions we classified as *very obvious* participants were mostly sure an interaction with technology took place (*M= 4.65, SE = 0.22*) and were confident in their

response (*M= 5.70, SE = 0.13*)

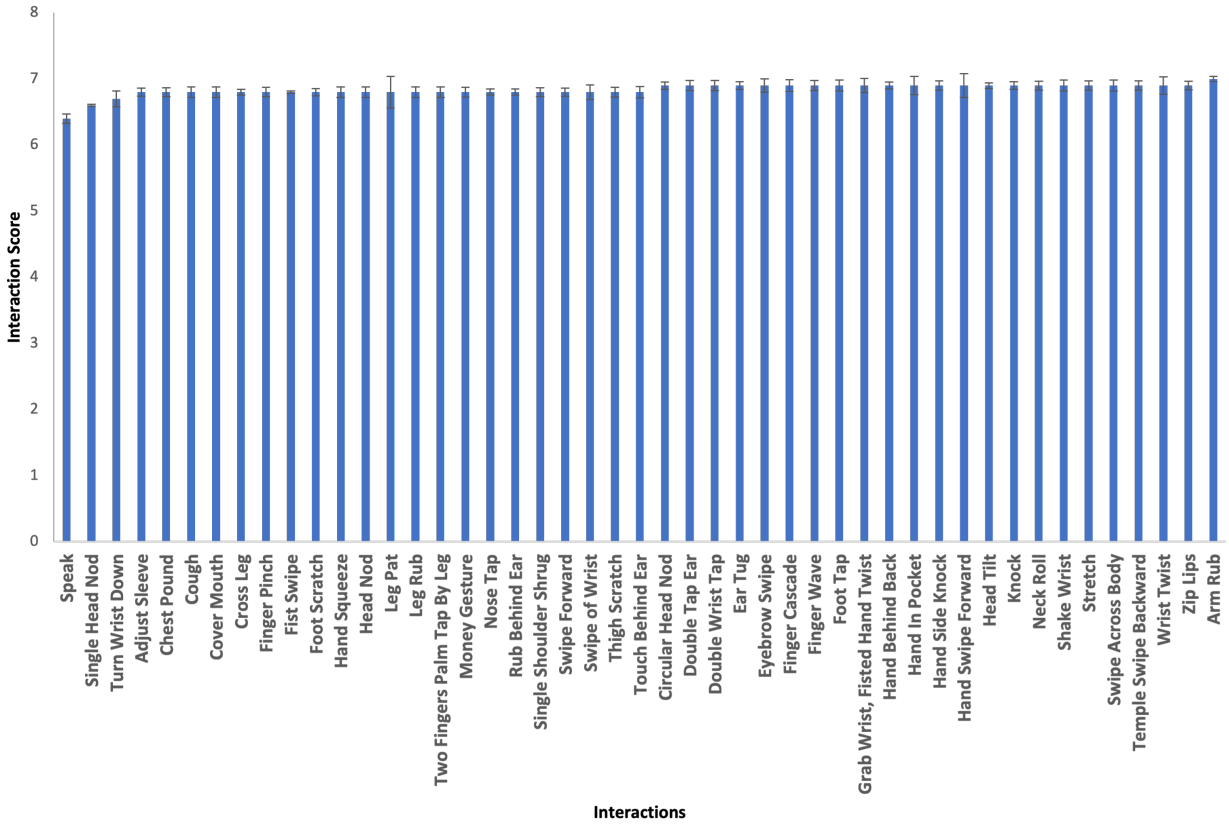


Figure 6.3. Interactions Perceived As Actions and Corresponding Interaction Score

6.3.2 Interactions perceived as an action

Figure 6.3 shows all the interactions that participants perceived as an action. Of the 50 interactions participants viewed, they considered 47 of those interactions to be an action, with an action score greater than or equal to five and the confidence greater than or equal to five. For the interactions participants considered to be actions the overall mean is (*M= 6.70, SE = 0.08*) and the confidence of that response is (*M= 6.75, SE = 0.08*).

6.3.3 Interactions perceived as Subtle

Figure 6.4 shows the interactions that participants perceived as subtle. Of the 50 videos participants viewed, there were 27 that had an interaction score below four. The overall mean interaction score for the interactions perceived as subtle, (*M= 2.98, SE = 0.25*) and the confidence of that response is (*M= 5.73, SE = 0.18*)

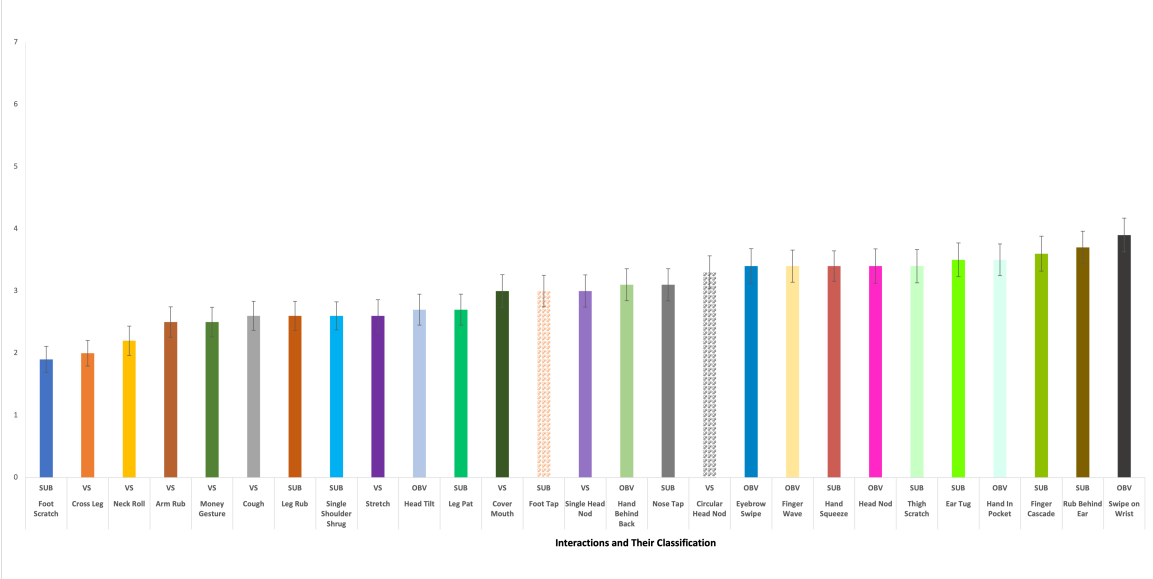


Figure 6.4. Interactions Perceived as Subtle and corresponding interaction score

6.3.4 Interactions Perceived As Interactions With Technology

Figure 6.5 shows all the interactions that participants perceived as an interaction with some technology. Of the 50 interactions participants viewed, they considered 10 of the video clips to be interactions with technology, with an interaction score greater than or equal to five and the confidence greater than or equal to five. For the interactions participants considered to be interactions the overall mean is (*M= 5.38, SE = 0.21*) and the confidence of that response is (*M= 5.95, SE = 0.15*)

6.3.5 Interactions perceived as invisible

All of the interactions in our set, teeth click is the only interaction perceived as invisible with a mean action score of (*M= 3.48, SE = 0.31*) and a mean confidence score of (*M= 5.96, SE = 0.20*). In terms of interaction with technology the mean interaction score was (*M= 2.3, SE =*

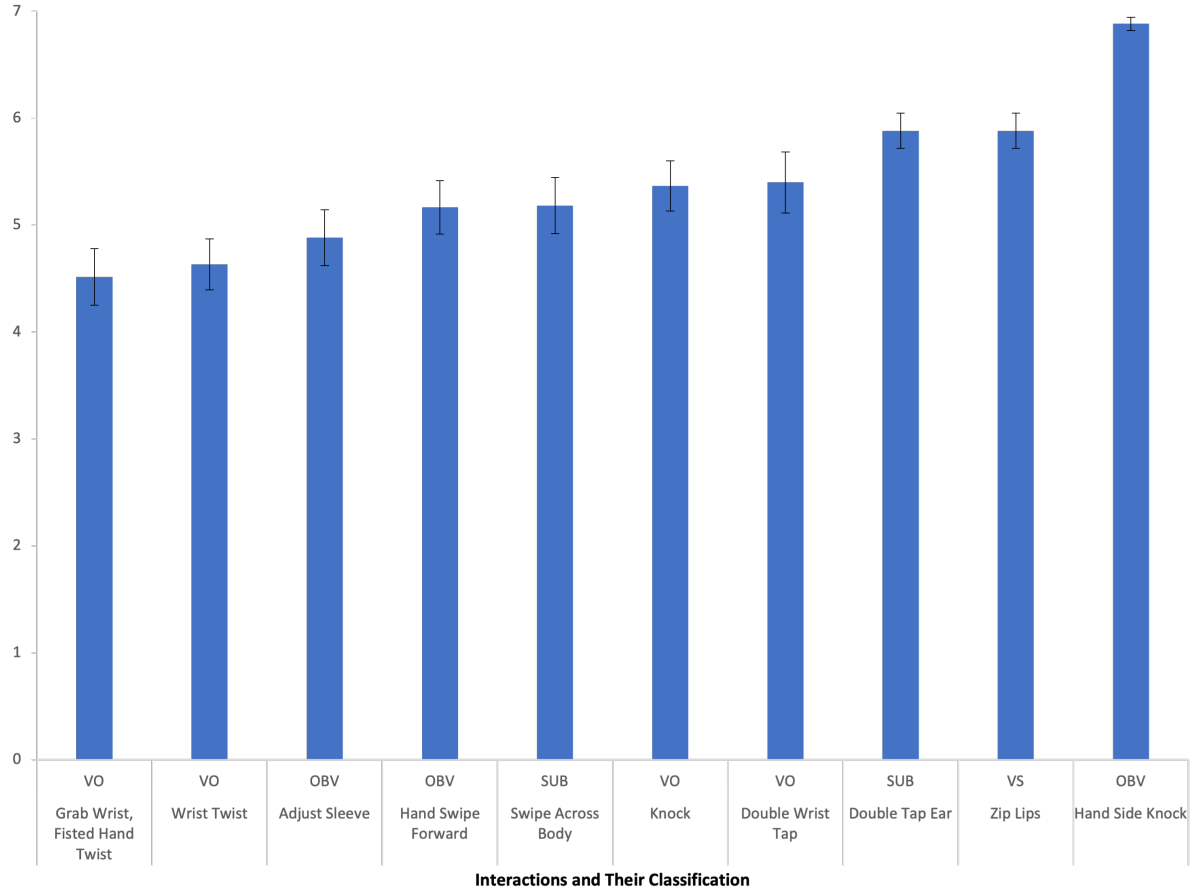


Figure 6.5. Perceived As Interactions With Technology

0.22) and a mean confidence score of (*M= 5.96, SE = 0.20*). Overall, participants were confident in their response (*M= 5.90, SE = 0.20*)

6.4 Discussion

Researchers and designers within the HCI community need to design and build interfaces that enable users to communicate privately with a device even while in the presence of others [25, 44, 272, 285, 288]. There may be situations where interaction with a wearable may not be socially acceptable, or a situation where there is a desire for privacy [44, 208, 272]. Hence subtle interactions allow users to continue to interact with their device under both circumstances [272]. As devices become more invisible, it is vital to consider novel methods that allow users to interact with them in a subtle or invisible way. While researchers within the HCI community have explored

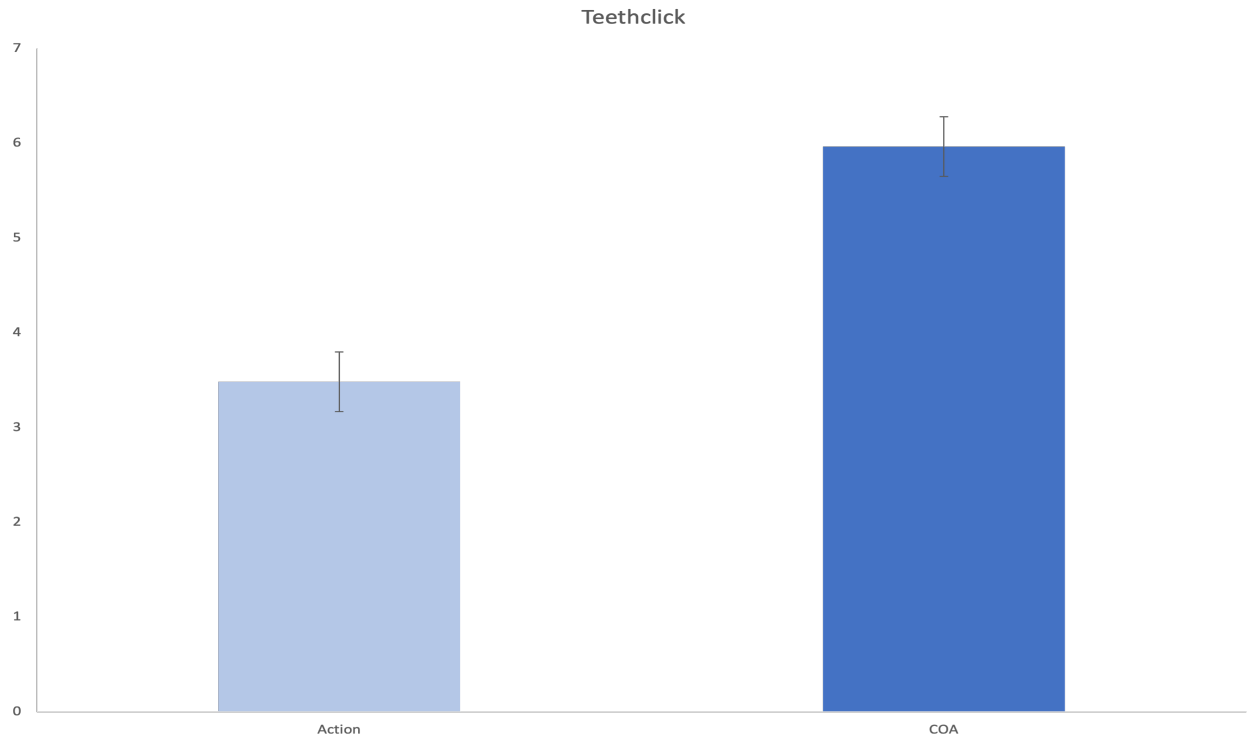


Figure 6.6. Interaction Perceived as Invisible

the concept of invisible interfaces [142, 153] and have also empirically explored ways for people with interact with devices where subtlety may be required[77, 142, 168, 247, 287], very few works that we know of have identified a set of interactions that could be used on wearables for discreet interaction.

In this chapter, we conducted a study where we evaluated a set of user-defined input interactions in terms of their subtlety while interacting with technology. We used an iterative approach to classify the interactions collected from the study in chapter 5. We first predefined categories utilizing a team of research experts but then expanded our evaluation of these categories using crowd-sourced participants. We did find some mismatch between what we identified as subtle or obvious in comparison to what participants viewed as subtle or obvious (See Table 6.2. This mismatch between user rating and participant rating supports the idea that designers may not share the same conceptual models as end-users [241]. Interestingly, when another set of participants further evaluated interactions in the full study, we find a slight mismatch between what was classified as obvious in comparison to what was classified as subtle in the final evaluation (See Table 6.4. The results suggest that careful empirical evaluations of interactions by participants are needed to determine

subtle interactions when interacting with wearables.

Based on our evaluations, we introduce 24 interactions that are subtle enough to allow a user to interact with their device without being noticed or disrupting others around them. The set of interactions we identify for subtle interactions is shown in Table 6.4. The set combines one completely invisible interaction (e.g., teeth click) and others that were subtle enough not to be noticed as interaction with technology. Table 6.4 also includes the original classification for each interaction. As the table shows, the majority of the interactions we identified as *subtle* or *very subtle* in our original classification based on results from the pilot also were identified as subtle There were six interactions we classified as obvious that were identified as subtle based on the full experiment.

While some of the interactions we identified as subtle could be used for emerging wearables technologies, it is essential to note that designers should consider sensors that can sense these types of interactions with any wearable interface. As of right now, there is no standardized way for building subtle interactions systems [272], but through more participatory design, we can see what types of interactions users prefer to use subtly. As noted in a systematic investigation into subtle interaction in the HCI literature [272], there need to be more empirical approaches for the subtlety of one's own interaction, as we did in this study. We see from prior works; there is also no lack of direct measure for subtlety. This is the first study we know of that has evaluated the subtlety of a set of interactions that users prefer in situations requiring subtlety. More work is needed to further explore this phenomenon by HCI researchers. There should be a collaborative effort with systems designers to see what hardware would be needed for these interactions to be deployed on wearables.

The results from this study could inform the development of new hardware for emerging wearables that allow for subtle interactions.

6.4.1 Limitations

There were several limitations from this study that we make note of in this section. The first limitation is that in the study from Chapter 5, we only elicited interactions for binary responses. In the majority of elicitation studies, researchers present participants with a set of referents about a known system and are asked to propose a gesture to execute that tasks [112, 293, 306, 309, 335, 337**?**]There could be other referents and context worth exploring to see what types of interactions users produce to interact with wearables discretely.

Another limitation worth noting is that the actor in the video did not have on a wearable

Interactions	Original Classification	Mean Interaction Score	Standard Error	Confidence of No Interaction	Standard Error
Arm Rub	Very Subtle	2.45	0.24	5.90	0.17
Circular Head Nod	Very Subtle	3.30	0.27	5.57	0.19
Cough	Very Subtle	2.55	0.23	5.75	0.18
Cover Mouth	Very Subtle	2.95	0.26	5.67	0.19
Cross Leg	Very Subtle	2.03	0.21	6.12	0.18
Eyebrow Swipe	Obvious	3.43	0.27	5.68	0.17
Finger Wave	Obvious	3.35	0.26	6.83	0.08
Foot Scratch	Subtle	1.88	0.21	6.20	0.17
Foot Tap	Subtle	3.03	0.25	5.48	0.21
Hand Behind Back	Obvious	3.13	0.26	5.32	0.22
Hand In Pocket	Obvious	3.45	0.26	5.43	0.21
Hand Squeeze	Subtle	3.38	0.24	5.18	0.22
Head Nod	Obvious	3.42	0.28	5.45	0.20
Head Tilt	Obvious	2.73	0.25	5.83	0.18
Leg Pat	Subtle	2.67	0.25	5.75	0.17
Leg Rub	Subtle	2.62	0.24	5.77	0.21
Money Gesture	Very Subtle	2.52	0.24	5.87	0.18
Neck Roll	Very Subtle	2.23	0.24	6.18	0.13
Nose Tap	Subtle	3.13	0.26	5.60	0.18
Single Head Nod	Very Subtle	2.98	0.26	5.55	0.21
Single Shoulder Shrug	Subtle	2.60	0.22	5.65	0.20
Stretch	Very Subtle	2.57	0.26	5.95	0.18
teeth click	Very Subtle	2.27	0.22	5.90	0.20
Thigh Scratch	Subtle	3.38	0.27	5.73	0.18

Table 6.4. Interaction Identified as Subtle Along With Original Classification

device in this experiment. While we designed this study using a device-agnostic approach to designing subtle interactions for any wearable, participants may get confused when they are asked to decide if an interaction with technology took place if they don't see one. While this approach introduces a limitation, it does allow us to first come up with a set of subtle enough interactions and then explore what software and hardware would be needed to implement these interactions on emerging wearables.

Another limitation worth noting is the research approach to evaluate the interactions. Although the video approach is convenient and repeatable in contrast with an in-person studies, it is still artificial. Participants are actively monitoring for deceptive behaviors and anomalies in the participant's actions and movements.

6.5 Conclusion

Using results from an interaction elicitation study conducted in 5, we present a set of user-defined input interactions to participants and asked them to evaluate if what they see the actor doing in a set of videos is an action and if that action is an interaction with technology. As a result, we were able to come up with a set of interactions that are subtle enough to be used by a wearable device for discrete interaction.

Chapter 7

Discussion of all Four Studies of the Dissertation

The four studies presented in this dissertation provide unique insight to help researchers and designers understand users' privacy needs and preferences regarding wearable technologies. When brought together, they work synergistically to paint a bigger picture of users' current needs and how researchers and designers can address these needs and improve privacy outcomes. We know that privacy is a key concern for wearables due to the mass collection of personal information[20, 118, 190, 232, 234, 266, 274]. Furthermore, wearables are not primarily designed to address these concerns [379] which exposes users to threats to their privacy [118, 202]. In addition, current privacy controls on wearables are ineffective at affording users control over their personal information due to constrained interaction capabilities [297]. As a result, I argue that when users have more granular sharing options over data from a wearable in terms of data recipient and valence of data, and when control interface mechanisms allow integrated, context-dependent, usable, granular control, it may reduce privacy related threats that could have a negative impact on the user [173] during and beyond the use of the device. The good news is that sensors are already available on commodity wearables that can be leveraged as input mechanisms that provide control to alleviate privacy concerns without any hardware changes. Still, designers need to explore further system interaction opportunities and constraints to develop proper mechanisms that would be usable for users to make privacy decisions.

To review, we see from study 1 (Chapter 3) that if people are offered privacy control options

over data from wearables, they exhibit granular preferences for control, and those preferences are contingent on the recipient of data and valence of data. We suggest the need for new interface options that allow users to exert this type of granular control and accommodate user preferences. However, it is unknown what types of interface options would best provide usable granular control over data from wearables. Hence, study 2 (Chapter 4) builds upon these findings to explore the user preferences and experiences of four settings interfaces that provide different privacy control options. The study results show that when privacy control interfaces are integrated on wearables, users report these interfaces as more straightforward to use than interfaces decoupled from the device. While differing options for the timing of privacy control did not impact evaluations of user experience as expected, the timing of control, ease of use of the control, and the perceived threat posed by using a control option did impact users' reported intent to use the wearable interface in the future, as shown in our exploratory analysis. These findings, along with the knowledge from prior works that suggest that integrated controls have the potential to enhance privacy outcomes for users [297], beg the question: how do we design interfaces that have integrated privacy controls? One solution is user-defined input interactions that can be integrated into wearables. Study 3 (Chapter 5) explores this solution. The study identified a set of user-defined interactions to exert granular control, but results show differences in the types of interactions people produce for situations requiring discretion vs. those that require less discretion, such as when people are alone. Study 4 (Chapter 6) expands on the findings of study 3 by evaluating what interactions would allow discreet privacy control engagement with the wearable, which resulted in a set of interactions that could be subtle enough not to be noticed as interaction with technology.

7.1 Contributions

This dissertation consists of four user studies: 1) understanding user preferences for sharing data from a wearable when recipient, type, and valence of data is considered; 2) investigating the user experience afforded by different privacy interfaces for wearable technologies; 3) identifying a set of interactions that allow in-the-moment privacy control over data from wearables, and 4) evaluating a set of interactions for wearables that are subtle enough that they cannot be recognized by others. In the following paragraphs, I discuss the contributions of each study.

First, I identified that adopters and potential adopters of wearable health technologies have

granular sharing preferences over personal health information from wearables. By quantifying user preference levels based on data type, recipient, and valence, we discover that adopters' and potential adopters' sharing behaviors fall within the avoidance category from the behavioral privacy model. Users have selective sharing preferences, and those preferences are mainly contingent on the recipient of the information and whether or not that information is positive or negative. These results reveal that privacy-enhanced, personalized granular controls are needed for wearables to address the wearer's privacy needs during and beyond the use of the device. Results also suggest that novel interface options are needed to accommodate granular control over wearables.

Second, knowing that users have granular sharing preferences, we evaluated a set of interfaces with different control options for this type of control. We find that the location of privacy control for wearables marginally influences the overall ease of use. This suggests that when privacy controls are integrated and allowed on the same device that collects the data, it may be easier for users to manage their privacy. We also find that the available decision timing options for a wearable interface, the interface's ease of use, and the interface's perceived oversharing threat influence behavioral intent to use privacy interfaces. Taking these two results into consideration, we recommend a modified taxonomy of design features (See Figure 4.8) that researchers should further explore when designing privacy interfaces for wearables that allow granular control options over data. We also recommend that researchers and designers further educate users on the importance of privacy interface options and provide tools to help users connect with the idea of privacy threats associated with wearables.

We know that wearable technologies already have sensors that can be leveraged to integrate sharing decisions with privacy interfaces and offer control in-the-moment. Using this knowledge, we explore the design space for integrated privacy controls on wearables, where privacy decisions can be made directly on the wearable using user-defined interaction techniques. Using an interaction-elicitation study where participants propose interactions that could be used that allow integrated in the moment privacy control, in chapter 5 we identified a set of interactions that users most commonly proposed. I believe merging privacy control into the user's interaction flow would be a more effective way to control personal information. In addition, this study also shows notable differences in the types of interactions people propose for situations requiring privacy in contrast to those that require less privacy. Hence, we further explored interactions collected from this study to identify a set of interactions that could be used for moments when a user needs to interact with their wearable discretely. Study 4 further evaluated these interactions in terms of their noticeability and

identified a potential set of interactions that could be used to allow integrated and in-the-moment control through subtle, discreet, and non-disruptive interactions.

To summarize, the contributions of this dissertation are:

- Leveraging the behavioral privacy model [52], to explore potential factors that may influence sharing behaviors based on type, recipient, and valence of data by quantifying preference level for these factors and examining them in combination in the context of wearable privacy.
  - Investigating adopters and potential adopters' preferences for privacy and sharing of extra clinical health information from a wearable device
  - Learning what types of data users are more willing to share
  - Learning what potential recipients users are more willing their data with.
  - Learning users' sharing preferences based on valence of data
  - Examining privacy control interfaces that allow users to manage their personal data from a wearable actively
- Creating a set of device-independent user-defined interactions that allow in-the-moment control over personal data from a wearable based on the knowledge gained from the two studies above
  - A set of user-defined interactions
  - Evaluating these interactions in terms of their noticeability and subtlety

7.2 Impact on Privacy Research

Privacy is one of the most persistent social issues connected to information technology [243] and is an intricate concept that can take on several definitions in different contexts [300]; in the scientific [376], industrial domains [188] and standardization bodies [72]. No privacy consensus exists [187], as users perceive it differently, due to personal [52, 240] or cultural [331] aspects. Sharing information can be critical or trivial depending on individual perceptions and involving circumstances. In the context of this work, we explore privacy as it relates to the content and recipient of information [52] and explore ways to give users more control over their data and with whom that data is shared with through user-defined interactions. We also explore what types of interactions would be suitable when users would need to express privacy decisions discretely. Within

the HCI community, we know of several works that have examined participants concerns within the context of wearables regarding the type of device, type of sensors used to collect data, type of data collected, perceived risk, and concerns toward the type of data collected [202, 234, 274, 275], but none of these studies use the behavioral privacy model to quantify levels of user preference based on type, recipient, and valence in combination. In this dissertation, I address this gap by leveraging the behavioral privacy model and discover that users have varying sharing behaviors that mostly fall within the avoidance category from the behavioral privacy model. We also know over the past 20 years, privacy interfaces have gained traction within the HCI community, exploring a wide range of context and application domains including, but not limited to: peer-to-peer file-sharing systems [130], interfaces for online social networks [173, 193, 198], and website privacy policies [80]. As far as we know, there are no works that have empirically evaluated user experience for privacy interfaces with wearables based on location and timing of privacy interface, which we adopt from the privacy design space [297]. There also are not any works that we know of that have explored novel interactions for wearables that allow users to express privacy decisions over data from a wearable, nor any works that explore how users can subtly express these privacy decisions. This dissertation encourages privacy researchers to create scientific literature, industrial guidelines, and solutions to provide adequate support for designers to build privacy-preserving solutions for wearable technologies.

7.3 Impact of the Future Design of Wearables

While it is interesting that users do not automatically select the thing that gives them the most control, as we see from study 2 (Chapter 4), control does not change their intent to use. We know from study 1 (Chapter 3) that users desire control over their personal information, but we see from study 2 (Chapter 4) there is a disconnect between their understanding and appreciating interfaces that allow this type of control. The good thing is this did not lessen their interest in adopting technologies that will enable more control. From a design perspective, the interface that gives less control are just as easy to use and have the same user evaluations as interfaces that offer more control. This means that designers should design interfaces that allow more personalized control without negatively impacting their user experience with the interface. Designers should also come up with ways to show the usefulness of this type of control. The desire is already there, but

we need to help users draw out the value or need for the technology to give them control. It is the responsibility of researchers and designers to bridge this gap. While all of the hypothesis in study 2 (Chapter 4) were not supported in terms of location and control, as for being practical and meaningful this study is beneficial because it shows that users see this type of design as equally valuable. We know from prior work the benefits of integrated in-the-moment control [259, 297], and we know that users desire some type of granular control [118, 202, 274], so it shows these types of designs would potentially be accepted by users. As researchers, we need to help users understand the disconnect that they desire the granular control and they want to avoid threats, but in doing so more, granular control options are needed. These issues need to be addressed from a design perspective and from a user educational standpoint. This calls for the need to bridge the world of design and education. From a design standpoint, creating systems that create better outcomes for privacy may be useful, but awareness and education should inform users of ways to control their data [118]. Designers should create educational campaigns that show that threat is not external, but the threat is also based on their decisions on using their technology and what features they use. I believe getting users to understand their responsibilities in mitigating threats instead of threats as being something that happens to them. Previous research posits that users' understanding is accentuated when information intended to educate them about the privacy implications associated with the collection of their data is visualized [15, 281, 333].

The results from the four studies have several implications for designing privacy controls for wearables. As illustrated in Study 1 (Chapter 3), users desire control over their personal information, but the results from Study 2 (Chapter 4)surprisingly illustrate a disconnect where users do not necessarily show a preference for interfaces which would afford them a higher level of privacy control, which is not what we expected. For example, the integrated+synchronous interface design did not receive significantly different scores on ease of use, perceived privacy control, perceived oversharing threat, or intent-to-use compared to the other three interfaces. While we hypothesized that integrated+synchronous interfaces would be better, a positive takeaway from this unexpected result is that arguably, users may not be deterred from adopting privacy interfaces that allow integrated and in-the-moment control, even though they may not be motivated to adopt them, either.

Building upon the findings of Study 2, we suggest that designers also introduce ways to show the usefulness of this type of integrated, synchronous control. The desire for granular sharing options is already there, but there is a pressing need to assist users in understanding the value that

integrated and synchronous privacy controls provide regarding promoting positive privacy outcomes. From a design perspective and as a privacy scholar, I know that a user's main task should not be managing their own privacy [34, 79]. It is the responsibility of researchers and designers to bridge this gap [79]. We know from prior work the benefits of integrated in-the-moment control [259, 297] and when privacy controls are more granular, users are more comfortable using them [323]. The literature illustrates, and the findings of my work posit that granular control options allow users the affordance to actively manage their privacy. This also shows that as these designs emerge, they will be accepted by users. From a design standpoint, creating systems that create better outcomes for privacy is useful, but education should inform users of ways to control their data and incentivize them to adopt interfaces that allow them greater privacy control [118]. If users had a better understanding of how they can improve or hinder their privacy outcomes through the choices they make on what privacy features and interfaces to adopt (versus viewing privacy threats as solely external), it could encourage users to take more control of their privacy outcomes. Previous research posits that users' understanding is accentuated when information intended to educate them about the privacy implications associated with the collection of their data is known or somehow visualized [15, 281, 333]. Designers should explore ways to visualize the privacy implications of using or declining different privacy control options.

When we combine the results from Study 3 (Chapter 5) and Study 4 (Chapter 6), we see that users are able to design certain interactions that allow integrated and in-the-moment control, but there may be a need for an additional set of interactions they can use in situations where others do not notice them. One implication from this work is that designers should consider building interfaces that enable users to not only allow integrated in-the-moment control, but also interfaces that allow users to make those decisions without being noticed. Inherent functions of existing wearables present key implications for the design and fabrication of emerging and invisible wearables. As we shift toward a new generation of wearables that are more flexible and unnoticeable, designers should prioritize subtle interaction capabilities for these emerging devices. [92, 100, 242, 256].

7.4 Broader Implications of this work

When we combine the findings from Study 1(chapter 3) and Study 2 (chapter 4), we find that, while people do desire granular control, they do not necessarily view interfaces that offer

integrated and synchronous privacy controls as more or less usable. The good news from this result is that it will likely be just as easy for users to adopt privacy interfaces that we consider as more useful from a privacy standpoint, as it would be useful to adopt those that are not as useful from a privacy standpoint. It seems like what people care about most is if the system is easy to use and if it provides a low perceived threat to their privacy. The perceived control over data afforded by the interface does not seem to factor into whether users intend to use the system or not. This result could explain why there were no differences between conditions of timing and location from study 2 (chapter 4). One future direction worth exploring is, how do we get users to connect the idea of control with the idea of the threat. If users are unable to make this connection, there will be issues with users adopting the technology. When we combine the results from Study 1 (chapter 3) and Study 3 (chapter 5) we see that users desire more granular control, and we discover what types of gestures could be used to express that granular control. A notable implication of our findings is that a subset of the interactions for privacy control we identify may be implemented on existing commodity wearables without hardware changes.

The outcome of this research will directly impact the field of wearable IoT by demonstrating novel approaches to understanding and designing privacy-enhanced technologies for emerging wearables. This work will also support scientists, designers, and researchers developing education tools to minimize privacy risks. The tools may be shared widely within the research community to enable broader experimentation around educating individuals about their privacy related to emerging wearable technologies. Furthermore, this work will advance scientific knowledge through the design and development of novel interaction mechanisms that are well-integrated into a system's interaction design [297] that allow privacy control over information produced by emerging medical devices.

7.5 Recommendations For Future Work

Using a human-centered approach, researchers should explore objective privacy risk [11] and concerns posed by the adoption of wearable and a new class of wearables. More specifically, research should focus on marginalized groups that are more at risk of privacy-related threats. I believe exploring the perceptions and behaviors of these groups in greater depth will lead toward the development of practical privacy-enhancing tools and techniques to protect these populations against potential threats and concerns when using wearable health technologies. As a long-term

vision for wearable IoT, it is also essential to understand what factors prohibit individuals from marginalized populations' privacy control. Computer Scientists, social scientists, HCI researchers, and Privacy Experts should all work together on this topic to inform the design of effective privacy controls for novel and emerging wearable devices. In doing so, we empower individuals populations who may be more vulnerable to privacy-related threats and educate them on ways to make informed decisions, gain better control over their personal data, and maintain better privacy practices.

7.6 Summary

Increasing concerns and threats to privacy in the context of wearable health technologies pose a significant risk to users. People need solutions to reduce these risk when using wearables that continuously collect personal information. Researchers have explored different approaches to understanding user concerns as it relates to wearable privacy and has even proposed frameworks to address these concerns [297]. For privacy to have any meaning in the context of wearables, granular control options are needed, as we noted in chapter 3. Our work informs the need for practical and theoretical frameworks to be developed to allow users more granular control over their data and ways to manage their privacy actively. This dissertation focused on understanding user preferences to share data from wearables and offer more privacy-enhanced solutions that align with user needs. This work aims to contribute toward the design of usable and effective privacy control mechanisms for wearables that allow adopter's and potential adopter's integrated and in-the-moment granular control over personal information.

Appendices

Appendix A Study 1 Materials

How would you interact with a Wearable?

What: Spend time interacting with a wearable device.
When: During flexible business hours. Get in touch for a schedule.
Why: We are investigating how people interact with wearable devices and we need your help.
Where: McAdams Hall
How much: $20 gift card

Would you like to participate in a gesture elicitation study? We are conducting a study to elicit gestures in order to implement granular privacy control on wrist-worn and head-mounted wearable devices. Your insight and feedback is valuable as we look to design methods to extend input space on wrist-worn wearables to give users control over their privacy!

The study consists of a gesture elicitation study that will take approximately one hour to complete. All information collected is confidential, and you will receive a US $20 gift card incentive for your participation.

If you are interested, please contact us by email (clemsonhatlab@gmail.com).

clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com	clemsonhatlab@gmail.com

Figure 1. Recruitment Flyer For Study 1

Information about Being in a Research Study
Clemson University

Gesture Elicitation Study

Description of the Study and Your Part in It
Byron Lowens, Kelly Caine and Jacob Sorber are inviting you to take part in a research study. The purpose of this research is to elicit gestures for users to implement granular privacy control on wrist-worn devices

Your part in this study will be to participate in a gesture elicitation study. We will begin the study by asking you some exploratory questions to gather your demographic information and experience with using wrist-worn devices. The next phase of the study will involve you interacting with a wrist-worn device (e.g. Fitbit, Apple Watch, etc.) and/or a head-mounted device (blue-tooth earbuds, wireless bone conduction headphones). You will be asked to come up with and perform input gestures you feel would match certain tasks. During this study, we will verbally describe the action carried out by the wrist-worn and/or head-mounted device and ask you to perform the input gesture and repeat the gesture. We will also record additional information such as verbal responses, and movements during interaction as well as classify and label each interaction mechanism to identify common themes. The study will be audio and video recorded, and photos will be taken during the session for documentation and analysis.

It will take you about one hour to be in this study.

Risks and Discomforts
We do not know of any risks or discomforts to you in this research study.

Possible Benefits
This research may help us to understand user need for granular privacy control on Wrist Worn and Head-Mounted Devices.

Incentives
You will receive a $20 gift card for your participation.

Protection of Privacy and Confidentiality
With your permission, photos, audio, and video recordings will be used to record important information. They will be stored on a secure server, and only the project researchers will have access to the data. All audio, video and photography files will be destroyed not later than seven years after their recording date. No information will be shared outside the research team without your permission.

CLEMSON
RESEARCH COMPLIANCE

IRB Number: IRB2015-143
Approved: 6/15/2017
Expiration: 6/14/2018

Figure 2. Informed Consent For Study 1

Gesture Elicitation Study Script

Introduction: Hello! My name is _____and I will be conducting the study today with you. Thank you for your participation. Let's begin

Explanation of Goal: As we mentioned previously, the goal of this study is understand your preferred input gestures to exert granular privacy control on wearable devices based on a series of tasks. This session will last about 1 hour. Once you have answered some survey questions we will begin the study. Please let me know once you have completed the survey questions.

Let's begin with some tasks.

Explanation of Tasks: Your task in this study will be to interact with a wrist-worn and/or head-mounted device, perform a set of pre-defined tasks, come up with input gesture to perform task, provide feedback, opinions and perspectives about the task and input gesture. First we will provide you with a basic scenario and then verbally describe the task to be performed based on that scenario. We will then ask you to produce an input gesture that would activate the device action. Please focus on how you design the gesture and assume all gestures that you preform will be recognized by the wrist-worn device and head-mounted device. You can also repeat a gesture for the given task if you feel the need to. Please feel free to think aloud as you perform the tasks and repeat your gesture one additional time. Once you complete the tasks we will provide you with a post-task questionnaire before proceeding to the next task. Let's begin! Here is the wearable that you will be using. Take a moment to get comfortable with the device and we will begin the set of tasks that you need to perform.

The wearable device you will be used strictly as a reference and will not provide any visual elements specific to the task you will be performing. Let's start off with the first scenario and task that you need to perform.

Example Scenario
Scenario 1
DEVICE: HMD
Investigator: Imagine that you are at home alone and you get the following prompt on your device.
Participant: Stress level indicates you were anxious today
Investigator: Would you share this information with your Employer?

Participant:
- Yes
- No

Investigator: You indicated that you _____ this information with your Employer. Can you please show me a gesture based on your decision to _____ this information with your Employer if you got this prompt on the device while you are at home alone

Scenario 2
DEVICE: HMD
Investigator: In the following scenario you will imagine that you are at work alone and you get the following prompt on your device.
Participant: Today you exceeded your calorie intake goal
Investigator: Would you share this information with your Broader Social Network.
Participant:

Figure 3. Study Script For Study 1 (page 1)

- Yes
- No

Investigator: You indicated that you _____ this information with your Broader Social Network. Can you please show me a gesture based on your decision to _____ this information with your Broader Social Network? if you got this prompt on the device while at work alone.

*Please notice that this script is indicative, comprehending all activities and questions planned for the study. Despite being complete, this study script may be subject to minor changes, as is common in qualitative research. These minor changes include for instance the order of the questions, their wording, details or phrasing, aiming at better clarifying the activity for participants whenever necessary.

Figure 4. Study Script For Study 1 (page 2)

Gesture Elicitation Study
Profile Survey

What is your gender?
- o Male
- o Female
- o Other
- o I prefer not to answer

What is your age?
- o 18-24 years old
- o 25-34 years old
- o 35-44 years old
- o 45-54 years old
- o 55+

What is your ethnicity?
- o White
- o Hispanic or Latino
- o Black or African American
- o Native American or American Indian
- o Asian / Pacific Islander
- o Other

Which of the following best describes your current employer?
- o Government
- o Educational institution
- o Business or industry
- o Non-profit organization
- o Other

What is the highest level of school you have completed or the highest degree you have received?
- o High school incomplete or less
- o High school graduate or GED (includes technical/vocational training that doesn't count towards college credit)
- o Some college (some community college, associate's degree)
- o Four year college degree/bachelor's degree
- o Some postgraduate or professional schooling, no postgraduate degree
- o Postgraduate or professional degree, including master's, doctorate, medical or law degree
- o I prefer not to answer

Which of these best describes you?
- o Married
- o Living with a partner
- o Divorced
- o Separated
- o Widowed
- o Never been married
- o I prefer not to answer

Figure 5. Pre-Survey Demographic Questionnaire For Study 1 (page 1)

Which of the following best describes your technology knowledge?

- o Basic
- o Intermediate
- o Advanced
- o Professional
- o None

About how often do you use Internet either on a computer or on a mobile device like a smartphone or a tablet?

- o Most of the day
- o Several times a day
- o About once a day
- o A few times a week
- o A few times a month
- o A few times a year
- o Never
- o I prefer not to answer

About how often do you visit social media sites such as Facebook, Twitter or LinkedIn?

- o Most of the day
- o Several times a day
- o About once a day
- o A few times a week
- o A few times a month
- o A few times a year
- o Never
- o I prefer not to answer

Do you own a wrist-worn wearable device (e.g., Fitbit, Apple Watch, etc.)?

- o Yes
- o No

Do you have interest in using wrist-worn wearable device (e.g., Fitbit, Apple Watch, etc.)?

- o Yes
- o No

Do you own a head-mounted wearable device (blue-tooth earbuds, wireless bone conduction headphones.)?

- o Yes
- o No

Do you have interest in using a head-mounted wearable device (blue-tooth earbuds, wireless bone conduction headphones.)?

- o Yes
- o No

Figure 6. Pre-Survey Demographic Questionnaire For Study 1 (page 2)

Privacy means different things to different people today. In thinking about all of your daily interactions - both online and offline - please tell us how important each of the following are to you:

Being in control of who can get information about you.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Being able to share confidential matters with someone you trust.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Not having someone watch you or listen to you without your permission.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Controlling what information is collected about you.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Not being disturbed at home.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Being able to have times when you are completely alone, away from anyone else.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Having individuals in social / work situations not ask you things that are highly personal.
- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Figure 7. Pre-Survey Demographic Questionnaire For Study 1 (page 3)

Being able to go around in public without always being identified.

- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Being in control of who can get information about you.

- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Not being monitored at work.

- o Not at all important
- o Not very important
- o Somewhat important
- o Very important
- o Don't know

Figure 8. Pre-Survey Demographic Questionnaire For Study 1 (page 4)

Please indicate how sensitive you consider the given information

	Very Sensitive	Somewhat Sensitive	Not too sensitive	Not at all sensitive	I prefer not to answer
You met your step goal for today	○	○	○	○	○
You did not meet your step goal for today	○	○	○	○	○
During your last workout you spent over 45 minutes in the Fat Burn Zone	○	○	○	○	○
During your last workout you burned less calories than average	○	○	○	○	○
You met your sleep quality goal	○	○	○	○	○
You did not meet your sleep quality goal	○	○	○	○	○
Sleep goal met for the week	○	○	○	○	○
Sleep goal not met for the week	○	○	○	○	○
Stress levels indicate you were calm today	○	○	○	○	○
Stress levels indicate you were anxious today	○	○	○	○	○
Your blood pressure was normal this week	○	○	○	○	○
Your blood pressure was high this week	○	○	○	○	○
Today you met your calorie intake goal	○	○	○	○	○

Figure 9. Post-Survey Questionnaire For Study 1 (page 1)

Figure 10. Post-Survey Questionnaire For Study 1(page 2)

Please indicate your rating of the following information

	Very Negative 1	2	Neutral 3	4	Very Positive 5
You met your step goal for today	○	○	○	○	○
You did not meet your step goal for today	○	○	○	○	○
During your last workout you spent over 45 minutes in the Fat Burn Zone	○	○	○	○	○
During your last workout you burned less calories than average	○	○	○	○	○
You met your sleep quality goal	○	○	○	○	○
You did not meet your sleep quality goal	○	○	○	○	○
Sleep goal met for the week	○	○	○	○	○
Sleep goal not met for the week	○	○	○	○	○
Stress levels indicate you were calm today	○	○	○	○	○
Stress levels indicate you were anxious today	○	○	○	○	○
Your blood pressure was normal this week	○	○	○	○	○
Your blood pressure was high this week	○	○	○	○	○

Figure 11. Post-Survey Questionnaire For Study 1 (page 3)

Figure 12. Post-Survey Questionnaire For Study 1 (page 4)

Appendix B Study 2 Materials

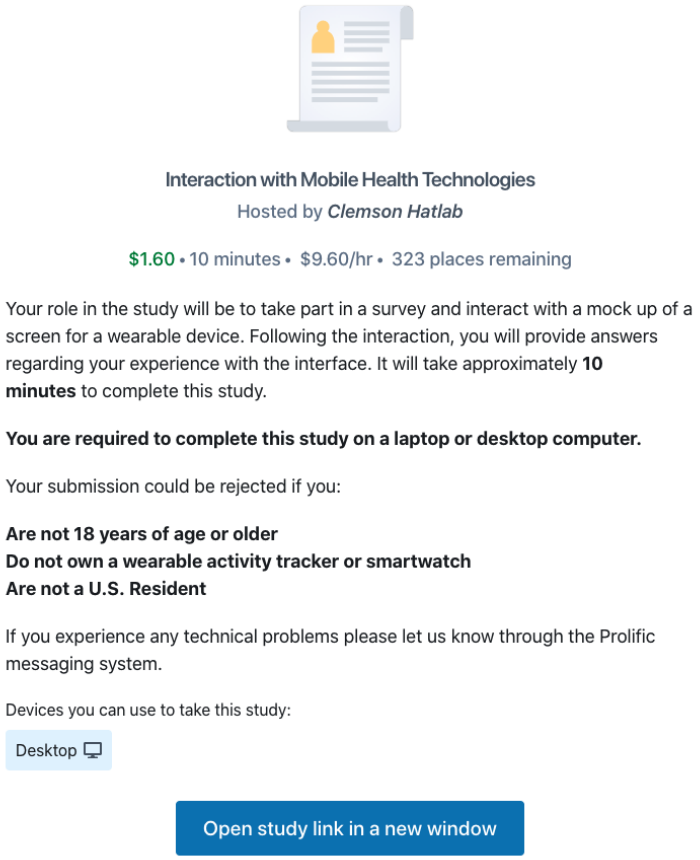


Figure 13. Recruitment Flyer used on Prolific For Study 2

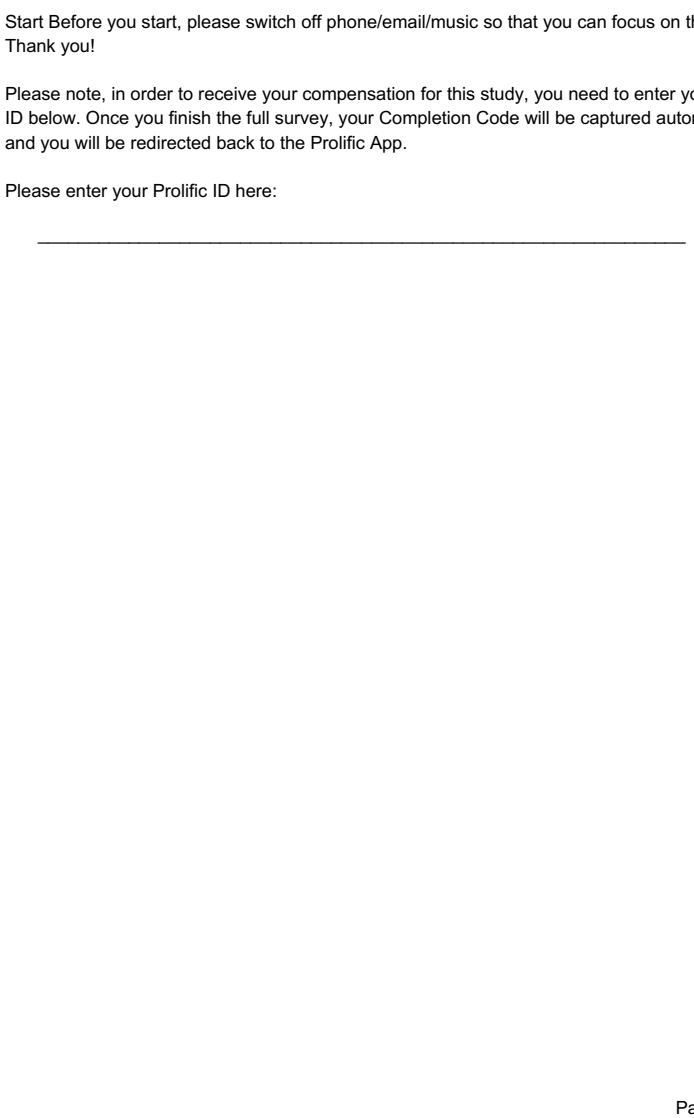


Figure 14. Page to record participants unique Prolific ID For Study 2

Information about Being in a Research Study

Clemson University is inviting you to take part in a research study. The purpose of this study is to gather information about interface controls for wearable technologies.

Your part in the study will be to take a survey where you will interact with a mock-up of a screen (i.e., an interface) for a wearable technology. Following the interaction, you will provide answers regarding your experience with the interface. It will take approximately **10 minutes** to complete this study.

Possible Risks and Discomforts
We do not know of any risks or discomforts to you in this research study.

Possible Benefits
While you may not benefit directly from taking part in the study, it is possible you will learn about the different interface mechanisms that could be implemented for wearable technologies. Additionally, this research may help us enable new interfaces for wearable devices.

Incentives
After completing the survey, **you will be compensated $1.60** for your participation.

Protection of Privacy and Confidentiality
We will not tell anyone outside of the research team of your participation in this study or what information we collect about you in particular. No sensitive information will be requested and information collected will be securely stored. The National Science Foundation (NSF), as the founder of this project, might have access to the study data and conclusive results of this research. Your identity will not be revealed in any publication or presentation that might result from this study.

Choosing to Be in the Study
You do not have to participate in this study. You may choose not to take part and you may choose to stop taking part at any time. You will not be punished in any way if you decide not to be in the study or to stop taking part in the study.

Contact Information
If you have any questions or concerns about this study or if any problems arise, please contact Clemson University Hatlab at clemsonhatlab@gmail.com or the Clemson University Office of Research Compliance (ORC) at irb@clemson.edu.
Clicking on the "agree" button indicates that: • You have read the above information • You voluntarily agree to participate • You are at least 18 years of age

○ I agree and I would like to participate in this study

○ I disagree and I would not like to participate in this study

Page 2 of 50

Figure 15. Informed Consent For Study 2

Q2 Which of the following best describes your technology knowledge?

- ○ Basic
- ○ Intermediate
- ○ Advanced
- ○ Professional
- ○ None

Q3 Which of the following wearable technologies do you own, if any? (Select all that apply.)

- ☐ Fitbit
- ☐ Apple Watch
- ☐ Xiaomi
- ☐ Samsung Galaxy Watch
- ☐ Huawei
- ☐ Jabra Sport Pulse Wireless Bluetooth Stereo Earbuds
- ☐ Other wearable health technology, smart watch, or activity tracker
- ☐ ⊗ I do not own a wearable device

Page 3 of 50

Figure 16. Screener Questionnaire For Study 2 (page 1)

Q1 We care about the quality of our survey data and hope to receive the most accurate measure of your opinions, so it is important to us that you thoughtfully provide your best answer to each question in the survey. Do you commit to providing your thoughtful and honest answers to the questions in this survey?

- ○ I will provide my best answers
- ○ I will not provide my best answers
- ○ I can't promise either way

Page Break

Page 4 of 50

Figure 17. Screener Questionnaire For Study 2 (page 2)

For the next part of this survey, we are going to present you with a scenario and an interactive mock-up of a wearable device. You'll be presented with a method for sharing health information collected from a wrist-worn health-tracking device (similar to a FitBit or Apple Watch). You will move through each part of the scenario by either clicking a "Next" button or interacting with a device mock-up (e.g., clicking on a notification or button on the device).

Imagine that you actually own the wearable device and use it daily. Please pay attention to how the sharing options are being presented to you, as you will be asked questions about your experience of that method.

End of Block: Instructions

Start of Block: Integrated Synchronous

Your health care provider advised you to purchase a new wearable activity tracker to track your daily activity so you can adopt a healthier lifestyle.

The activity tracker is able to track your daily steps, activity levels, mood, and food intake. Your health care provider advised you to set a goal to complete 10,000 steps a day and share that data automatically with him/her once it is completed.

When you complete 10,000 steps, your wearable device will notify you at that moment and provide sharing options on the wearable device.

Click Here To Proceed

Page 5 of 50

Figure 18. Experimental Condition For IS Interface

IS1.1 Please select the letter indicated in the last screen of the interactive scenario above.

- ○ A
- ○ B
- ○ C
- ○ I was not able to make it to the last screen

Page Break

Page 6 of 50

Figure 19. Attention Check question used to to check if participants were attentive during the IS Conditions

IS2 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to share your data in-the-moment from the wearable device. Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IS2.1 Using this settings interface would be easy for me.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IS2.2 I find it easy to get this settings interface to do what I want it to do.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page 7 of 50

Figure 20. Interface Evaluation for the IS Condition (Perceived Ease of Use page 1)

IS2.3 My interaction with the settings interface was clear and understandable.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IS2.4 I find the settings interface easy to use.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 21. Interface Evaluation for the IS Condition (Perceived Ease of Use page 2)

IS2.5 Managing my sharing preferences using the settings interface was convenient.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page Break

Page 9 of 50

Figure 22. Interface Evaluation for the IS Condition (Perceived Ease of Use page 3)

IS3 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to share your data in-the-moment from the wearable device. Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IS3.1 The settings interface restricted me from my preferred choice of how to share my data.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IS3.2 I had limited control over my personal information using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 23. Interface Evaluation for the IS Condition (Perceived Privacy Control page 1)

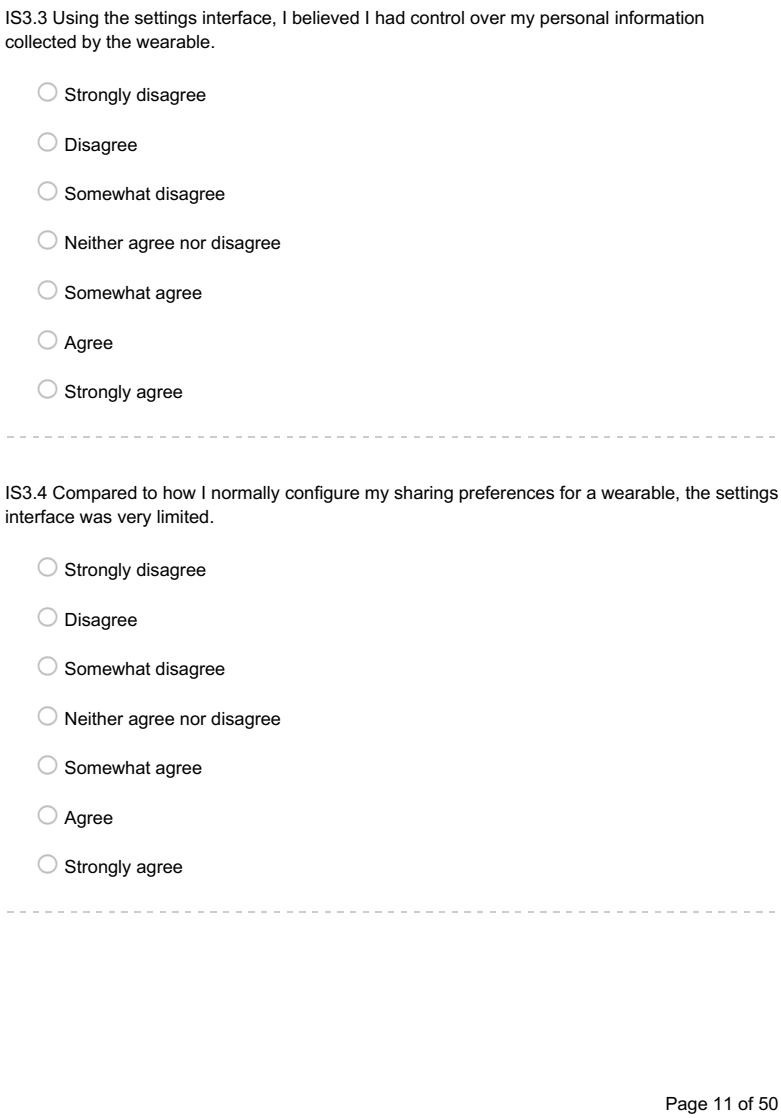


Figure 24. Interface Evaluation for the IS Condition (Perceived Privacy Control page 2)

Figure 25. Interface Evaluation for the IS Condition (Perceived Privacy Control page 3)

IS4 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to share your data in-the-moment from the wearable device. Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IS4.1 Using the settings interface, I believe too much of my data will be shared.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IS4.2 I am comfortable with the amount of data that could be shared using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page 13 of 50

Figure 26. Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 1)

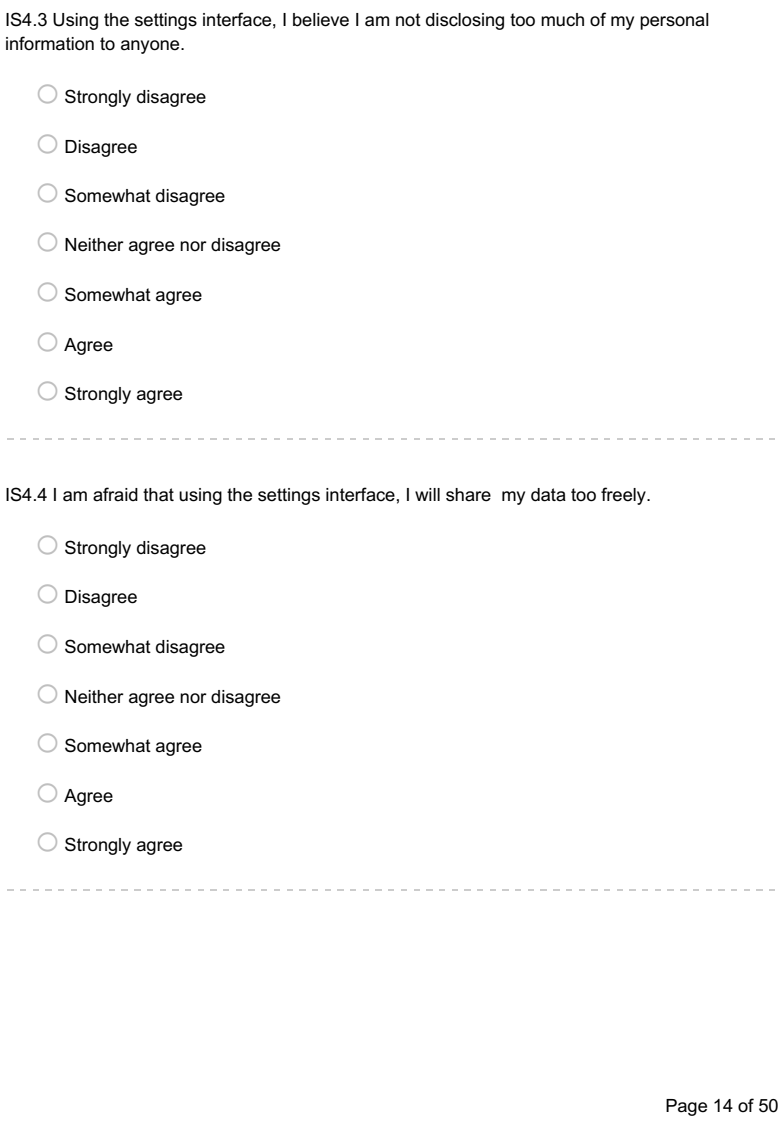


Figure 27. Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 2)

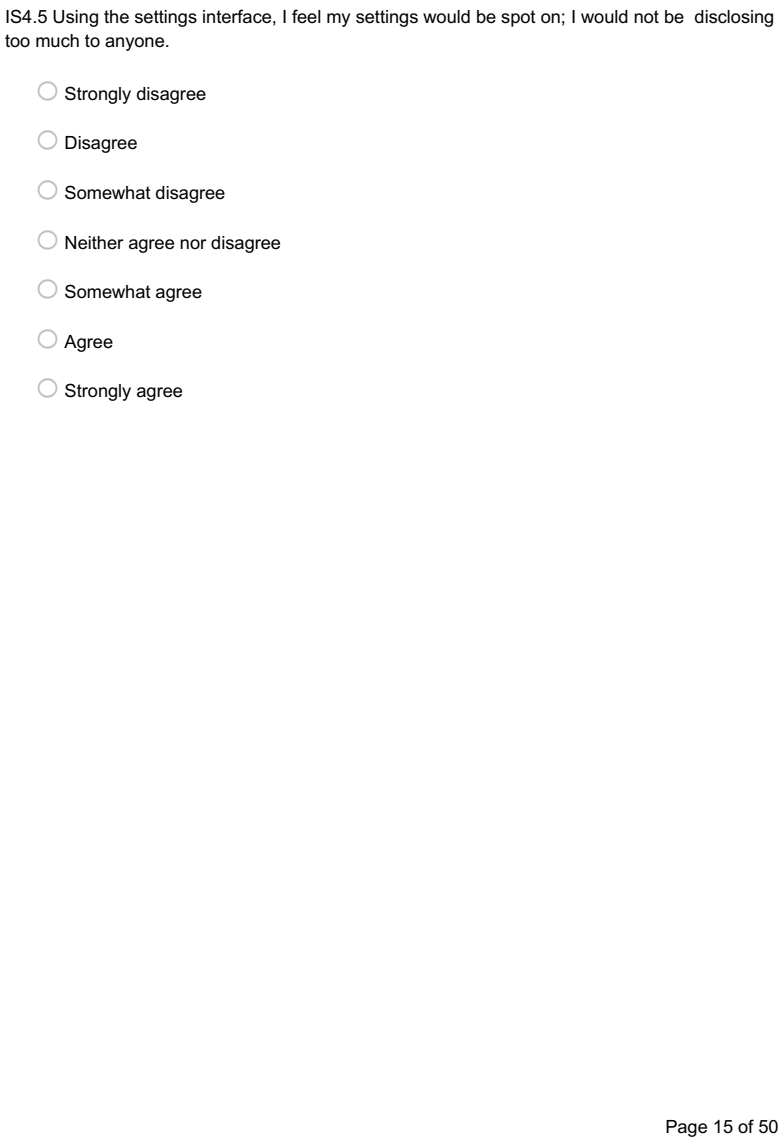


Figure 28. Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 3)

Your health care provider advised you to purchase a new wearable activity tracker to track your daily activity so you can adopt a healthier lifestyle.

The activity tracker is able to track your daily steps, activity levels, mood, and food intake. Your health care provider advised you to set a goal to complete 10,000 steps a day and share that data automatically with him/her once it is completed.

Your wearable device will notify you at the beginning of the day so that you can specify whether or not your data will be shared once you complete 10,000 steps for that day.

Click Here To Proceed

IA1.1 Please select the letter indicated in the last screen of the interactive scenario above.

- A
- B
- C
- I was not able to make it to the last screen

Page Break

Page 16 of 50

Figure 29. Experimental Condition For IA Interface + Attention Check question used to to check if participants were attentive

IA2 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use the wearable device to make a choice about sharing your step goal data before you completed your goal for the day. Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IA2.1 Using this settings interface would be easy for me.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IA2.2 I find it easy to get this settings interface to do what I want it to do.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page 17 of 50

Figure 30. Interface Evaluation for the IA Condition (Perceived Ease of Use page 1)

IA2.3 My interaction with the settings interface was clear and understandable.

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

IA2.4 I find the settings interface easy to use.

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

Figure 31. Interface Evaluation for the IA Condition (Perceived Ease of Use page 2)

IA2.5 Managing my sharing preferences using the settings interface was convenient.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page Break

Page 19 of 50

Figure 32. Interface Evaluation for the IA Condition (Perceived Ease of Use page 3)

IA3 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use the wearable device to make a choice about sharing your step goal data before you completed your goal for the day.** Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IA3.1 The settings interface restricted me from my preferred choice of how to share my data.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IA3.2 I had limited control over my personal information using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 33. Interface Evaluation for the IA Condition (Perceived Privacy Control page 1)

IA3.3 Using the settings interface , I believed I had control over my personal information collected by the wearable.

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

IA3.4 Compared to how I normally configure my sharing preferences for a wearable, the settings interface was very limited.

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

Page 21 of 50

Figure 34. Interface Evaluation for the IA Condition (Perceived Privacy Control page 2)

IA3.5 I would like to have more control over the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page Break

Page 22 of 50

Figure 35. Interface Evaluation for the IA Condition (Perceived Privacy Control page 3)

IA4 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use the wearable device to make a choice about sharing your step goal data before you completed your goal for the day.** Please think about your experience interacting with the wearable in the scenario as you answer the following questions.

IA4.1 Using the settings interface, I believe too much of my data will be shared.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

IA4.2 I am comfortable with the amount of data that could be shared using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 36. Interface Evaluation for the IA Condition (Perceived Oversharing Threat page 1)

IA4.3 Using the settings interface, I believe I am not disclosing too much of my personal information to anyone.

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

IA4.4 I am afraid that using the settings interface, I will share my data too freely.

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

Figure 37. Interface Evaluation for the IS Condition (Perceived Oversharing Threat page 2)

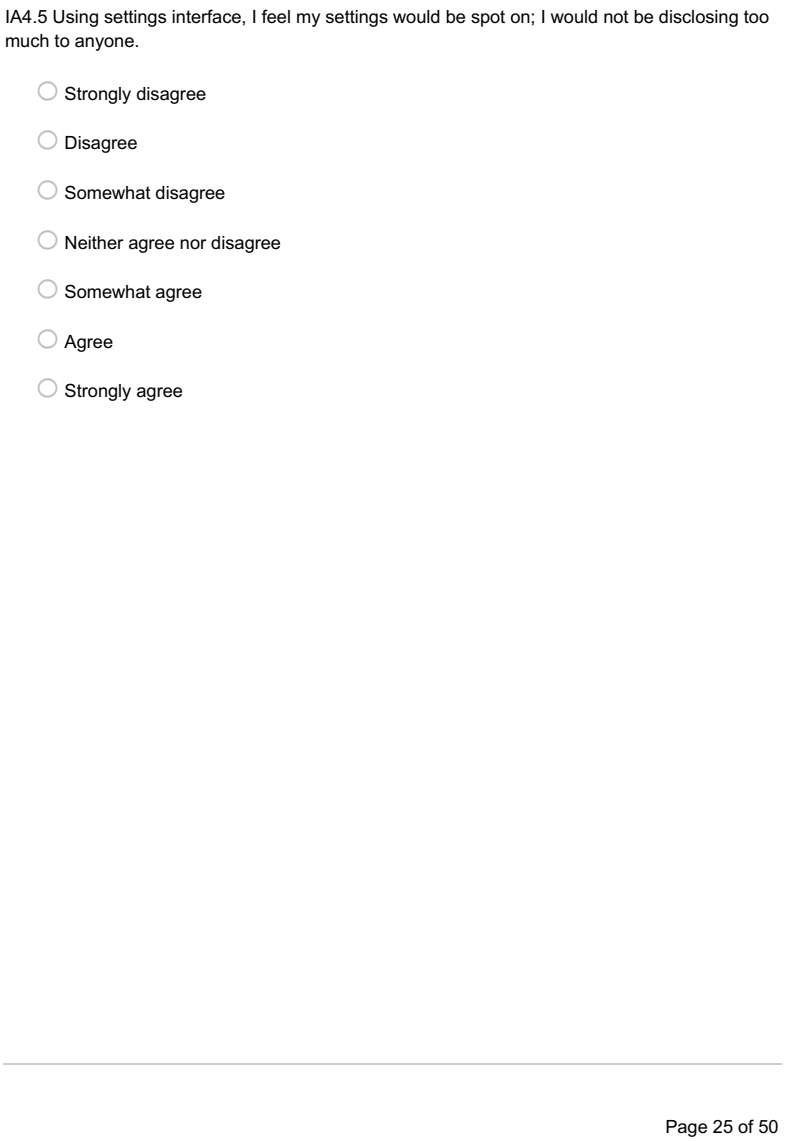


Figure 38. Interface Evaluation for the IA Condition (Perceived Oversharing Threat page 3)

Start of Block: Decoupled Synchronous

Your health care provider advised you to purchase a new wearable activity tracker to track your daily activity so you can adopt a healthier lifestyle.

The activity tracker is able to track your daily steps, activity levels, mood, and food intake. Your health care provider advised you to set a goal to complete 10,000 steps a day and share that data automatically with him/her once it is completed.

When you complete 10,000 steps, your wearable device will notify you at that moment and provide you with sharing options that can be made via a mobile device.

Click Here To Proceed

DS1.1 Please select the letter indicated in the last screen of the interactive scenario above.

- A
- B
- C
- I was not able to make it to the last screen

Page Break

Page 26 of 50

Figure 39. Experimental Condition For DS Interface + Attention Check question used to to check if participants were attentive

DS2 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) notified you of your step goal in-the-moment via the wearable and allowed you to make a sharing decision from a mobile device.** Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

DS2.1 Using this settings interface would be easy for me.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page 27 of 50

Figure 40. Interface Evaluation for the DS Condition (Perceived Ease of Use page 1)

DS2.2 I find it easy to get this settings interface to do what I want it to do.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DS2.3 My interaction with the settings interface was clear and understandable.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 41. Interface Evaluation for the DS Condition (Perceived Ease of Use page 2)

DS2.4 I find the settings interface easy to use.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DS2.5 Managing my sharing preferences using the settings interface was convenient.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page Break

Figure 42. Interface Evaluation for the DS Condition (Perceived Ease of Use page 3)

DS3 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) notified you of your step goal in-the-moment via the wearable and allowed you to make a sharing decision from a mobile device. Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

DS3.1 The settings interface restricted me from my preferred choice of how to share my data.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DS3.2 I had limited control over my personal information using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 43. Interface Evaluation for the DS Condition (Perceived Privacy Control page 1)

DS3.3 Using the settings interface, I believed I had control over my personal information collected by the wearable.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DS3.4 Compared to how I normally configure my sharing preferences for a wearable, the settings interface was very limited.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 44. Interface Evaluation for the DS Condition (Perceived Privacy Control page 2)

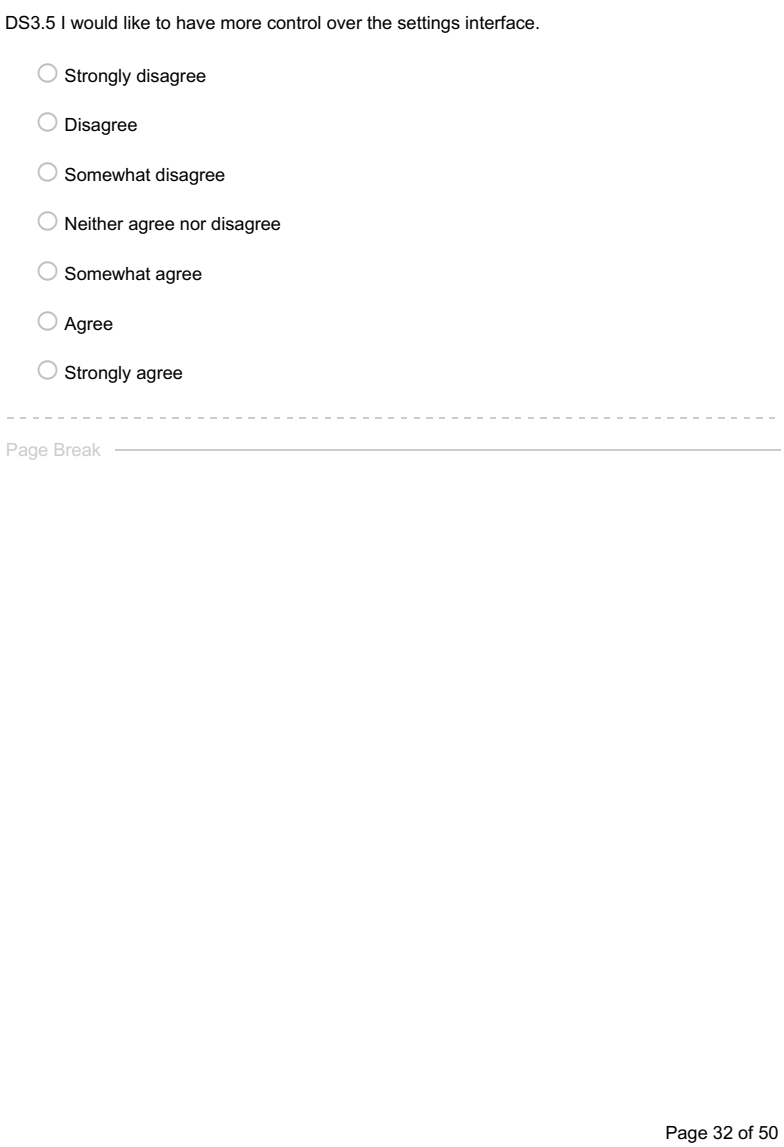


Figure 45. Interface Evaluation for the DS Condition (Perceived Privacy Control page 3)

Q133 In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) notified you of your step goal in-the-moment via the wearable and allowed you to make a sharing decision from a mobile device. Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

Q134 Using the settings interface, I believe too much of my data will be shared.

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

Q135 I am comfortable with the amount of data that could be shared using the settings interface.

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

Page 33 of 50

Figure 46. Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 1)

Q136 Using the settings interface, I believe I am not disclosing too much of my personal information to anyone.

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

Q137 I am afraid that using the settings interface, I will share my data too freely.

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

Figure 47. Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 2)

Q138 Using settings interface, I feel my settings would be spot on; I would not be disclosing too much to anyone.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 48. Interface Evaluation for the DS Condition (Perceived Oversharing Threat page 3)

Start of Block: Decoupled Asynchronous

DA1

Your health care provider advised you to purchase a new wearable activity tracker to track your daily activity so you can adopt a healthier lifestyle.

The activity tracker is able to track your daily steps, activity levels, mood, and food intake. Your health care provider advised you to set a goal to complete 10,000 steps a day and share that data automatically with him/her once it is completed.

Your mobile device will notify you at the beginning of the day so that you can specify whether or not your data will be shared once you complete 10,000 steps for that day.

Click Here To Proceed

DA1.1 Please select the letter indicated in the last screen of the interactive scenario above.

- A
- B
- C
- I was not able to make it to the last screen

Page Break

Page 36 of 50

Figure 49. Experimental Condition For DA Interface + Attention Check question used to to check if participants were attentive

DA2 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use your mobile device to make a choice about sharing your step goal data before you completed your goal for the day.** Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

DA2.1 Using this settings interface would be easy for me.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DA2.2 I find it easy to get this settings interface to do what I want it to do.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page 37 of 50

Figure 50. Interface Evaluation for the DA Condition (Perceived Ease of Use page 1)

DA2.3 My interaction with the settings interface was clear and understandable.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DA2.4 I find the settings interface easy to use.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 51. Interface Evaluation for the DA Condition (Perceived Ease of Use page 2)

DA2.5 Managing my sharing preferences using the settings interface was convenient.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Page Break

Figure 52. Interface Evaluation for the DA Condition (Perceived Ease of Use page 3)

DA3 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use your mobile device to make a choice about sharing your step goal data before you completed your goal for the day.** Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

DA3.1 The settings interface restricted me from my preferred choice of how to share my data.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

DA3.2 I had limited control over my personal information using the settings interface.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 53. Interface Evaluation for the DA Condition (Perceived Privacy Control page 1)

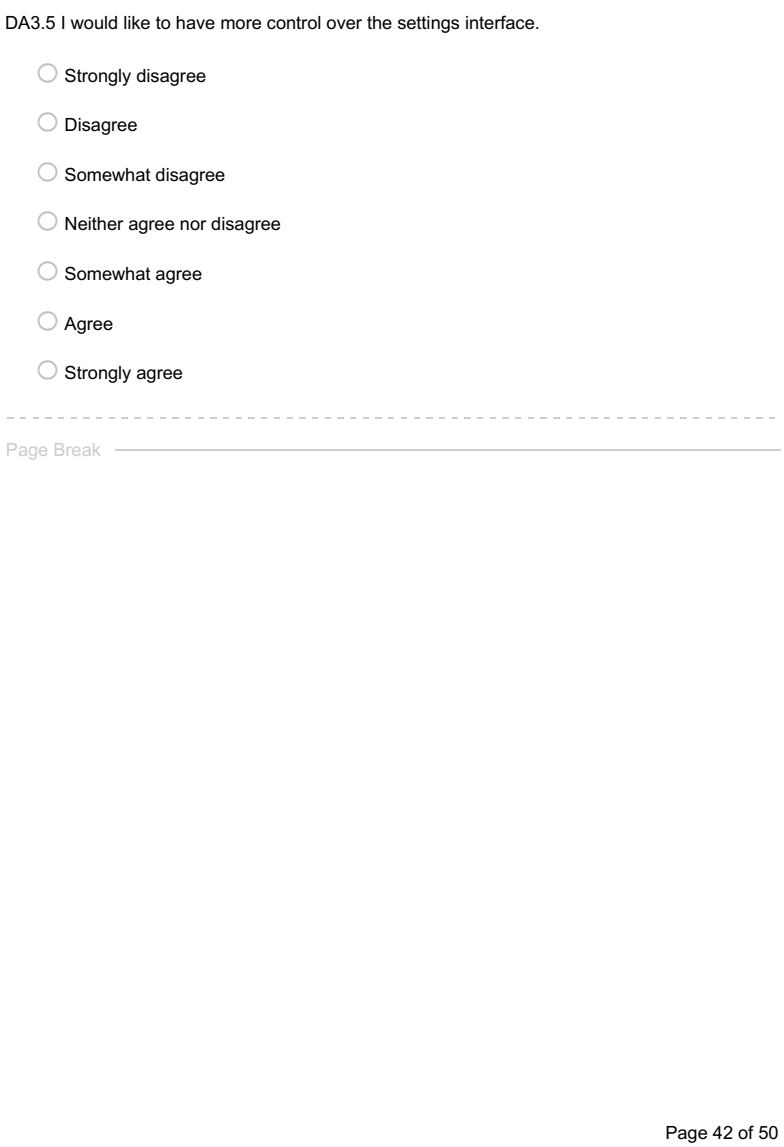


Figure 54. Interface Evaluation for the DA Condition (Perceived Privacy Control page 2)

DA4 **In the scenario you just completed, the settings interface (i.e. the method for sharing your step goal) allowed you to use your mobile device to make a choice about sharing your step goal data before you completed your goal for the day.** Please think about your experience interacting with the wearable and the mobile device in the scenario as you answer the following questions.

DA4.1 Using the settings interface, I believe too much of my data will be shared.

- ○ Strongly disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Figure 55. Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 1)

DA4.2 I am comfortable with the amount of data that could be shared using the settings interface.

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

DA4.3 Using the settings interface, I believe I am not disclosing too much of my personal information to anyone.

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

Figure 56. Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 2)

DA4.4 I am afraid that using the settings interface, I will share my data too freely.

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

DA4.5 Using settings interface, I feel my settings would be spot on; I would not be disclosing too much to anyone.

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

End of Block: Decoupled Asynchronous

Start of Block: Demographics

Figure 57. Interface Evaluation for the DA Condition (Perceived Oversharing Threat page 3)

Q31 Privacy means different things to different people today. In thinking about all of your daily interactions-both online and offline-please tell us how important each of the following are to you:

	Not at all Important	Not very Important	Somewhat Important	Very Important	I do not know
Being in control of who can get information about you	○	○	○	○	○
Being able to share confidential matters with someone you trust	○	○	○	○	○
Not having someone watch or listen to you without your permission	○	○	○	○	○
Controlling what information is collected about you	○	○	○	○	○
Being able to have times when you are completely alone, away from anyone else	○	○	○	○	○
Having individuals in social/work situations not ask you things that are highly personal	○	○	○	○	○
Being able to go around in public without	○	○	○	○	○

Page 46 of 50

Figure 58. Post-Survey Questionnaire For Study 2 (page 1)

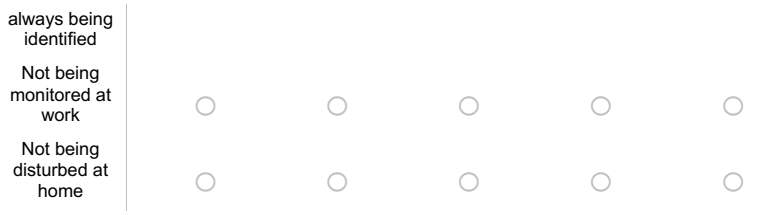


Figure 59. Post-Survey Questionnaire For Study 2 (page 2)

D1 What is your gender?

- Male
- Female
- Other
- I prefer not to answer

D2 What is your race/ethnicity?

- White
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Other
- I prefer not to answer

Page Break

Page 48 of 50

Figure 60. Post-Survey Questionnaire For Study 2 (page 3)

Q25 Which of the following categories best describes your employment status?

- Student
- Employed (working 40 or more hours per week)
- Employed (working 1-39 hours per week)
- Not employed (looking for work)
- Not employed (not looking for work)
- Retired
- Disabled
- I prefer not to answer

Page Break

Figure 61. Post-Survey Questionnaire For Study 2 (page 4)

Appendix C Study 4 Materials

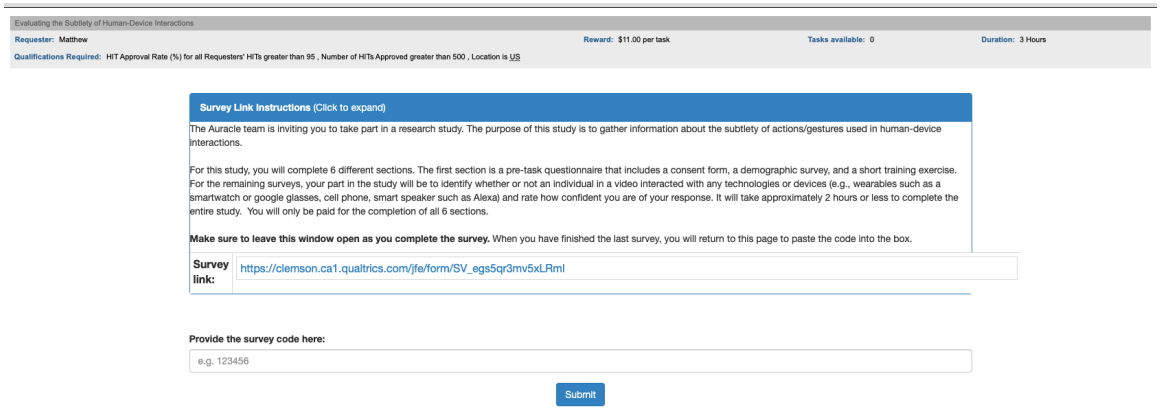


Figure 62. Recruitment Flyer Used On Amazon Mechanical Turk For Study 4

Information about Being in a Research Study
Clemson University

Title of Study: Evaluating the Subtlety of Human-Device Interactions

Description of the Study and Your Part in It
Clemson University and Dartmouth College are inviting you to take part in a research study. The purpose of this study is to gather information about the subtlety of actions/gestures used in human-device interactions.

Your part in the study will be to identify whether or not an individual in a video interacted with any technologies or devices (e.g., wearable such as smart watch or google glasses, cell phone, smart speaker such as Alexa) and rate how confident you are of your response.

It will take approximately 90 minutes to complete this study.

Risks and Discomforts
We do not know of any risks or discomforts to you in this research study.

Possible Benefits
While you may not benefit directly from taking part in the study, it is possible you will learn about the subtlety of actions performed in communicating with a wearable device. Additionally, this research may help us enable private and discrete communication in human-device interactions.

Incentives
After completing the experiment, you will be compensated $11.00 for your participation via the MTurk website, according to the reward per assignment listed on the MTurk website. Note that credit for taking the survey won't be given if you do not complete all 6 sections in the experiment or if you fail more two or more attention check questions.

After the questionnaire is completed you will see a code on the last page of the survey, which is a valid proof-of-work. You will need to submit the code on Mechanical Turk to receive $11.00.

Protection of Privacy and Confidentiality
We will not tell anyone outside of the research team of your participation in this study or what information we collect about you in particular. No sensitive information will be requested and information collected will be securely stored. The National Science Foundation (NSF), as the founder of this project, might have access to the study data and conclusive results of this research. Your identity will not be revealed in any publication or presentation that might result from this study.

Choosing to Be in the Study You do not have to be in this study. You may choose not to take part and you may choose to stop taking part at any time. You will not be punished in any way if

Figure 63. Informed Consent For Study 4 (page 1)

you decide not to be in the study or to stop taking part in the study. **Contact Information** If you have any questions or concerns about this study or if any problems arise, please contact Clemson University Hatlab at clemsonhatlab@gmail.com or the Clemson University Office of Research Compliance (ORC) at irb@clemson.edu.

Clicking on the "agree" button indicates that:
• You have read the above information
• You voluntarily agree to participate
• You are at least 18 years of age

- ○ I agree and I would like to participate in this study
- ○ I disagree and I would not like to participate in this study

Skip To: End of Survey If Information about Being in a Research Study Clemson University Title of Study: Evaluating the... = I disagree and I would not like to participate in this study

---

Start of Block: Sub Profile Survey

What is your gender?

- ○ Male
- ○ Female
- ○ Other
- ○ I prefer not to answer

Figure 64. Informed Consent For Study 4 (page 2)

What is your age?

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55+

What is your ethnicity?

- ○ White
- ○ Black or African American
- ○ American Indian or Alaska Native
- ○ Asian
- ○ Native Hawaiian or Pacific Islander
- ○ Other

Which of the following best describes your current employer

- ○ Government
- ○ Educational Institution
- ○ Business or industry
- ○ Non-profit organization
- ○ Other

Page 3 of 16

Figure 65. Pre-Survey Demographic Questionnaire For Study 4 (page 2)

What is the highest level of school you have completed or the highest degree you have received?

- ○ High school incomplete or less
- ○ High school graduate or GED (includes technical/vocational training that doesn't count towards college credit)
- ○ Some college (some community college, associate's degree)
- ○ Four year college degree/bachelor's degree
- ○ Some postgraduate or professional schooling, no postgraduate degree
- ○ Postgraduate or professional degree, including master's doctorate, medical or law degree
- ○ I prefer not to answer

Which of the following best describes you?

- ○ Married
- ○ Living with a partner
- ○ Divorced
- ○ Seperated
- ○ Widowed
- ○ Never been married
- ○ I prefer not to answer

Page 4 of 16

Figure 66. Pre-Survey Demographic Questionnaire For Study 4 (page 3)

Which of the following best describes your technology knowledge?

- Basic
- Intermediate
- Advanced
- Professional
- None

Do you own a wearable device (Fitbit, Apple Watch, blue-tooth enabled earbuds, wireless bone conduction headphones)?

- Yes
- No

Display This Question:

If Do you own a wearable device (Fitbit, Apple Watch, blue-tooth enabled earbuds, wireless bone cond... = No

Do you have an interest in using a head-mounted wearable device (Fitbit, Apple Watch, blue-tooth earbuds, wireless bone conduction headphones.)?

- Yes
- No

Page 5 of 16

Figure 67. Pre-Survey Demographic Questionnaire For Study 4 (page 4)

Privacy means different things to different people today. In thinking about all of your daily interactions-both online and offline-please tell us how important each of the following are to you:

	Not at all Important	Not very Important	Somewhat Important	Very Important	I do not know
Being in control of who can get information about you.	○	○	○	○	○
Being able to share confidential matters with someone you trust	○	○	○	○	○
Not having someone watch or listen to you without your permission	○	○	○	○	○
Controlling what information is collected about you	○	○	○	○	○
Being able to have times when you are completely alone, away from anyone else.	○	○	○	○	○
Having individuals in social/work situations not ask you things that are highly personal	○	○	○	○	○
Being able to go around in public without	○	○	○	○	○

Page 6 of 16

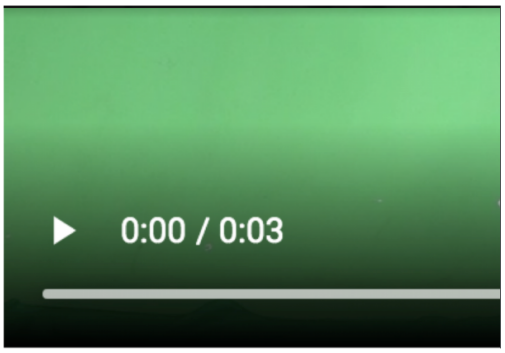
Figure 68. Pre-Survey Demographic Questionnaire For Study 4 (page 5)

always being identified					
Not being monitored at work.	○	○	○	○	○
Not being disturbed at home	○	○	○	○	○

Instructions

First, please watch each video clip. Play the video clip by clicking the play button. You may watch the video clip again as many times as you want.

If the video does not automatically play, please click the play button.



(This image shows what the video player looks like. To play the video, press the play button)

Figure 69. Pre-Survey Demographic Questionnaire For Study 4 (page 6) + Training Instructions (page 1)

Next, answer the questions about the video clip.

Instructions

You should also indicate whether there were any issues with the video. Indicate “yes” if you notice an issue with the video, such as a missing portion or some malfunction with the video or “no” if there is not an issue with the video.

Instructions

You may re-read these instructions at any time by clicking the "Instructions" button in the questionnaire.

Page 8 of 16

Figure 70. Training Instructions For Study 4 (page 2)

Instructions

Now, let's do some training to make sure you understand the task. This part of the study will take about 4-5 minutes.

Start of Block: Training 1 Block

Was there an issue with video?

- ○ Yes
- ○ No

Did the person in the video take any action?

- ○ Yes
- ○ No

How confident are you about your response

- ○ Completely unconfident 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ Completely confident 7

Page 9 of 16

Figure 71. Training For Study 4 (page 1)

You are correct. The person in the video did a thumbs down action. Good Job!

Page Break

Describe the issue you experienced with the video?

_____

_____

_____

_____

_____

Skip To: End of Block If Condition: Describe the issue you expe... Is Not Empty. Skip To: End of Block.

End of Block: Training 1 Block

Start of Block: Training 2 Block

Was there an issue with video?

- ○ Yes
- ○ No

Did the person in the video take any action?

- ○ Yes
- ○ No

Figure 72. Training For Study 4 (page 2)

How confident are you about your response

- ○ Completely unconfident 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ Completely confident 7

You are correct. The person in the video did an thumbs up action. Great Job!

Describe the issue you experienced with the video.

_____

_____

_____

_____

_____

End of Block: Training 2 Block

Start of Block: Traing 2 CTRL Blocker

Was there an issue with video?

- ○ Yes
- ○ No

Figure 73. Training For Study 4 (page 3)

Skip To: Q24 If Instructions Instructions Was there an issue with video? = Yes

Please describe the issue with the video

_____

_____

_____

_____

_____

Page Break

Instructions

Did the person in the video take any action?

- ○ Yes
- ○ No

Figure 74. Training For Study 4 (page 4)

How confident are you about your response

- ○ Completely unconfident 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ Completely confident 7

Page Break

Figure 75. Training For Study 4 (page 5)

You are correct. The person in the video did not take any action. Good Job!

Skip To: End of Block If You are correct. The person in the video did not take any action. Good Job! Is Displayed

Page Break

Figure 76. Training For Study 4 (page 6)

End of Block: Traing 2 CTRL Blocker

Start of Block: Training Glitch Block

Was there an issue with the video?

- ○ Yes
- ○ No

Good Job! There was an issue with this video.
You are correct!. There was a issue with this video. Good job.

Please describe the issue with the video

_____

_____

_____

_____

_____

How confident are you about your response

- ○ Completely unconfident 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ Completely confident 7

Page 15 of 16

Figure 77. Training For Study 4 (page 7)

You have successfully completed the training portion of the study.
Please proceed to the next section of the study, where you will see the next series of videos, and answer similar questions as you did during training. There are a total of 6 sections, and a short questionnaire at the end that will ask you about the compensation for this study. After completing the the final questionnaire please make note of the confirmation code at the end.

○ Click to proceed

End of Block: EOF Tblock

Page 16 of 16

Figure 78. Training For Study 4 (page 8)

Instructions

First, please watch each video clip. Play the video clip by clicking the play button. You may watch the video clip again as many times as you want.

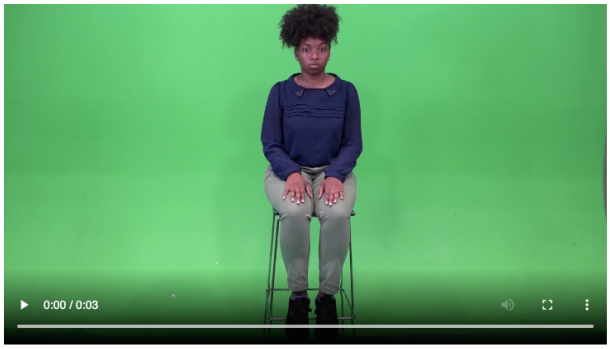
Next, answer the questions about the video clip.

Your task is to provide your opinion about whether the person in the video takes any action, as well as whether they are interacting with any technologies or devices (e.g., wearable such as smart watch or google glasses, cell phone, smart speaker such as Alexa).

Please note that the person in the video may be interacting with a technology or device, even if you do not see the technology or device.

You should also indicate whether there were any issues with the video. Indicate “yes” if you notice an issue with the video, such as a missing portion or some malfunction with the video or “no” if there is not an issue with the video.

Figure 79. Instructions For Study 4



Was there an issue with the video?

- Yes
- No

Skip To: BLKGlitch If Instructions First, please watch each video clip. Play the video clip by clicking the play button... = Yes

Display This Question:

If Instructions First, please watch each video clip. Play the video clip by clicking the play button... = Yes

*

Please describe the issue with the video.

_____

_____

_____

_____

_____

Page 2 of 5

Figure 80. Study 4 Experimental Stimuli(Issue With Video Question)

The person in the video took an action.

- Strongly Disagree 1
- 2
- 3
- 4
- 5
- 6
- Strongly Agree 7

Page 3 of 5

Figure 81. Study 4 Experimental Stimuli(Action Question)

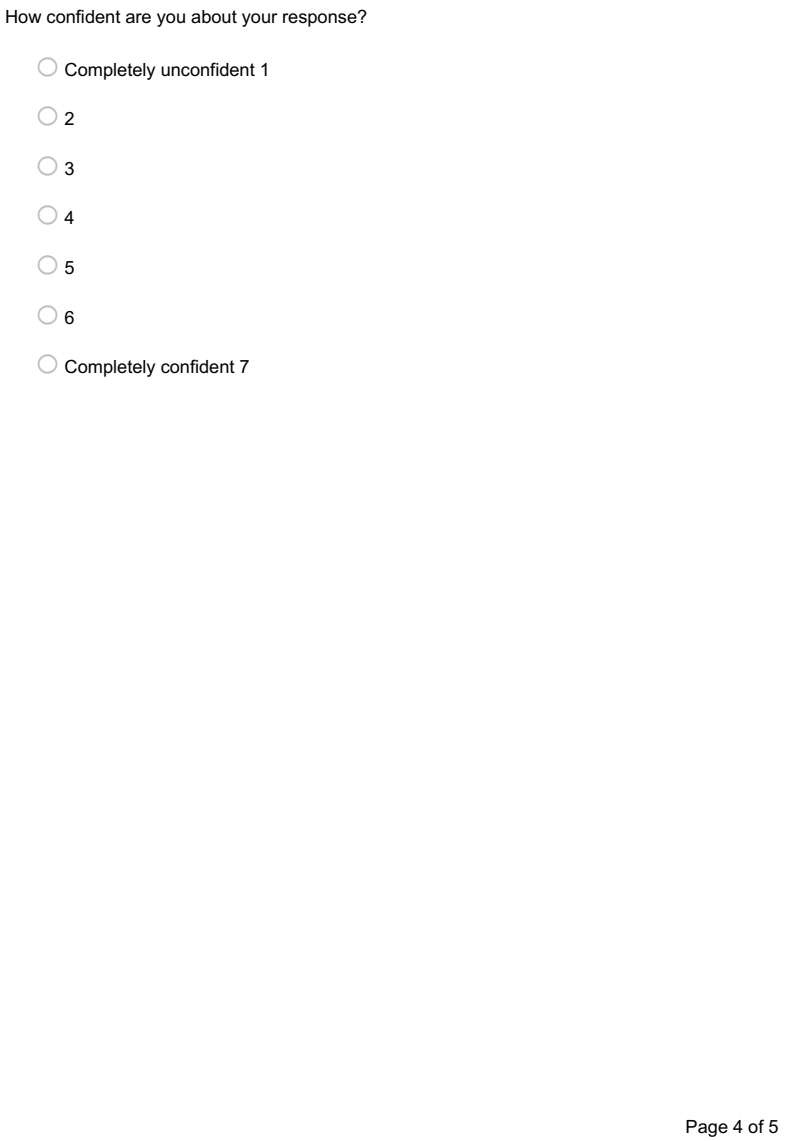
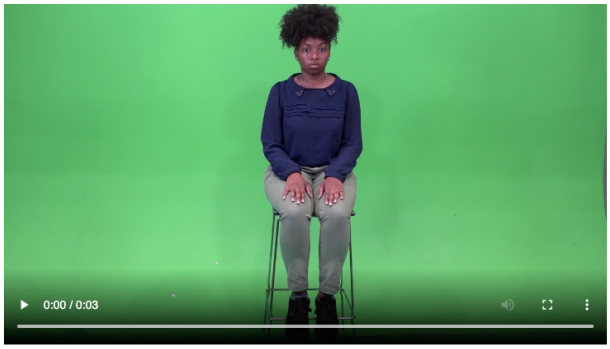


Figure 82. Study 4 Experimental Stimuli(Confidence of Action Question)



The person in the video interacted with technology and/or devices.

- ○ Strongly Disagree 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ Strongly Agree 7

Page 5 of 5

Figure 83. Study 4 Experimental Stimuli(Interaction Question)

Thank you for completing the first part of the study. The next part of the study should take approximately 10-15 minutes.

○ Click to proceed

In this section, you will be shown videos where you indicated that the person interacted with a technology/device. Please click to watch each video again.

Your task is to identify which part of the body the interaction primarily involved and describe the interaction.

Page 1 of 5

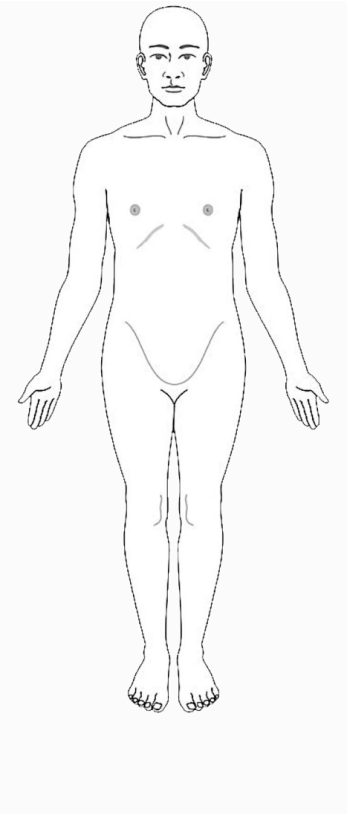
Figure 84. Study 4 Experimental Stimuli(Part 2 Page 1)

You reported that the person in the video interaction with a technology/device

=

Figure 85. Study 4 Experimental Stimuli(Part 2 Page 2)

Which part of the body did the interaction primarily involve? (please click the area to make your selection)



Page Break

Figure 86. Study 4 Experimental Stimuli(Part 2 Page 3)

Please describe the interaction you observed.

_____

_____

_____

_____

_____

Page Break

Figure 87. Study 4 Experimental Stimuli(Part 2 Page 4)

What kind of device/technology was the person in the video interacting with?

_____

_____

_____

_____

_____

Page 5 of 5

Figure 88. Study 4 Experimental Stimuli(Part 2 Page 5)

Congratulations! You have completed the final section of the experiment. Please proceed to answer two questions about compensation and your experience completing this experiment.

End of Block: Block 1

Start of Block: Compensation

The compensation for this task was fair.

- ○ Strongly Disagree
- ○ Disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Agree
- ○ Strongly agree

Was the compensation for this task fair? Please briefly explain why or why not?

_____

Page 1 of 1

Figure 89. Study 4 Compensation Question

Bibliography

[1] Fitbit community dashboard: Random friend requests?, May 2017.

[2] Guiding you through your privacy choices, Jan 2020.

[3] Cathy Russey . Wearables market projected to grow 137% by 2024, Aug 2020.

[4] M. Shankar A. Adams and H. Tecco. 50 things we now know about digital health consumers. `https://rockhealth.com/reports/digital-health-consumer-adoption-2016/`, November 2016.

[5] James D Abbey and Margaret G Meloy. Attention by design: Using attention checks to detect inattentive respondents and improve data quality. *Journal of Operations Management*, 53:63–70, 2017.

[6] Mohamed Abdelhamid, Joana Gaia, and G Lawrence Sanders. Putting the focus back on the patient: How privacy concerns affect personal health information sharing intentions. *Journal of medical Internet research*, 19(9), 2017.

[7] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*, pages 1–8, 1999.

[8] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International workshop on privacy enhancing technologies*, pages 36–58. Springer, 2006.

[9] Gabrielle Addonizio. The privacy risks surrounding consumer health and fitness apps, associated wearable devices, and hippa's limitations. 2016.

[10] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the ninth symposium on usable privacy and security*, pages 1–11, 2013.

[11] Idris Adjerid, Eyal Peer, and Alessandro Acquisti. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *Available at SSRN 2765097*, 2016.

[12] David Ahlström, Khalad Hasan, and Pourang Irani. Are you comfortable doing that?: acceptance studies of around-device gestures in and for public settings. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*, pages 193–202. ACM, 2014.

[13] Hamad Ahmed and Muhammad Tahir. Improving the accuracy of human body orientation estimation with wearable imu sensors. *IEEE Transactions on instrumentation and measurement*, 66(3):535–542, 2017.

[14] Sima Ajami and Fotooheh Teimouri. Features and application of wearable biosensors in medical care. *Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences*, 20(12):1208, 2015.

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

[16] Amr Alanwar, Moustafa Alzantot, Bo-Jhang Ho, Paul Martin, and Mani Srivastava. Selecon: Scalable iot device selection and control using hand gestures. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 47–58, 2017.

[17] Abdullah X Ali, Meredith Ringel Morris, and Jacob O Wobbrock. Crowdlicit: A system for conducting distributed end-user elicitation and identification studies. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[18] Linda Quinn Allen. The effects of emblematic gestures on the development and access of mental representations of french expressions. *The Modern Language Journal*, 79(4):521–529, 1995.

[19] Abdulmajeed Alqhatani and Heather Richter Lipford. "there is nothing that i need to keep secret": Sharing practices and concerns of wearable fitness data. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[20] Zakaria Alrababah. Privacy and security of wearable devices, 2020.

[21] Mayda Alrige and Samir Chatterjee. Toward a taxonomy of wearable technologies in healthcare. In *International Conference on Design Science Research in Information Systems*, pages 496–504. Springer, 2015.

[22] Florian Alt, Sabrina Geiger, and Wolfgang Höhl. Shapelineguide: Teaching mid-air gestures for large interactive displays. In *Proceedings of the 7th ACM International Symposium on Pervasive Displays*, pages 1–8, 2018.

[23] Irwin Altman. Privacy regulation: Culturally universal or culturally specific? *Journal of social issues*, 33(3):66–84, 1977.

[24] Brian Amento, Will Hill, and Loren Terveen. The sound of one hand: a wrist-mounted bio-acoustic fingertip gesture interface. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems*, pages 724–725, 2002.

[25] Fraser Anderson, Tovi Grossman, Daniel Wigdor, and George Fitzmaurice. Supporting subtlety with deceptive devices and illusory interactions. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1489–1498, 2015.

[26] Lisa Anthony, Quincy Brown, Jaye Nias, Berthel Tate, and Shreya Mohan. Interaction and recognition challenges in interpreting children's touch and gesture input on mobile devices. In *Proceedings of the 2012 ACM international conference on Interactive tabletops and surfaces*, pages 225–234, 2012.

[27] Shaikh Shawon Arefin Shimon, Courtney Lutton, Zichun Xu, Sarah Morrison-Smith, Christina Boucher, and Jaime Ruiz. Exploring non-touchscreen gestures for smartwatches. In *Proceedings of the 2016 chi conference on human factors in computing systems*, pages 3822–3833. ACM, 2016.

[28] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2):99–109, April 2015.

[29] Daniel Lee Ashbrook. *Enabling mobile microinteractions*. PhD thesis, Georgia Institute of Technology, 2010.

[30] Eric R Bachmann, Xiaoping Yun, and Robert B McGhee. Sourceless tracking of human posture using small inertial/magnetic sensors. In *Proceedings 2003 IEEE International Symposium on Computational Intelligence in Robotics and Automation. Computational Intelligence in Robotics and Automation for the New Millennium (Cat. No. 03EX694)*, volume 2, pages 822–829. IEEE, 2003.

[31] Karla Badillo-Urquiola, Xinru Page, and Pamela Wisniewski. Literature review: Examining contextual integrity within human-computer interaction. *Available at SSRN 3309331*, 2018.

[32] Gilles Bailly, JöRg MüLler, and Eric Lecolinet. Design and evaluation of finger-count interaction: Combining multitouch gestures and menus. *International Journal of Human-Computer Studies*, 70(10):673–689, 2012.

[33] Rebecca Balebako. *Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice*. PhD thesis, Carnegie Mellon University, 2014.

[34] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. " little brothers watching you" raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–11, 2013.

[35] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. The impact of timing on the salience of smartphone app privacy notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 63–74, 2015.

[36] G Bally, J Müller, M Rohs, D Wigdor, and S Kratz. Shoesense: a new perspective on hand gestures and wearable applications. In *Proc. CHI*, volume 12, 2012.

[37] Syagnik Banerjee, Thomas Hemphill, and Phil Longstreet. Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, 34(1), 2018.

[38] Debjanee Barua, Judy Kay, and Cécile Paris. Viewing and controlling personal sensor data: what do users want? In *International Conference on Persuasive Technology*, pages 15–26. Springer, 2013.

[39] Moritz Becker, Christian Matt, Thomas Widjaja, and Thomas Hess. Understanding privacy risk perceptions of consumer health wearables–an empirical taxonomy. 2017.

[40] Abdelkareem Bedri, Richard Li, Malcolm Haynes, Raj Prateek Kosaraju, Ishaan Grover, Temiloluwa Prioleau, Min Yan Beh, Mayank Goel, Thad Starner, and Gregory Abowd. Earbit: Using wearable sensors to detect eating episodes in unconstrained environments. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):37, 2017.

[41] Sebastian Benthall, Seda Gürses, Helen Nissenbaum, et al. *Contextual integrity through the lens of computer science*. Now Publishers, 2017.

[42] Ceylan Beşevli, Oğuz Turan Buruk, Merve Erkaya, and Oğuzhan Özcan. Investigating the effects of legacy bias: User elicited gestures from the end users perspective. In *Proceedings of the 2018 ACM Conference Companion Publication on Designing Interactive Systems*, pages 277–281, 2018.

[43] Shengjie Bi, Tao Wang, Nicole Tobias, Josephine Nordrum, Shang Wang, George Halvorsen, Sougata Sen, Ronald Peterson, Kofi Odame, Kelly Caine, et al. Auracle: Detecting eating episodes with an ear-mounted sensor. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–27, 2018.

[44] Ahmet Börütecene, Idil Bostan, Ekin Akyürek, Alpay Sabuncuoglu, Ilker Temuzkusu, Çaglar Genç, Tilbe Göksun, and Oguzhan Özcan. Through the glance mug: A familiar artefact to support opportunistic search in meetings. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*, pages 674–683, 2018.

[45] Jana Bressem and Silva H Ladewig. Rethinking gesture phases: Articulatory features of gestural movement? *Semiotica*, 2011(184):53–91, 2011.

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

[47] US Census Bureau. Educational attainment in the united states: 2019, Mar 2020.

[48] Attaullah Buriro, Rutger Van Acker, Bruno Crispo, and Athar Mahboob. Airsign: a gesture-based smartwatch user authentication. In *2018 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5. IEEE, 2018.

[49] Kelly Caine. Privacy is healthy. *IEEE Pervasive Computing*, 15(4):14–19, 2016.

[50] Kelly Caine and Rima Hanania. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, 20(1):7–15, 2012.

[51] Kelly Caine and Rima Hanania. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, 20(1), 2013.

[52] Kelly Erinn Caine. Exploring everyday privacy behaviors and misclosures. 2009.

[53] Jean Camp and Kay Connelly. *Beyond consent: privacy in ubiquitous computing (Ubicomp)*. Auerbach Publications, 2007.

[54] Marta E Cecchinato, Anna L Cox, and Jon Bird. Smartwatches: the good, the bad and the ugly? In *Proceedings of the 33rd Annual ACM Conference extended abstracts on human factors in computing systems*, pages 2133–2138. ACM, 2015.

[55] Pew Research Center. Pew research center demographic question, May 2015. `http://assets.pewresearch.org/wp-content/uploads/sites/12/2015/03/Demographic-Questions-Web-and-Mail-English-3-20-2015.pdf`.

[56] Edwin Chan, Teddy Seyed, Wolfgang Stuerzlinger, Xing-Dong Yang, and Frank Maurer. User elicitation on single-hand microgestures. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3403–3414. ACM, 2016.

[57] Liwei Chan, Rong-Hao Liang, Ming-Chang Tsai, Kai-Yin Cheng, Chao-Huai Su, Mike Y Chen, Wen-Huang Cheng, and Bing-Yu Chen. Fingerpad: private and subtle interaction using fingertips. In *Proceedings of the 26th annual ACM symposium on User interface software and technology*, pages 255–260, 2013.

[58] Marie Chan, Daniel Estève, Jean-Yves Fourniols, Christophe Escriba, and Eric Campo. Smart wearable systems: Current status and challenges. *Artificial intelligence in medicine*, 56(3):137–156, 2012.

[59] Younghoon Chang, Siew Fan Wong, and Hwansoo Lee. Understanding perceived privacy: A privacy boundary management model. In *PACIS*, page 78, 2015.

[60] Zhen Chen, Xiaochi Ma, Zeya Peng, Ying Zhou, Mengge Yao, Zheng Ma, Ci Wang, Zaifeng Gao, and Mowei Shen. User-defined gestures for gestural interaction: extending from hands to other body parts. *International Journal of Human–Computer Interaction*, 34(3):238–250, 2018.

[61] Eun-Jung Choi, Sung-Hyuk Kwon, Dong-Hun Lee, Ho-Jin Lee, and Min-K Chung. Design of hand gestures for smart home appliances based on a user centered approach. *Journal of Korean Institute of Industrial Engineers*, 38(3):182–190, 2012.

[62] Eric Y Chow, Milton M Morris, and Pedro P Irazoqui. Implantable rf medical devices: The benefits of high-speed communication and much greater communication distances in biomedical applications. *IEEE Microwave Magazine*, 14(4):64–73, 2013.

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

[64] Chia-Fang Chung, Nanna Gorm, Irina A Shklovski, and Sean Munson. Finding the right fit: understanding health tracking in workplace wellness programs. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 4875–4886. ACM, 2017.

[65] Andrea Civan, Meredith M Skeels, Anna Stolyar, and Wanda Pratt. Personal health information management: consumers' perspectives. In *AMIA Annual Symposium Proceedings*, volume 2006, page 156. American Medical Informatics Association, 2006.

[66] Jacob Cohen. *Statistical power analysis for the behavioral sciences (2nd ed.* 1988.

[67] Andrea Colaço, Ahmed Kirmani, Hye Soo Yang, Nan-Wei Gong, Chris Schmandt, and Vivek K Goyal. Mime: compact, low power 3d gesture sensing for interaction with head mounted displays. In *Proceedings of the 26th annual ACM symposium on User interface software and technology*, pages 227–236, 2013.

[68] Federal Trade Commission et al. Mobile privacy disclosures: Building trust through transparency. *USA: Federal Trade Commission*, 2013.

[69] Federal Trade Commission et al. Internet of things: Privacy & security in a connected world. *Washington, DC: Federal Trade Commission*, 2015.

[70] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: why, when, & what people want to share. In

Proceedings of the SIGCHI conference on Human factors in computing systems, pages 81–90. ACM, 2005.

[71] Alissa Cooper, Hannes Tschofenig, Bernard Aboba, Jon Peterson, J Morris, Marit Hansen, and Rhys Smith. Privacy considerations for internet protocols. Technical report, 2013.

[72] Alissa Cooper, Hannes Tschofenig, Bernard Aboba, Jon Peterson, J Morris, Marit Hansen, and Rhys Smith. Privacy considerations for internet protocols. *Internet Architecture Board*, 2013.

[73] Jason J Corso, Guangqi Ye, and Gregory D Hager. Analysis of composite gestures with a coherent probabilistic graphical model. *Virtual Reality*, 8(4):242–252, 2005.

[74] Nathan Cortez. The mobile health revolution. *UCDL Rev.*, 47:1173, 2013.

[75] Enrico Costanza, Samuel A Inverso, and Rebecca Allen. Toward subtle intimate interfaces for mobile devices using an emg controller. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 481–489, 2005.

[76] Enrico Costanza, Samuel A Inverso, Rebecca Allen, and Pattie Maes. Intimate interfaces in action: Assessing the usability and subtlety of emg-based motionless gestures. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 819–828, 2007.

[77] Enrico Costanza, Samuel A Inverso, Rebecca Allen, and Pattie Maes. Intimate interfaces in action: Assessing the usability and subtlety of emg-based motionless gestures. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 819–828. ACM, 2007.

[78] Enrico Costanza, Samuel A Inverso, Elan Pavlov, Rebecca Allen, and Pattie Maes. Eye-q: Eyeglass peripheral display for subtle intimate notifications. In *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, pages 211–218, 2006.

[79] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.", 2005.

[80] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 13(2):135–178, 2006.

[81] Paul D'alessandro and Trine Tsouderos. Health wearables: Early days.

[82] Lavinia Andreea Danielescu. *Discoverable Free Space Gesture Sets for Walk-up-and-use Interactions*. PhD thesis, Arizona State University, 2019.

[83] Reece Dano. Health and fitness wearables: Affecting healthy behaviors, moving beyond fashion, 2015.

[84] Prerit Datta, Akbar Siami Namin, and Moitrayee Chatterjee. A survey of privacy concerns in wearable devices. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 4549–4553. IEEE, 2018.

[85] Fred D Davis. *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. PhD thesis, Massachusetts Institute of Technology, 1985.

[86] Fred D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[87] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. User acceptance of computer technology: A comparison of two theoretical models. *Management science*, 35(8):982–1003, 1989.

[88] Michelle De Mooy and Shelten Yuen. Towards privacy-aware research and development in wearable health. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[89] Judith DeCew. Privacy. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2015 edition, 2015.

[90] Juan Deng, Yan Wang, Shu Zhao, Lei Wang, Yunjie Tian, and Hong Sha. A full-implantable continuous blood glucose monitoring system design. In *Proceedings of the 2019 9th International Conference on Biomedical Engineering and Technology*, pages 240–247, 2019.

[91] Roberto Di Pietro and Luigi V Mancini. Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, 46(9):74–79, 2003.

[92] Christine Dierk, Scott Carter, Patrick Chiu, Tony Dunnigan, and Don Kimber. Use your head! exploring interaction modalities for hat technologies. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, pages 1033–1045. ACM, 2019.

[93] Nem Khan Dim, Chaklam Silpasuwanchai, Sayan Sarcar, and Xiangshi Ren. Designing mid-air tv gestures for blind people using user-and choice-based elicitation approaches. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, pages 204–214. ACM, 2016.

[94] Tilman Dingler, Rufat Rzayev, Alireza Sahami Shirazi, and Niels Henze. Designing consistent gestures across device types: eliciting rsvp controls for phone, watch, and glasses. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 419. ACM, 2018.

[95] Catherine Dinh-Le, Rachel Chuang, Sara Chokshi, and Devin Mann. Wearable health technology and electronic health record integration: Scoping review and future directions. *JMIR mHealth and uHealth*, 7(9):e12861, 2019.

[96] Bruce H Dobkin. Wearable motion sensors to continuously measure real-world physical activities. *Current opinion in neurology*, 26(6), 2013.

[97] Guishan Dong, Yuxiang Chen, Jia Fan, Dijun Liu, Yao Hao, and Zhen Wang. A privacy-user-friendly scheme for wearable smart sensing devices based on blockchain. In *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 481–486. IEEE, 2018.

[98] Steven Dow, Blair MacIntyre, Jaemin Lee, Christopher Oezbek, Jay David Bolter, and Maribeth Gandy. Wizard of oz support throughout an iterative design process. *IEEE Pervasive Computing*, 4(4):18–26, 2005.

[99] Stuart Dredge. Why the workplace of 2016 could echo orwell's 1984. *The Guardian*, 2015.

[100] Ann Hill Duin, Diane Willow, Julianna Abel, Aaron Doering, Lucy Dunne, and Maki Isaka. Exploring the future of wearables and embodied computing: A report on interdisciplinary collaboration. In *2018 IEEE International Professional Communication Conference (ProComm)*, pages 47–50. IEEE, 2018.

[101] Lucy Dunne, Halley Profita, and Clint Zeagler. Social aspects of wearability and interaction. In *Wearable Sensors*, pages 25–43. Elsevier, 2014.

[102] Nathan Eagle and Alex Pentland. Wearables in the workplace: Sensing interactions at the office. In *ISWC*, pages 256–257, 2003.

[103] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. Timing is everything? the effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 319–328, 2009.

[104] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 319–328. ACM, 2009.

[105] Omar F El-Gayar, Loknath Sai Ambati, and Nevine Nawar. Wearables, artificial intelligence, and the future of healthcare. In *AI and Big Data's Potential for Disruptive Innovation*, pages 104–129. IGI Global, 2020.

[106] Dennis Ellis, Tony Kennedy, Vamsi Pasupuleti, Adam Williams, and Yalu Ye. Strive: student-athletes transitioning with camaraderie and competition. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, pages 2585–2590. ACM, 2013.

[107] Daniel A Epstein, Alan Borning, and James Fogarty. Fine-grained sharing of sensed physical activity: a value sensitive approach. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, pages 489–498. ACM, 2013.

[108] Daniel A Epstein, Bradley H Jacobson, Elizabeth Bales, David W McDonald, and Sean A Munson. From nobody cares to way to go!: A design framework for social sharing in personal

informatics. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pages 1622–1636. ACM, 2015.

[109] Augusto Esteves, Eduardo Velloso, Andreas Bulling, and Hans Gellersen. Orbits: Gaze interaction for smart watches using smooth pursuit eye movements. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, pages 457–466, 2015.

[110] Kelly R Evenson, Michelle M Goto, and Robert D Furberg. Systematic review of the validity and reliability of consumer-wearable activity trackers. *International Journal of Behavioral Nutrition and Physical Activity*, 12(1):159, 2015.

[111] Xenofon Fafoutis, Letizia Marchegiani, Georgios Z Papadopoulos, Robert Piechocki, Theo Tryfonas, and George Oikonomou. Privacy leakage of physical activity levels in wireless embedded wearable systems. *IEEE Signal Processing Letters*, 24(2):136–140, 2016.

[112] Yasmin Felberbaum and Joel Lanir. Better understanding of foot gestures: An elicitation study. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 334. ACM, 2018.

[113] Michela Ferron, Nadia Mana, Ornella Mich, Leonardo Badino, and Ryad Benosman. Designing, implementing and evaluating mid-air gestures and speech-based interaction. In *Proceedings of the 12th Biannual Conference on Italian SIGCHI Chapter*, pages 1–3, 2017.

[114] Org. for Econ. Co-operation & Dev. Oecd guidelines on the protection of privacy and transborder flows of personal data, 1980.

[115] Batya Friedman, Peter H Kahn, Alan Borning, and Alina Huldtgren. Value sensitive design and information systems. In *Early engagement and new technologies: Opening up the laboratory*, pages 55–95. Springer, 2013.

[116] Nico H Frijda et al. *The emotions*. Cambridge University Press, 1986.

[117] Thomas Fritz, Elaine M Huang, Gail C Murphy, and Thomas Zimmermann. Persuasive technology in the real world: a study of long-term use of activity sensing devices for fitness. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 487–496. ACM, 2014.

[118] Sandra Gabriele and Sonia 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*, pages 1–12, 2020.

[119] Lingling Gao and Xuesong Bai. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, 2014.

[120] Susan A Gelman and Cristine H Legare. Concepts and folk theories. *Annual review of anthropology*, 40:379–398, 2011.

[121] Vivian Genaro Motti and Kelly Caine. An overview of wearable applications for healthcare: requirements and challenges. In *UbiComp/ISWC'15 Adjunct*. ACM, 2015.

[122] Bogdan-Florin Gheran, Jean Vanderdonckt, and Radu-Daniel Vatavu. Gestures for smart rings: Empirical results, insights, and design implications. In *Proceedings of the 2018 Designing Interactive Systems Conference*, pages 623–635. ACM, 2018.

[123] Alan Godfrey, Victoria Hetherington, H Shum, Paolo Bonato, NH Lovell, and S Stuart. From a to z: Wearable technology explained. *Maturitas*, 113:40–47, 2018.

[124] Alan Godfrey, Victoria Hetherington, Hubert Shum, Paolo Bonato, NH Lovell, and S Stuart. From a to z: Wearable technology explained. *Maturitas*, 113:40–47, 2018.

[125] Erving Goffman et al. The presentation of self in everyday life. 1959. *Garden City, NY*, 259, 2002.

[126] Malarie Gokey. Smart earrings pack all the functionality of a fitness band into a tiny stud, Nov 2014.

[127] Jun Gong, Yu Wu, Lei Yan, Teddy Seyed, and Xing-Dong Yang. Tessutivo: Contextual interactions on interactive fabrics with inductive sensing. In *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*, pages 29–41, 2019.

[128] Jun Gong, Xing-Dong Yang, and Pourang Irani. Wristwhirl: One-handed continuous smartwatch input using wrist gestures. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*, pages 861–872, 2016.

[129] Nathaniel S Good, Jens Grossklags, Deirdre K Mulligan, and Joseph A Konstan. Noticing notice: a large-scale experiment on the timing of software license agreements. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 607–616, 2007.

[130] Nathaniel S Good and Aaron Krekelberg. Usability and privacy: a study of kazaa p2p file-sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 137–144, 2003.

[131] Nanna Gorm and Irina Shklovski. Sharing steps in the workplace: Changing privacy concerns over time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4315–4319. ACM, 2016.

[132] Nanna Gorm and Irina Shklovski. Steps, choices and moral accounting: Observations from a step-counting campaign in the workplace. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 148–159. ACM, 2016.

[133] Xinning Gui, Yu Chen, Clara Caldeira, Dan Xiao, and Yunan Chen. When fitness meets social networks: Investigating fitness tracking and social practices on werun. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 1647–1659, 2017.

[134] Katrina Guido and Asimina Kiourti. Wireless wearables and implants: A dosimetry review. *Bioelectromagnetics*, 41(1):3–20, 2020.

[135] Richard F Gunst and Robert L Mason. Fractional factorial design. *Wiley Interdisciplinary Reviews: Computational Statistics*, 1(2):234–244, 2009.

[136] Fangfang Guo, Yu Li, Mohan S Kankanhalli, and Michael S Brown. An evaluation of wearable activity monitoring devices. In *Proceedings of the 1st ACM international workshop on Personal data meets distributed multimedia*, pages 31–34. ACM, 2013.

[137] Petrus Guriting and Nelson Oly Ndubisi. Borneo online banking: evaluating customer perceptions and behavioural intention. *Management research news*, 2006.

[138] Hooman Hafezi, Timothy L Robertson, Greg D Moon, Kit-Yee Au-Yeung, Mark J Zdeblick, and George M Savage. An ingestible sensor for measuring medication adherence. *IEEE Transactions on Biomedical Engineering*, 62(1):99–109, 2014.

[139] Loni Hagen. Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy. In *Proceedings of the 18th Annual International Conference on Digital Government Research*, pages 598–599. ACM, 2017.

[140] Cory Hallam and Gianluca Zanella. Wearable device data and privacy: A study of perception and behavior. *World*, 7(1), 2016.

[141] KD Harris. Privacy on the go: Recommendations for the mobile ecosystem. california department of justice, 2013.

[142] Chris Harrison, Hrvoje Benko, and Andrew D Wilson. Omnitouch: wearable multitouch interaction everywhere. In *Proceedings of the 24th annual ACM symposium on User interface software and technology*, pages 441–450, 2011.

[143] Chris Harrison and Scott E Hudson. Abracadabra: wireless, high-precision, and unpowered finger input for very small mobile devices. In *Proceedings of the 22nd annual ACM symposium on User interface software and technology*, pages 121–124. ACM, 2009.

[144] Jeremy Rosenberg Harry Brignull, Marc Miquel and James Offer. Dark patterns - user interfaces designed to trick people., 2015.

[145] Andrea Hartzler, Meredith M Skeels, Marlee Mukai, Christopher Powell, Predrag Klasnja, and Wanda Pratt. Sharing is caring, but not error free: Transparency of granular controls for sharing personal health information in social networks. In *AMIA Annual Symposium Proceedings*, volume 2011, page 559. American Medical Informatics Association, 2011.

[146] Yangyang He. Recommending privacy settings for internet-of-things. 2019.
[147] Jason Healey, Neal Pollard, and Beau Woods. The healthcare internet of things: rewards and risks. *Atlantic Council*, 2015.
[148] Jeffrey Heer and Michael Bostock. Crowdsourcing graphical perception: using mechanical turk to assess visualization design. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 203–212, 2010.
[149] Anne Marie Helm and Daniel Georgatos. Privacy and mhealth: how mobile health apps fit into a privacy framework not limited to hipaa. *Syracuse L. Rev.*, 64:131, 2014.
[150] Jose Mauro C Hernandez and Jose Afonso Mazzon. Adoption of internet banking: proposition and implementation of an integrated methodology approach. *International journal of bank marketing*, 2007.
[151] Josiah Hester, Travis Peters, Tianlong Yun, Ronald Peterson, Joseph Skinner, Bhargav Golla, Kevin Storer, Steven Hearndon, Kevin Freeman, Sarah Lord, et al. Amulet: An energy-efficient, multi-application wearable platform. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 216–229. ACM, 2016.
[152] Lynn Hoff, Eva Hornecker, and Sven Bertel. Modifying gesture elicitation: Do kinaesthetic priming and increased production reduce legacy bias? In *Proceedings of the TEI'16: Tenth International Conference on Tangible, Embedded, and Embodied Interaction*, pages 86–91, 2016.
[153] Kasper Hornbæk and Antti Oulasvirta. What is interaction? In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5040–5052, 2017.
[154] John J Horton, David G Rand, and Richard J Zeckhauser. The online laboratory: Conducting experiments in a real labor market. *Experimental economics*, 14(3):399–425, 2011.
[155] Steven Houben, Simon Perrault, and Marcos Serrano. Bonjour! greeting gestures for collocated interaction with wearables. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, pages 1146–1152. ACM, 2015.
[156] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 571–582. ACM, 2014.
[157] Giovanni Iachello and Jason Hong. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1(1):1–137, 2007.
[158] Robert SH Istepanian, Emil Jovanov, and YT Zhang. Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity. *IEEE Transactions on information technology in biomedicine*, 8(4):405–414, 2004.
[159] Girardin Jean-Louis, Daniel F Kripke, William J Mason, Jeffrey A Elliott, and Shawn D Youngstedt. Sleep estimation from wrist movement quantified by different actigraphic modalities. *Journal of neuroscience methods*, 105(2):185–191, 2001.
[160] Lei Jing, Zixue Cheng, Yinghui Zhou, Junbo Wang, and Tongjun Huang. Magic ring: A self-contained gesture input device on finger. In *Proceedings of the 12th International Conference on Mobile and Ubiquitous Multimedia*, pages 1–4, 2013.
[161] Haik Kalantarian and Majid Sarrafzadeh. Audio-based detection and evaluation of eating behavior using the smartwatch platform. *Computers in biology and medicine*, 65:1–9, 2015.
[162] Maria Karam et al. A taxonomy of gestures in human computer interactions. 2005.
[163] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3393–3402, 2013.
[164] Finn Kensing and Jeanette Blomberg. Participatory design: Issues and concerns. *Computer supported cooperative work (CSCW)*, 7(3-4):167–185, 1998.
[165] Don Kerr, Kerryn Butler-Henderson, and Tony Sahama. Security, privacy, and ownership issues with the use of wearable health technologies. *Managing Security Issues and the Hidden Dangers of Wearable Technologies*, page 161, 2016.

[166] Sumbul Khan and Bige Tunçer. Intuitive and effective gestures for conceptual architectural design: An analysis of user elicited hand gestures for 3d cad modeling. 2017.

[167] Dan J Kim, Donald L Ferrin, and H Raghav Rao. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems*, 44(2):544–564, 2008.

[168] Ju-Whan Kim, Han-Jong Kim, and Tek-Jin Nam. M. gesture: an acceleration-based gesture authoring system on multiple handheld and wearable devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 2307–2318, 2016.

[169] Jungsoo Kim, Jiasheng He, Kent Lyons, and Thad Starner. The gesture watch: A wireless contact-free gesture based wrist interface. In *Wearable Computers, 2007 11th IEEE International Symposium on*, pages 15–22. IEEE, 2007.

[170] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. Exploring privacy concerns about personal sensing. In *International Conference on Pervasive Computing*, pages 176–183. Springer, 2009.

[171] Bart P Knijnenburg and Alfred Kobsa. Making decisions about privacy: information disclosure in context-aware recommender systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, 3(3):1–23, 2013.

[172] Bart Piet Knijnenburg. *A user-tailored approach to privacy decision support*. PhD thesis, UC Irvine, 2015.

[173] Bart Piet Knijnenburg and Alfred Kobsa. Increasing sharing tendency without reducing satisfaction: Finding the best privacy-settings user interface for social networks. In *ICIS*, 2014.

[174] Alfred Kobsa and Maximilian Teltzrow. Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing and purchase behavior. In *International Workshop on Privacy Enhancing Technologies*, pages 329–343. Springer, 2004.

[175] Steven Komarov, Katharina Reinecke, and Krzysztof Z Gajos. Crowdsourcing performance evaluations of user interfaces. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 207–216, 2013.

[176] Anne Köpsel and Nikola Bubalo. Benefiting from legacy bias. *interactions*, 22(5):44–47, 2015.

[177] Danielle Kosecki. Ask fitbit: How can i keep my stats private?, Oct 2017.

[178] David Kotz, Carl A Gunter, Santosh Kumar, and Jonathan P Weiner. Privacy and security in mobile health: A research agenda. *Computer*, 49(6):22–30, 2016.

[179] David Kotz, Carl A Gunter, Santosh Kumar, and Jonathan P Weiner. Privacy and security in mobile health: a research agenda. *Computer*, 49(6):22–30, 2016.

[180] Daniel St Clair Kreitzberg, Stephanie L Dailey, Teresa M Vogt, Donald Robinson, and Yaguang Zhu. What is your fitness tracker communicating?: Exploring messages and effects of wearable fitness devices. *Qualitative Research Reports in Communication*, 17(1):93–101, 2016.

[181] Jacob Kröger. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In *IFIP International Internet of Things Conference*, pages 147–159. Springer, 2018.

[182] Jacob Leon Kröger, Philip Raschke, and Towhidur Rahman Bhuiyan. Privacy implications of accelerometer data: a review of possible inferences. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pages 81–87, 2019.

[183] Christine Kühnel, Tilo Westermann, Fabian Hemmert, Sven Kratz, Alexander Müller, and Sebastian Möller. I'm home: Defining and evaluating a gesture set for smart-home control. *International Journal of Human-Computer Studies*, 69(11):693–704, 2011.

[184] Vishakha Kumari and Sara Anne Hook. The privacy, security and discoverability of data on wearable health devices: Fitness or folly? In *International Conference on Universal Access in Human-Computer Interaction*, pages 50–64. Springer, 2017.

[185] Karen Lamb, Hsiao-Ying Huang, Andrew Marturano, and Masooda Bashir. Users' privacy perceptions about wearable technology: Examining influence of personality, trust, and usability. In *Advances in Human Factors in Cybersecurity*, pages 55–68. Springer, 2016.

[186] Paul Lamkin. Smartwatch popularity booms with fitness trackers on the slide. https://www.forbes.com/sites/paullamkin/2018/02/22/smartwatch-popularity-booms-with-fitness-trackers-on-the-slide/?sh=764db2397d96, February 2018.

[187] Marc Langheinrich. Privacy by design- principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[188] Marc Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[189] Frederic Lardinois. Google's atap is bringing its project soli radar sensor to smartwatches and speakers, May 2016.

[190] Linda Lee, J Lee, Serge Egelman, and David Wagner. Information disclosure concerns in the age of wearable computing. In *NDSS Workshop on Usable Security (USEC)*, volume 1, 2016.

[191] He Li, Jing Wu, Yiwen Gao, and Yao Shi. Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International journal of medical informatics*, 88:8–17, 2016.

[192] Xiaolong Li, Wouter A Serdijn, Wei Zheng, Yubo Tian, and Bing Zhang. The injectable neurostimulator: an emerging therapeutic device. *Trends in biotechnology*, 33(7):388–394, 2015.

[193] Yifang Li. Investigating obfuscation as a tool to enhance photo privacy on social networks sites. 2020.

[194] Yifang Li, Nishant Vishwamitra, Hongxin Hu, and Kelly Caine. Towards a taxonomy of content sensitivity and sharing preferences for photos. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[195] Jaime Lien, Nicholas Gillian, M Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, and Ivan Poupyrev. Soli: Ubiquitous gesture sensing with millimeter wave radar. *ACM Transactions on Graphics (TOG)*, 35(4):1–19, 2016.

[196] Robert Lindenberg, Marie Uhlig, Dag Scherfeld, Gottfried Schlaug, and Ruediger J Seitz. Communication with emblematic gestures: shared and distinct neural correlates of expression and reception. *Human brain mapping*, 33(4):812–823, 2012.

[197] E Lingg, G Leone, K Spaulding, and R Cardea B'Far. Cloud based employee health and wellness integrated wellness application with a wearable device and the hcm data store. In *Proceedings of the 2014 IEEE World Forum on Internet of Things*, pages 6–8, 2014.

[198] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in facebook with an audience view. *UPSEC*, 8:1–8, 2008.

[199] Christian Loclair, Sean Gustafson, and Patrick Baudisch. Pinchwatch: a wearable device for one-handed microinteractions. In *Proc. MobileHCI*, volume 10, 2010.

[200] A Chris Long Jr, James A Landay, Lawrence A Rowe, and Joseph Michiels. Visual similarity of pen gestures. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 360–367. ACM, 2000.

[201] Allan Christian Long Jr, James A Landay, and Lawrence A Rowe. Implications for a gesture design tool. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 40–47, 1999.

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

[203] Joseph Y Lucisano, Timothy L Routh, Joe T Lin, and David A Gough. Glucose monitoring in individuals with diabetes using a long-term implanted sensor/telemetry system and model. *IEEE transactions on biomedical engineering*, 64(9):1982–1993, 2016.

[204] Joanna Lumsden and Stephen Brewster. A paradigm shift: alternative interaction techniques for use with mobile & wearable devices. In *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*, pages 197–210. IBM Press, 2003.

[205] Deborah Lupton. Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, health & sexuality*, 17(4):440–453, 2015.

[206] Mary Madden and Lee Rainie. Americans' attitudes about privacy, security and surveillance, May 2015.
`http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/`.

[207] Angela Mahr, Christoph Endres, Christian Müller, and Tanja Schneeberger. Determining human-centered parameters of ergonomic micro-gesture interaction for drivers using the theater approach. In *Proceedings of the 3rd International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, pages 151–158, 2011.

[208] Ville Mäkelä, Johannes Kleine, Maxine Hood, Florian Alt, and Albrecht Schmidt. Hidden interaction techniques: Concealed information acquisition and texting on smartphones and wearables. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

[209] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[210] Steve Mann. Wearable computing: Toward humanistic intelligence. *IEEE Intelligent Systems*, 16(3):10–15, 2001.

[211] Mokhinabonu Mardonova and Yosoon Choi. Review of wearable device technology and its applications to the mining industry. *Energies*, 11(3):547, 2018.

[212] David Matsumoto and Hyisung C Hwang. Cultural similarities and differences in emblematic gestures. *Journal of Nonverbal Behavior*, 37(1):1–27, 2013.

[213] Keenan R May, Thomas M Gable, and Bruce N Walker. Designing an in-vehicle air gesture set using elicitation methods. In *Proceedings of the 9th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, pages 74–83. ACM, 2017.

[214] Justin McCarthy. One in five u.s. adults use health apps, wearable trackers, Apr 2020.

[215] Evelyn Z McClave. Linguistic functions of head movements in the context of speech. *Journal of pragmatics*, 32(7):855–878, 2000.

[216] Holly L McClung, Lauren T Ptomey, Robin P Shook, Anju Aggarwal, Anna M Gorczyca, Edward S Sazonov, Katie Becofsky, Rick Weiss, and Sai Krupa Das. Dietary intake and physical activity assessment: current tools, techniques, and technologies for use in adult populations. *American journal of preventive medicine*, 55(4):e93–e104, 2018.

[217] Rísin McNaney, John Vines, Daniel Roggen, Madeline Balaam, Pengfei Zhang, Ivan Poliakov, and Patrick Olivier. Exploring the acceptability of google glass as an everyday assistive device for people with parkinson's. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2551–2554. ACM, 2014.

[218] David McNeill. *Hand and mind: What gestures reveal about thought*. University of Chicago press, 1992.

[219] Vikram Mehta, Arosha K Bandara, Blaine A Price, and Bashar Nuseibeh. Wearables for physical privacy. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 942–945. ACM, 2016.

[220] Monika Mital, Victor Chang, Praveen Choudhary, Armando Papa, and Ashis K Pani. Adoption of internet of things in india: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change*, 136:339–346, 2018.

[221] Robb Mitchell. Sensing mine, yours, theirs, and ours: interpersonal ubiquitous interactions. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, pages 933–938. ACM, 2015.

[222] Calkin S Montero, Jason Alexander, Mark T Marshall, and Sriram Subramanian. Would you do that?: understanding social acceptance of gestural interfaces. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services*, pages 275–278. ACM, 2010.

[223] Jeff Montes, Tori M Stone, Jacob W Manning, Damon McCune, Debra K Tacad, John C Young, Mark DeBeliso, and James W Navalta. Using hexoskin wearable technology to obtain body metrics during trail hiking. *International journal of exercise science*, 8(4):425, 2015.

[224] Kathryn Montgomery, Jeff Cester, and Katharina Kopp. Health wearable devices in the big data era: Ensuring privacy, security, and consumer protection. *Centre for Digital Democracy Report*, 2016.

[225] Hawley E Montgomery-Downs, Salvatore P Insana, and Jonathan A Bond. Movement toward a novel activity monitoring device. *Sleep and Breathing*, 16(3), 2012.

[226] Meredith Ringel Morris. Web on the wall: insights from a multimodal interaction elicitation study. In *Proceedings of the 2012 ACM international conference on Interactive tabletops and surfaces*, pages 95–104. ACM, 2012.

[227] Meredith Ringel Morris, Andreea Danielescu, Steven Drucker, Danyel Fisher, Bongshin Lee, Jacob O Wobbrock, et al. Reducing legacy bias in gesture elicitation studies. *interactions*, 21(3):40–45, 2014.

[228] Meredith Ringel Morris, Jacob O Wobbrock, and Andrew D Wilson. Understanding users' preferences for surface gestures. In *Proceedings of graphics interface 2010*, pages 261–268. Canadian Information Processing Society, 2010.

[229] Steven A Morris and Thomas E Marshall. Perceived control in information systems. *Journal of Organizational and End User Computing (JOEUC)*, 16(2):38–56, 2004.

[230] Vivian Genaro Motti. Wearable interaction. In *Wearable Interaction*, pages 81–107. Springer, 2020.

[231] Vivian Genaro Motti and Kelly Caine. Human factors considerations in the design of wearable devices. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 58, pages 1820–1824. SAGE Publications Sage CA: Los Angeles, CA, 2014.

[232] Vivian Genaro Motti and Kelly Caine. Understanding the wearability of head-mounted devices from a human-centered perspective. In *Proceedings of the 2014 ACM International Symposium on Wearable Computers*, pages 83–86. ACM, 2014.

[233] Vivian Genaro Motti and Kelly Caine. Micro interactions and multi dimensional graphical user interfaces in the design of wrist worn wearables. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 59, pages 1712–1716. SAGE Publications Sage CA: Los Angeles, CA, 2015.

[234] Vivian Genaro Motti and Kelly Caine. Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*. Springer, 2015.

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

[236] Vivian Genaro Motti and Kelly Caine. Towards a visual vocabulary for privacy concepts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 60, pages 1078–1082. SAGE Publications Sage CA: Los Angeles, CA, 2016.

[237] Vivian Genaro Motti and Kelly Caine. Towards a visual vocabulary for privacy concepts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 60, pages 1078–1082. SAGE Publications Sage CA: Los Angeles, CA, 2016.

[238] Miguel A Nacenta, Yemliha Kamber, Yizhou Qiang, and Per Ola Kristensson. Memorability of pre-designed and user-defined gesture sets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1099–1108. ACM, 2013.

[239] Mark W Newman, Debra Lauterbach, Sean A Munson, Paul Resnick, and Margaret 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. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, pages 341–350. ACM, 2011.

[240] David H Nguyen and Elizabeth D Mynatt. Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems. 2002.

[241] Michael Nielsen, Moritz Störring, Thomas B Moeslund, and Erik Granum. A procedure for developing intuitive and ergonomic gesture interfaces for hci. In *International gesture workshop*, pages 409–420. Springer, 2003.

[242] Wendy Nilsen. The future of wearables in health. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 1–1. IEEE, 2020.

[243] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[244] Helen Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.

[245] Donald A Norman and Stephen W Draper. *User centered system design: New perspectives on human-computer interaction*. CRC Press, 1986.

[246] Future of Privacy Forum. `https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf`, 2016.

[247] Eyal Ofek, Shamsi T Iqbal, and Karin Strauss. Reducing disruption from subtle information delivery during a conversation: mode and bandwidth investigation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3111–3120, 2013.

[248] Masa Ogata and Michita Imai. Skinwatch: skin gesture interaction for smart watch. In *Proceedings of the 6th Augmented Human International Conference*, pages 21–24. ACM, 2015.

[249] Judith S Olson, Jonathan Grudin, and Eric Horvitz. A study of preferences for sharing and privacy. In *CHI'05 extended abstracts on Human factors in computing systems*, pages 1985–1988, 2005.

[250] Sharon Oviatt. Ten myths of multimodal interaction. *Communications of the ACM*, 42(11):74–81, 1999.

[251] M Pacelli, G Loriga, N Taccini, and R Paradiso. Sensing fabrics for monitoring physiological and biomechanical variables: E-textile solutions. In *2006 3rd IEEE/EMBS International Summer School on Medical Devices and Biosensors*, pages 1–4. IEEE, 2006.

[252] Leysia Palen and Paul Dourish. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, 2003.

[253] Jihun Park, Joohee Kim, So-Yun Kim, Woon Hyung Cheong, Jiuk Jang, Young-Geun Park, Kyungmin Na, Yun-Tae Kim, Jun Hyuk Heo, Chang Young Lee, et al. Soft, smart contact lenses with integrations of wireless circuits, glucose sensors, and displays. *Science advances*, 4(1):eaap9841, 2018.

[254] Kunwoo Park, Ingmar Weber, Meeyoung Cha, and Chul Lee. Persistent sharing of fitness app status on twitter. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 184–194, 2016.

[255] Sungmee Park and Sundaresan Jayaraman. Enhancing the quality of life through wearable technology. *IEEE Engineering in medicine and biology magazine*, 22(3):41–48, 2003.

[256] Sungmee Park and Sundaresan Jayaraman. Wearables: Fundamentals, advancements, and a roadmap for the future. In *Wearable sensors*, pages 3–27. Elsevier, 2021.

[257] Sameer Patil, Greg Norcie, Apu Kapadia, and Adam J Lee. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–15, 2012.

[258] Sameer Patil, Roman Schlegel, Apu Kapadia, and Adam J Lee. Reflection or action? how feedback and control affect location sharing decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 101–110, 2014.

[259] Andrew S Patrick and Steve Kenny. From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In *International Workshop on Privacy Enhancing Technologies*, pages 107–124. Springer, 2003.

[260] Greig Paul and James Irvine. Privacy implications of wearable health devices. In *Proceedings of the 7th International Conference on Security of Information and Networks*, pages 117–121, 2014.

[261] Jennifer Pearson, Simon Robinson, Matt Jones, Anirudha Joshi, Shashank Ahire, Deepak Sahoo, and Sriram Subramanian. Chameleon devices: investigating more secure and discreet mobile interactions via active camouflaging. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5184–5196. ACM, 2017.

[262] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[263] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. Reputation as a sufficient condition for data quality on amazon mechanical turk. *Behavior research methods*, 46(4):1023–1031, 2014.

[264] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. Reputation as a sufficient condition for data quality on amazon mechanical turk. *Behavior research methods*, 46(4):1023–1031, 2014.

[265] Scott R Peppet. Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93:85, 2014.

[266] Alfredo J Perez and Sherali Zeadally. Privacy issues and solutions for consumer wearables. *It Professional*, 20(4):46–56, 2017.

[267] Travis Peters. An assessment of single-channel emg sensing for gestural input. *Online: http://www. cs. dartmouth. edu/˜ traviswp/papers/TR/peters_emg_14. pdf diakses pada tanggal*, 3, 2014.

[268] Sandra Petronio. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

[269] Joshua M Pevnick, Kade Birkeland, Raymond Zimmer, Yaron Elad, and Ilan Kedan. Wearable technology for cardiology: an update and framework for the future. *Trends in cardiovascular medicine*, 28(2):144–150, 2018.

[270] Thammathip Piumsomboon, Adrian Clark, Mark Billinghurst, and Andy Cockburn. User-defined gestures for augmented reality. In *IFIP Conference on Human-Computer Interaction*, pages 282–299. Springer, 2013.

[271] L. Piwek, D.A. Ellis, S. Andrews, and A. Joinson. The rise of consumer health wearables: promises and barriers. *PLos Med*, 13:e1001953, February 2016.

[272] Henning Pohl, Andreea Muresan, and Kasper Hornbæk. Charting subtle interaction in the hci literature. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2019.

[273] Maija Poikela and Eran Toch. Understanding the valuation of location privacy: a crowdsourcing-based approach. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

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

[275] Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise Anthony, and David Kotz. Understanding user privacy preferences for mhealth data sharing. *mHealth: Multidisciplinary verticals*, pages 545–569, 2014.

[276] PricewaterhouseCoopers. The wearable life 2.0: Connected living in a wearable world, May 2016.

[277] Dmitry Pyryeskin, Mark Hancock, and Jesse Hoey. Comparing elicited gestures to designer-created gestures for selection above a multitouch surface. In *Proceedings of the 2012 ACM international conference on Interactive tabletops and surfaces*, pages 1–10, 2012.

[278] Francis Quek, David McNeill, Robert Bryll, Susan Duncan, Xin-Feng Ma, Cemil Kirbas, Karl E McCullough, and Rashid Ansari. Multimodal human discourse: gesture and speech. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 9(3):171–193, 2002.

[279] Emilee Rader. Awareness of behavioral tracking and information privacy concern in facebook and google. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 51–67, 2014.

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

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

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

[283] Leena Rao. Sexual activity tracked by fitbit shows up in google search results, Jul 2011.

[284] Blaine Reeder and Alexandria David. Health at hand: A systematic review of smart watch uses for health and wellness. *Journal of Biomedical Informatics*, 63:269–276, 2016.

[285] Mark D Reilly, Haifeng Shen, Paul R Calder, and Henry Been-Lirn Duh. Understanding the effects of discreet real-time social interaction on student engagement in lectures. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration*, pages 193–196, 2013.

[286] Katharina Reinecke and Krzysztof Z Gajos. Labinthewild: Conducting large-scale online experiments with uncompensated samples. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pages 1364–1378, 2015.

[287] Jun Rekimoto. Gesturewrist and gesturepad: Unobtrusive wearable interaction devices. In *Proceedings Fifth International Symposium on Wearable Computers*, pages 21–27. IEEE, 2001.

[288] Julie Rico. Evaluating the social acceptability of multimodal mobile interactions. In *CHI'10 Extended Abstracts on Human Factors in Computing Systems*, pages 2887–2890. 2010.

[289] Everett M Rogers. Diffusion of innovations the free press of glencoe. *NY*, 32:891–937, 1962.

[290] Megan E Rollo, Rebecca L Williams, Tracy Burrows, Sharon I Kirkpatrick, Tamara Bucher, and Clare E Collins. What are they really eating? a review on new approaches to dietary intake assessment and validation. *Current nutrition reports*, 5(4):307–314, 2016.

[291] Sirinthip Roomkham, Michael Hittle, Joseph Cheung, David Lovell, Emmanuel Mignot, and Dimitri Perrin. Sleep monitoring with the apple watch: comparison to a clinically validated actigraph. *F1000Research*, 8(754):754, 2019.

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

[293] Jaime Ruiz, Yang Li, and Edward Lank. User-defined motion gestures for mobile interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 197–206. ACM, 2011.

[294] Jaime Ruiz and Daniel Vogel. Soft-constraints to reduce legacy and performance bias to elicit whole-body gestures with low arm fatigue. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 3347–3350, 2015.

[295] T Scott Saponas, Desney S Tan, Dan Morris, Ravin Balakrishnan, Jim Turner, and James A Landay. Enabling always-available input with muscle-computer interfaces. In *Proceedings of the 22nd annual ACM symposium on User interface software and technology*, pages 167–176, 2009.

[296] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. Designing effective privacy notices and controls. *IEEE Internet Computing*, 2017.

[297] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, 2015.

[298] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 1–17, 2015.

[299] Florian Schaub, Bastian Könings, and Michael Weber. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, 14(1):34–43, 2015.

[300] Florian Marcus Schaub. *Dynamic privacy adaptation in ubiquitous computing*. PhD thesis, Universität Ulm, 2014.

[301] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. Understanding the impact of information representation on willingness to share information. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2019.

[302] Stefan Schneegass and Alexandra Voit. Gesturesleeve: using touch sensitive fabrics for gestural input on the forearm for controlling smartwatches. In *Proceedings of the 2016 ACM International Symposium on Wearable Computers*, pages 108–115, 2016.

[303] Douglas Schuler and Aki Namioka. *Participatory design: Principles and practices*. CRC Press, 1993.

[304] Charles E. Schumer. Schumer reveals: Without their knowledge, fitbit bracelets amp; smartphone apps are tracking users movements and health data that could be sold to third parties; calls for ftc to require mandatory opt-out opportunity before any personal data can be sold, Aug 2014.

[305] B Schwartz and A Baca. Wearables and apps for health promotion.

[306] Marcos Serrano, Barrett M Ens, and Pourang P Irani. Exploring the use of hand-to-face input for interacting with head-worn displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 3181–3190. ACM, 2014.

[307] John J Shaughnessy, Eugene B Zechmeister, and Jeanne S Zechmeister. *Research methods in psychology*. McGraw-Hill, 2000.

[308] Hong Sheng, Fiona Fui-Hoon Nah, and Keng Siau. An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, 9(6):15, 2008.

[309] Shaikh Shawon Arefin Shimon, Sarah Morrison-Smith, Noah John, Ghazal Fahimi, and Jaime Ruiz. Exploring user-defined back-of-device gestures for mobile devices. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 227–232, 2015.

[310] Manya Sleeper, Justin Cranshaw, Patrick Gage Kelley, Blase Ur, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. " i read my twitter the next morning and was astonished" a conversational perspective on twitter regrets. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3277–3286, 2013.

[311] Liz Sly. U.s. soldiers are revealing sensitive and dangerous information by jogging, Jan 2018.

[312] Oleg Špakov and Päivi Majaranta. Enhanced gaze interaction using simple head gestures. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 705–710, 2012.

[313] Steven Spann. Wearable fitness devices: Personal health data privacy in washington state. *Seattle UL Rev.*, 39:1411, 2015.

[314] Thad Starner. The challenges of wearable computing: Part 2. *Ieee Micro*, 21, 2001.

[315] Thad Starner, Jake Auxier, Daniel Ashbrook, and Maribeth Gandy. The gesture pendant: A self-illuminating, wearable, infrared computer vision system for home automation control and medical monitoring. In *Wearable computers, the fourth international symposium on*, pages 87–94. IEEE, 2000.

[316] Matteo Stoppa and Alessandro Chiolerio. Wearable electronics and smart textiles: a critical review. *Sensors*, 14(7):11957–11992, 2014.

[317] Matteo Stoppa and Alessandro Chiolerio. Wearable electronics and smart textiles: a critical review. *Sensors*, 14(7), 2014.

[318] Jeroen Stragier, Tom Evens, and Peter Mechant. Broadcast yourself: an exploratory study of sharing physical activity on social networking sites. *Media International Australia*, 155(1):120–129, 2015.

[319] Melane Swan. Health 2050: The realization of personalized medicine through crowdsourcing, the quantified self, and the participatory biocitizen. *Journal of personalized medicine*, 2:93–118, 2012.

[320] Melanie Swan. Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. *International journal of environmental research and public health*, 6(2):492–525, 2009.

[321] Nasim Talebi, Cory Hallam, and Gianluca Zanella. The new wave of privacy concerns in the wearable devices era. In *2016 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 3208–3214. IEEE, 2016.

[322] Nasim Talebi, Cory Hallam, and Gianluca Zanella. The new wave of privacy concerns in the wearable devices era. In *2016 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 3208–3214, 2016.

[323] Karen Tang, Jason Hong, and Dan Siewiorek. The implications of offering more disclosure choices for social location sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 391–394, 2012.

[324] R Core Team et al. R: A language and environment for statistical computing. 2013.

[325] Rannie Teodoro and Mor Naaman. Fitter with twitter: Understanding personal health and fitness activity in social media. *ICWSM*, 2013:611–620, 2013.

[326] Richard P Troiano, David Berrigan, Kevin W Dodd, Louise C Masse, Timothy Tilert, and Margaret McDowell. Physical activity in the united states measured by accelerometer. *Medicine & Science in Sports & Exercise*, 40(1):181–188, 2008.

[327] Janice Y Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Location-sharing technologies: Privacy risks and controls. *Isjlp*, 6:119, 2010.

[328] Matthew Turk. Multimodal interaction: A review. *Pattern Recognition Letters*, 36:189–195, 2014.

[329] Emmanuel Sebastian Udoh and Abdulwahab Alkharashi. Privacy risk awareness and the behavior of smartwatch users: A case study of indiana university students. In *2016 Future Technologies Conference (FTC)*, pages 926–931. IEEE, 2016.

[330] Blase Ur and Yang Wang. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22nd International Conference on World Wide Web*, pages 755–762. ACM, 2013.

[331] Blase Ur and Yang Wang. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22nd International Conference on World Wide Web*, pages 755–762, 2013.

[332] Dirk Van Der Linden, Anna Zamansky, Irit Hadar, Barnaby Craggs, and Awais Rashid. Buddy's wearable is not your buddy: Privacy implications of pet wearables. *IEEE Security & Privacy*, 17(3):28–39, 2019.

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

[334] Jean Vanderdonckt, Nathan Magrofuoco, Suzanne Kieffer, Jorge Pérez, Ysabelle Rase, Paolo Roselli, and Santiago Villarreal. Head and shoulders gestures: Exploring user-defined gestures with upper body. In *International Conference on Human-Computer Interaction*, pages 192–213. Springer, 2019.

[335] Radu-Daniel Vatavu. User-defined gestures for free-hand tv control. In *Proceedings of the 10th European conference on Interactive tv and video*, pages 45–48. ACM, 2012.

[336] Radu-Daniel Vatavu and Jacob O Wobbrock. Formalizing agreement analysis for elicitation studies: New measures, significance test, and toolkit. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1325–1334. ACM, 2015.

[337] Radu-Daniel Vatavu and Ionut-Alexandru Zaiti. Leap gestures for tv: insights from an elicitation study. In *Proceedings of the ACM International Conference on Interactive Experiences for TV and Online Video*, pages 131–138, 2014.

[338] Viswanath Venkatesh and Fred D Davis. A model of the antecedents of perceived ease of use: Development and test. *Decision sciences*, 27(3):451–481, 1996.

[339] Viswanath Venkatesh and Michael G Morris. Why don't men ever stop to ask for directions? gender, social influence, and their role in technology acceptance and usage behavior. *MIS quarterly*, pages 115–139, 2000.

[340] Santiago Villarreal-Narvaez, Jean Vanderdonckt, Radu-Daniel Vatavu, and Jacob A Wobbrock. A systematic review of gesture elicitation studies: What can we learn from 216 studies. In *Proceedings of ACM Int. Conf. on Designing Interactive Systems (DIS'20)*, 2020.

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

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

[343] Emily A. Vogels. About one-in-five americans use a smart watch or fitness tracker.

[344] Panagiotis Vogiatzidakis and Panayiotis Koutsabasis. Gesture elicitation studies for mid-air interaction: A review. *Multimodal Technologies and Interaction*, 2(4):65, 2018.

[345] Isabel Wagner, Ying He, Duska Rosenberg, and Helge Janicke. User interface design for privacy awareness in ehealth technologies. In *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, pages 38–43. IEEE, 2016.

[346] Xiaojun Wang, Leroy White, Xu Chen, Yiwen Gao, He Li, and Yan Luo. An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, 2015.

[347] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. " i regretted the minute i pressed share" a qualitative study of regrets on facebook. In *Proceedings of the seventh symposium on usable privacy and security*, pages 1–16, 2011.

[348] Yi-Shun Wang, Yu-Min Wang, Hsin-Hui Lin, and Tzung-I Tang. Determinants of user acceptance of internet banking: an empirical study. *International journal of service industry management*, 2003.

[349] Roy Want, Bill N Schilit, Norman I Adams, Rich Gold, Karin Petersen, David Goldberg, John R Ellis, and Mark Weiser. An overview of the parctab ubiquitous computing experiment. *IEEE personal communications*, 2(6), 1995.

[350] Marc Weiser. The world is not a desktop. *interactions*, 1(1):7–8, 1994.

[351] Mark Weiser. The computer for the 21 st century. *Scientific american*, 265(3):94–105, 1991.

[352] Mark Weiser. Ubiquitous computing. In *ACM Conference on Computer Science*, volume 418, pages 197530–197680, 1994.

[353] Alan F Westin. Privacy and freedom atheneum. *New York*, 7:431–453, 1967.

[354] F.A. Westin. *Privacy and Freedom*. 1967.

[355] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0.

[356] Alexander Wieneke, Christiane Lehrer, Raphael Zeder, and Reinhard Jung. Privacy-related decision-making in the context of wearable use. In *Proceeding of the 20th Pacific Asia Conference on Information Systems (PACIS 2016)*, 2016.

[357] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I Hong, and John Zimmerman. Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 197–206. ACM, 2011.

[358] Daniel Wigdor and Dennis Wixon. *Brave NUI world: designing natural user interfaces for touch and gesture*. Elsevier, 2011.

[359] James Williamson, Qi Liu, Fenglong Lu, Wyatt Mohrman, Kun Li, Robert Dick, and Li Shang. Data sensing and analysis: Challenges for wearables. In *Design Automation Conference (ASP-DAC), 2015 20th Asia and South Pacific*, pages 136–141. IEEE, 2015.

[360] Jacob O Wobbrock, Htet Htet Aung, Brandon Rothrock, and Brad A Myers. Maximizing the guessability of symbolic input. In *CHI'05 extended abstracts on Human Factors in Computing Systems*, pages 1869–1872. ACM, 2005.

[361] Jacob O Wobbrock, Meredith Ringel Morris, and Andrew D Wilson. User-defined gestures for surface computing. In *CHI 2009*. ACM, 2009.

[362] Jacob O Wobbrock, Brad A Myers, and John A Kembel. Edgewrite: a stylus-based text entry method designed for high accuracy and stability of motion. In *Proceedings of the 16th annual ACM symposium on User interface software and technology*, pages 61–70, 2003.

[363] Stephen P Wright, Tyish S Hall Brown, Scott R Collier, and Kathryn Sandberg. How consumer physical activity monitors could transform human physiology research. *American Journal of Physiology-Regulatory, Integrative and Comparative Physiology*, 312(3):R358–R367, 2017.

[364] Huiyue Wu, Yu Wang, Jiayi Liu, Jiali Qiu, and Xiaolong Luke Zhang. User-defined gesture interaction for in-vehicle information systems. *Multimedia Tools and Applications*, 79(1):263–288, 2020.

[365] Huiyue Wu, Yu Wang, Jiali Qiu, Jiayi Liu, and Xiaolong Zhang. User-defined gesture interaction for immersive vr shopping applications. *Behaviour & Information Technology*, 38(7):726–741, 2019.

[366] Jian Wu, Lu Sun, and Roozbeh Jafari. A wearable system for recognizing american sign language in real-time using imu and surface emg sensors. *IEEE journal of biomedical and health informatics*, 20(5):1281–1290, 2016.

[367] Min Wu and Jake Luo. Wearable technology applications in healthcare: A literature review. *Online Journal of Nursing Informatics Contributors (OJNI)*, 23(3), 2019.

[368] Yoram Wurmser. Wearables 2019 : Advanced wearables pick up pace as fitness trackers slow, Jan 2019.

[369] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12):1, 2011.

[370] Heng Xu, Hock-Hai Teo, and Bernard Tan. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *ICIS 2005 proceedings*, page 71, 2005.

[371] Xuhai Xu, Haitian Shi, Xin Yi, Wenjia Liu, Yukang Yan, Yuanchun Shi, Alex Mariakakis, Jennifer Mankoff, and Anind K Dey. Earbuddy: Enabling on-face interaction via wireless earbuds. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2020.

[372] Yukang Xue. A review on intelligent wearables: Uses and risks. *Human Behavior and Emerging Technologies*, 2019.

[373] Tong Yan, Yachao Lu, and Nan Zhang. Privacy disclosure from wearable devices. In *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing*, pages 13–18. ACM, 2015.

[374] Huanfen Yao, Angela J Shum, Melissa Cowan, Ilkka Lähdesmäki, and Babak A Parviz. A contact lens with embedded sensor for monitoring tear glucose level. *Biosensors and Bioelectronics*, 26(7):3290–3296, 2011.

[375] Tuo Yu, Haiming Jin, and Klara Nahrstedt. Shoesloc: In-shoe force sensor-based indoor walking path tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(1):1–23, 2019.

[376] Edward N Zalta, Uri Nodelman, Colin Allen, and John Perry. Stanford encyclopedia of philosophy, 1995.

[377] Sherali Zeadally and Mohamad Badra. *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*. Springer, 2015.

[378] Cheng Zhang, Junrui Yang, Caleb Southern, Thad E Starner, and Gregory D Abowd. Watchout: extending interactions on a smartwatch with inertial sensing. In *Proceedings of the 2016 ACM International Symposium on Wearable Computers*, pages 136–143, 2016.

[379] Wei Zhou and Selwyn Piramuthu. Security/privacy of wearable fitness tracking iot devices. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–5. IEEE, 2014.

[380] Haining Zhu, Joanna Colgan, Madhu Reddy, and Eun Kyoung Choe. Sharing patient-generated data in clinical practices: an interview study. In *AMIA Annual Symposium Proceedings*, volume 2016, page 1303. American Medical Informatics Association, 2016.

[381] Yaguang Zhu, Stephanie L Dailey, Daniel Kreitzberg, and Jay Bernhardt. "social networkout": Connecting social features of wearable fitness trackers with physical exercise. *Journal of health communication*, 22(12):974–980, 2017.

[382] Michael Zimmer, Priya Kumar, Jessica Vitak, Yuting Liao, and Katie Chamberlain Kritikos. 'there's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, 23(7):1020–1037, 2020.