5-2018

Self-Regulation within the Wearable Device Industry and The Alignment to Device Users' Perceptions of Health Data Privacy

Tegan Ayers
tma6868@rit.edu

R·I·T

Self-Regulation within the Wearable Device Industry and The Alignment to Device Users' Perceptions of Health Data Privacy

By

Tegan Ayers

A Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science in Science, Technology, and Public Policy.

Department of Public Policy

College of Liberal Arts

Rochester Institute of Technology

Rochester, NY

May 2018

R·I·T

Self-Regulation within the Wearable Device Industry and
The Alignment to Device Users' Perceptions of Health Data Privacy

By

Tegan Ayers

Master of Science, Science, Technology and Public Policy
Thesis Submitted in Partial Fulfillment of the Graduation Requirements for the

College of Liberal Arts/Public Policy Program at
ROCHESTER INSTITUTE OF TECHNOLOGY
Rochester, New York

May 2018

Submitted by:

Tegan Ayers		
Student Name	Signature	Date

Accepted by:

Josephine Wolff/Faculty Thesis Advisor		
Public Policy, Rochester Institute of Technology	Signature	Date

Mehdi Mirakhorli/Co-advisor		
Software Engineering, Rochester Institute of Technology	Signature	Date

Christopher Paetsch/Committee Member		
Analytical Research, Bose Corporation	Signature	Date

Franz Foltz/Graduate Director		
Public Policy, Rochester Institute of Technology	Signature	Date

Abstract

Health data privacy has become increasingly pertinent as the Internet-of-Things (IoT), specifically, health-monitoring, wearable devices, has become more advanced. Today's regulatory framework allows wearable device companies to self-regulate how data is collected and used, thus leaving consumer, health data at risk of possible mishandling or abuse. Consequently, this research sought to examine whether data privacy practices adopted by major wearable manufacturers align with consumer expectations about these devices and the data they collect. Both consumers' understanding of health data privacy and the corresponding tech companies' stance on protecting consumer privacy were evaluated by performing crowd-sourced surveys and a thematic analyses of current privacy policies. Results of the survey suggest that most consumers are unaware of the possible risks associated with collecting health data; and, this lack of informativeness has led to what appear to be a lack of concern for their health data. However, many consumers still express an interest in protecting their privacy, regardless if they fully comprehend the risks, and most participants (79.4%) believed there should be additional regulations placed on the wearable industry. As such, it is recommended that a widely-known, non-government body, such as IEEE, develop a three-tier data privacy certification that wearable companies may apply for, but not be forced to adhere to. In principle, the market demand for increased data privacy controls would drive companies to classify each of their products as bronze, silver or gold-certified, which corresponds to increasingly stringent data privacy and security regulation.

Table of Contents

Abstract 3

Table of Contents 4

Introduction 6

Literature Review 9

- Perceived Risks and Benefits 9
- Specific Privacy Concerns 13
- Users' Understanding of Privacy 17
- Relevance to Research 19

Research Questions 21

Methodology 23

- Initial Consumer Insights Survey 23
- Privacy Policy Analysis 24
- Comprehensive Consumer Insights Survey 24

Findings 26

- Survey Participants 26
  - Survey 1 26
  - Survey 2 26
- Consumer Awareness and Concern for Health Data Privacy 27
  - Privacy Normalization 27
  - Data Awareness 28
  - Regulatory Awareness 31
  - User Actions 33
- Privacy Policy Effectiveness 36
  - Privacy Policy Analysis 36
  - Privacy Policy Understanding 39
- Wearable Industry Self-Regulation 40
  - Open-Ended Questions 40

Discussion & Significance 42

- Consumer Awareness and Concern for Health Data Privacy 42
- Privacy Policy Effectiveness 46

Wearable Industry Self-Regulation 47
Policy Recommendations 49
Limitations 52
Conclusion 53
References 55
Appendix 60
Appendix A: Survey 1 60
Appendix B: Survey 2 64

Introduction

Wearable devices ('wearables'), defined for the purposes of this research as body-worn, network-connected devices, and the software applications ('apps') associated with these devices, have become increasingly popular in recent years. In 2016, more than 250 million consumer wearables were sold globally, an 800 percent increase from 2012 sales (Comstock, 2015). This exponential market growth is expected to continue well into the next decade as wearables continue to become more affordable and reliable ("Gartner Says", 2017). Additionally, as analytics continue to advance, the health metrics collected, and experiences offered by these devices will continue to evolve, attracting even more users. With this enormous growth in the number of users comes an overwhelming amount of user data and, consequently, new and emerging consumer health data privacy concerns as well.

Many of today's wearables focus on fitness and activity tracking as the primary use case, thus aggregating large amounts of personal health data (herein referred to as "primary" data), such as heart rate and steps taken, that is capable of being shared or stolen. Furthermore, additional health data, including sleep and sex patterns, can sometimes be extracted from collected data using big data analytic techniques (herein referred to as "secondary" data). Collecting, analyzing and storing this type of data can lead to severe privacy breaches which may cause embarrassment, discrimination or even financial harm to the user.

A 2014 survey performed by PricewaterhouseCooper (PwC) found that 82% of respondents were concerned about wearables invading personal privacy ("The wearable future", 2014). Consumers perceive that they face a heightened amount of risk when using wearable devices due to how the industry has developed and the response of various federal regulatory bodies. For example, leaders of the wearable industry are comprised of today's largest

technology companies, such as Apple, Samsung and Fitbit, rather than medical device companies that are versed in health data privacy protocols and face greater regulatory oversight. Moreover, wearable devices, and the data they collect, are not protected under current health privacy laws, such as the Heath Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH). Finally, various federal agencies, such as the Food and Drug Administration (FDA), Federal Trade Commission (FTC) and Health and Human Services (HHS), who have the authority to impose regulations or oversee the sales of such devices, have decided to adopt a hands-off approach in order to promote innovation, allowing tech companies to self-regulate. This unique industry and regulatory structure allows companies to freely collect, use and share data from wearable devices and their corresponding mobile applications. Consequently, consumers have become dependent upon the discretion of the wearable device manufacturers to adopt fair and ethical privacy practices.

This thesis aims to determine whether data privacy practices adopted by major wearable manufacturers align with consumer expectations about these devices and the data they collect. To answer this question, a mixed methodological approach was taken to evaluate both consumers' understanding of privacy policies governing wearable devices and the corresponding tech companies' stance on protecting consumer data and privacy. Two consumer surveys, the first employed to gain initial insights and the second performed in order to delve deeper into those insights, were conducted to assess users' concerns about privacy and understanding of the data practices used by wearable device manufacturers. The privacy policies of those manufacturers were also analyzed to help identify areas of possible user concern and guide the questions within

the secondary survey. The extent to which self-regulating, wearable device companies are informing consumers and protecting their data was then evaluated by analyzing these results.

Literature Review

Although wearable devices are a relatively new type of technology, the data privacy concerns of these devices, and similar Internet-of-Things (IoT) devices, is not a new topic. According to IBM, over 90 percent of the data available today has been created within the last two years due to advancements in technology, such as wearable devices, smartphones and smart home appliances (Loechner, 2016). Consequently, due to the enormity and diversity of data collected by IoT devices, concerns regarding data privacy have increased greatly in recent years.

The purpose of this review was to understand the past research that has been conducted regarding consumers' awareness and concern about data privacy in regard to IoT devices and to analyze if their behaviors are analogous to their attitudes. Three key themes emerged from this review, including, (1) consumers tend to perform a risk-benefit analysis prior to adopting new technology, (2) consumers' specific privacy concerns are highly contextualized and non-uniform, and (3) device users, although claiming to value their privacy, tend to engage in risky behavior.

Perceived Risks and Benefits

Past research has concluded that consumers tend to perform a risk-benefit analysis prior to engaging with new technology (Anderson & Agarwal, 2011; Atienza et al., 2015; Gao et al., 2015; Li et al., 2016; Lopez et al., 2016; Talebi et al., 2016; Yang et al., 2016, Zhang et al., 2017). More specifically, potential device users weigh the potential risks of using a device against the perceived benefits the device may offer to determine the net perceived value (Atienza et al., Li et al., 2016; Lopez et al., 2016; Yang et al., 2016). Yang defines "perceived value" as "consumer's overall assessment of the utility of a product based on the perception of what is received and what is given" (Yang et al., 2016, p. 257). Calculating a positive perceived value leads to consumers' adopting the new technology, in this case a wearable device. Figure 1

summarizes the potential risks and benefits that various studies have identified as statistically significant factors consumers tends to consider in a risk-benefit analysis; this type of analysis is especially useful from a marketing perspective.

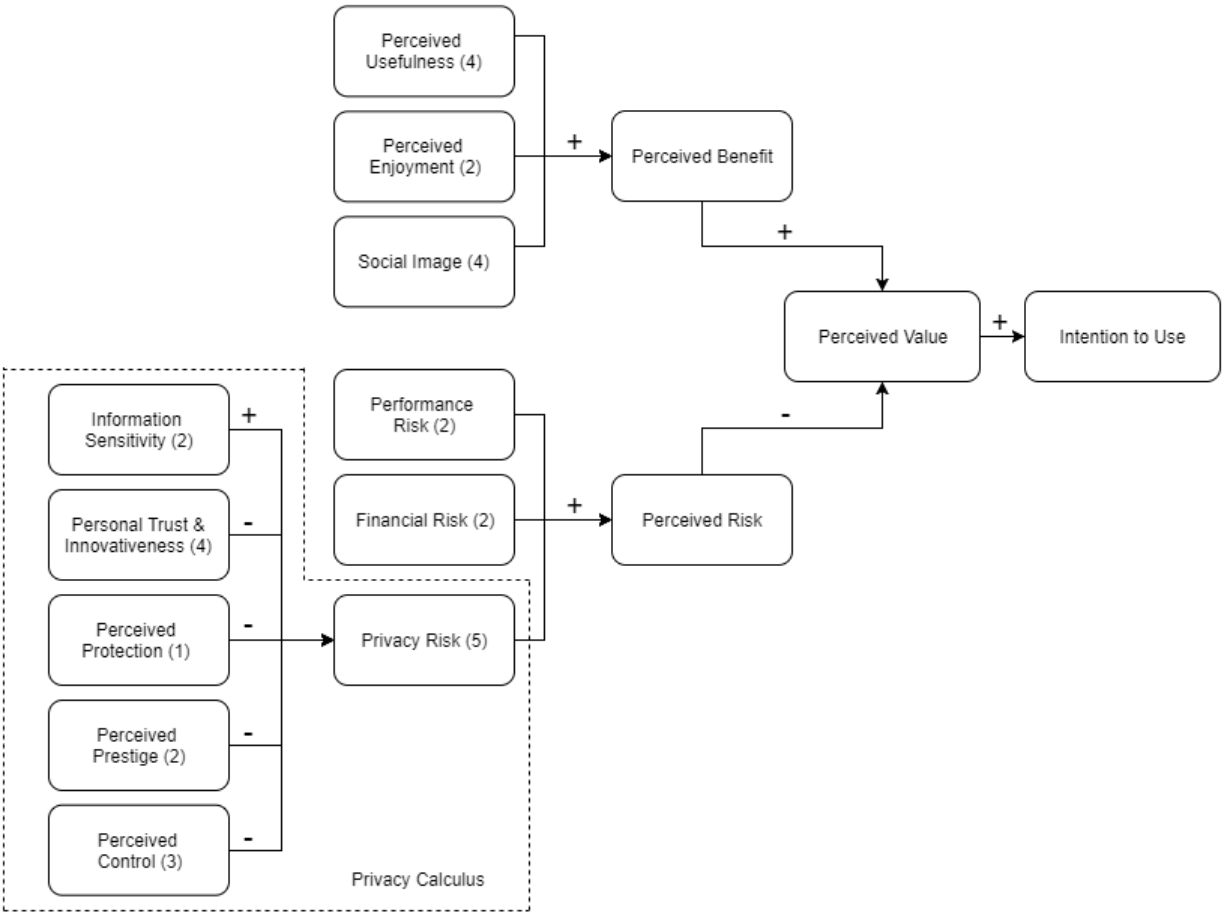

Figure 1: Risk-benefit analysis of potential consumers' intention to use a wearable device. Numbers in parentheses represent how many studies identified these characteristics as important to consumers. The dotted box outlines concerns that may be considered when determining whether to disclose personal information, referred to as "privacy calculus".

Antecedents to perceived benefits include personal enjoyment, device usefulness and the social image created as a result of using the device. In this review, enjoyment is defined as the ability of the device to provide entertainment regardless of the expected functionality of the device. Although still significant, personal enjoyment tends to contribute the least to users' perceived benefits (Yang et al., 2016). In contrast, both device usefulness and the users' social

image created from using a device significantly impact consumer's perceived benefits. Usefulness refers to the device's ability to enhance a users' performance in certain activities; these can include improving health, making better financial decisions, or remembering specific tasks (Gao et al., 2015; Li et al., 2016; Yang, et al., 2016). The social image created from using a device refers to the extent to which users receive positive feedback from peers as a result of using the device. Social image may be due to the manufacturers' prestige, the visual aesthetic of the device or the praise users receive from sharing data with friends (Talebi et al., 2016; Yang et al., 2016). For example, one study found that many wearable device users continue prolonged usage of the device due to the "confirmation with their group [of friends]" when sharing improvements within their health (Lowens et al., 2017). In contrast, another study correlated the positive effects of one's social image to the "snob effect". In other words, consumers desire to distinguish themselves by buying "status commodities", such as wearable devices, in order to make "consumer's economic and social status visible" (Zhang et al., 2017). Therefore, there is conflicting theories as to the effect of social image, with some arguing that consumers want to fit in with friends, while others argue that consumer's want to stand out.

Antecedents to perceived risks include performance, financial and privacy risks. Most studies included within this review tended to focus primarily on privacy in order to perform a type of modeling commonly known as privacy calculus. Two studies, however, included performance and financial risk into the risk-benefits analysis as well. Interestingly, both risks were found to have a significantly negative impact on perceived value in *potential* device users, but were not significant in *actual* device users (Lopez et al., 2016; Yang et al., 2016).

Privacy calculus refers to a narrower risk-benefit analysis in which potential benefits are weighted against privacy risks, only (Anderson & Agarwal, 2011; Li et al., 2015). This type of

analysis is performed by a consumer when determining their willingness to disclose personal data. Factors that influence privacy risk include information sensitivity, users' levels of trust and innovation, users' perceived protection of data and credibility of third parties, and finally, users' perceived control of his or her own data.

Information sensitivity refers to the type of information collected by the device. Data types may include, but are not limited to, preferences, biometric and health data, photos and emails. This factor positively contributes to privacy risk which means increasing data sensitivity also increases the amount of risk a user associates with the device (Li et al., 2016). A more in-depth discussion regarding the effect of specific data types on users' perception of data privacy will be presented in Section 3.2.

The second factor involved in privacy calculus involves the users' levels of trust and innovation. Trust may refer to the users' willingness to trust others *or* to trust electronics; whereas innovation refers to users' attitudes towards emerging technology. Both contribute significantly to consumers' perception of privacy risk, which suggests that specific personality traits of a potential device user can impact his or her decision to adopt an IoT device (Anderson & Agarwal, 2011; Atienza et al., 2015; Lamb et al., 2016; Talebi et al., 2016).

Thirdly, people's perception of data protection can factor into the privacy calculus model. This protection could come in the form of legislative protection, transparent privacy policies or the option to customize privacy settings. It was found that this factor negatively affected privacy risk, meaning that people feel safer if regulations are in place and device companies allow privacy settings to be managed by the user (Li et al., 2011). It should be noted, however, only one study included this factor into their privacy calculus model and within this study it was unclear if participants were aware of the current legislation in place to protect their data privacy.

This suggests that there is more work to be done regarding device users' perception of IoT device federal regulations.

Closely linked to perceived protection is the perceived prestige of the device manufacturer. When consumers trust a provider, have used a providers' past products and were satisfied with the outcome, the perceived level of privacy risk will decrease (Anderson & Agarwal, 2011). This, however, is another factor that was only included within two articles. There were no articles found that investigated the effect of company size and length of establishment on privacy risk. For example, perhaps within the wearable device industry consumers will be less concerned about a device manufactured by a large corporation such as Apple as opposed to a small, start-up such as Bellabeat.

Finally, IoT device users' sense of control is often included within many privacy calculus models. Control can refer to users' sense of ownership of their own data, their ability to choose who has access to the data or the ability to know the intended use of data once it is shared. When surveyed, device users identified control of data as the most significant privacy risk (Atienza et al., 2015; Lopez et al., 2016). A more in-depth discussion regarding the sharing and control of data will be presented in Section 3.2.

Specific Privacy Concerns

In quantifying specific privacy concerns, often researchers will conduct surveys and interviews with questions referencing specific devices or types of data. Of the included articles within this review, five studies addressed concerns pertaining to wearable devices while an additional study referred only to smartphones. It was found that certain demographics can play a significant role in level of privacy concern, with females and the older population tending to be more concerned (Felt et al., 2012; Jensen et al., 2005; Lee et al., 2015; Lopez et al., 2016;

Williams et al., 2017). Figure 2 summarizes the specific privacy concerns that device users tend to consider when addressing privacy.

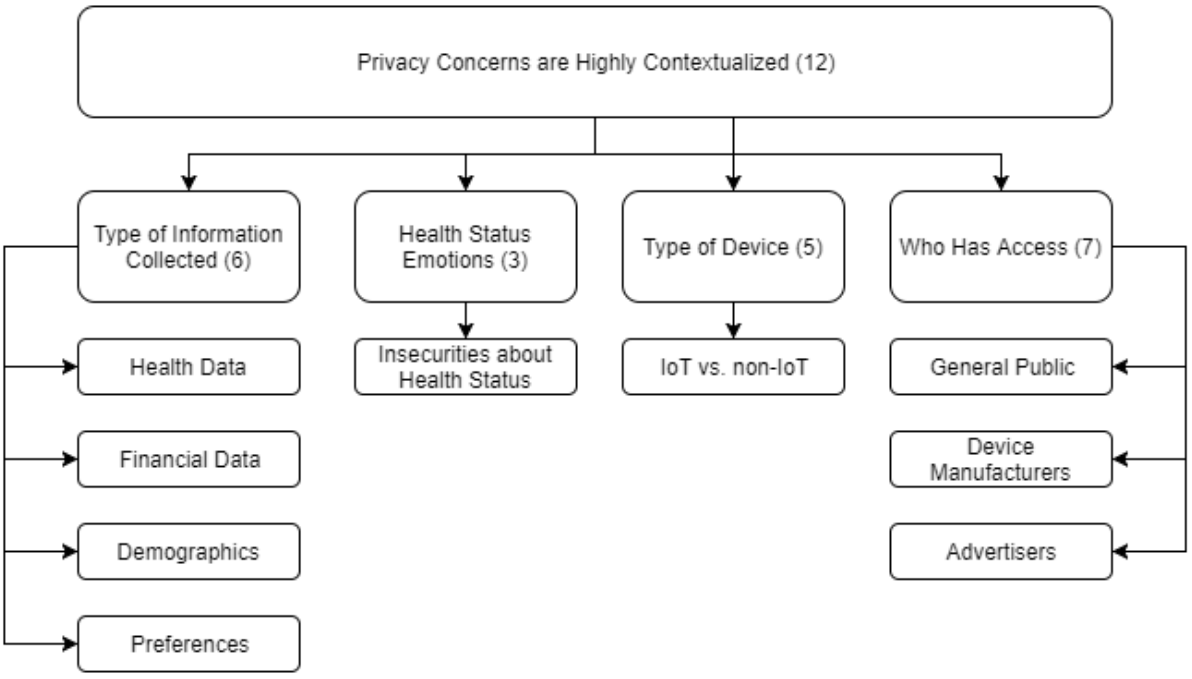

Figure 2: Specific data privacy concerns considered by device users. Numbers in parentheses represent how many studies identified these characteristics as important to consumers.

Privacy concerns among IoT device users are highly contextualized. In other words, an individual's level of concern regarding data privacy is dependent on several personal and technological factors and furthermore, these concerns are not identical across the population. Factors that may contribute to an individual's perception and desire for privacy include the type of device collecting data, the type of data being collected, the health status of the individual, and with whom the data is shared (Atienza et al., 2015; Felt et al., 2012; Lamb et al., 2016; Lee et al., 2015; Lopez et al., 2016).

The type of device an individual is interacting with, and the familiarity of said device, can affect user's privacy concerns. In other words, societally accepted technologies, such as desktops, laptops and smartphones, tend to be less worrisome to consumers than less familiar

technology. As wearable devices are a newer technology, the general population tends to be wearier of the possible privacy implications. However, current wearable device users exhibit less concern as the devices are more familiar and the risks more well understood. (Williams et al., 2017).

The architecture of IoT devices allows for these technologies to aggregate an abundance of information about an individual. For example, devices may contain built-in sensors that collect health and location data about an individual and; in addition, users often grant devices permission to access additional information, such as user preferences, photos and communication data. This allows the device and therefore, the device manufacturers, to collect and store data that users' may be uncomfortable with sharing. Consequently, the type of data a device collects and is given access to can affect users' perception of privacy (Atienza et al., 2016; Hoyle et al., 2014; Lee et al., 2015; Lopez et al., 2016; Motti et al., 2015). Specifically, data types such as personal photos, videos, and financial information have been identified as particularly concerning to individuals (Lee at al., 2015). In contrast, when put in the larger context of all data types, health data has been found to be of lesser concern to individuals (Lee et al., 2015; Lopez et al., 2016). For example, survey participants were asked to rank the level of concern they would feel if specific data types were exposed to the public and results found that medical conditions, physical state, and heart rate received "Very Upset Rates" (VUR) of 76%, 48% and 28%, respectively (Lee et al., 2015). Additionally, publicly available or observable information, such as gender, age, weight and habits were of even lesser concern to individuals (Lopez et al., 2016). These results, however, may be skewed due to the methodology of the studies. Presenting participants with *all* types of data may create biases in the results, as participants are more likely to place a higher value on data types that have blatantly obvious risks. For example, most participants will

object to their bank account information and passwords being publicized as there is an obvious risk to their financial well-being. In contrast, participants may not understand the risks involved with sharing health data, such as discrimination, and consequently, will be more willing to share this information publicly. Therefore, possible future work may involve narrowing the scope of a survey to include only health data while also educating participants about the risks of sharing such data; thus, giving more insight into concerns specifically regarding health data privacy.

Studies that have revolved around medical wearable devices have begun to delve into this field of health data privacy, prompting the argument that the emotional appeal people feel towards their health status contributes a significant amount in privacy calculus. In other words, people who feel negatively about their personal health will view medical wearable devices as a higher risk to their privacy than those who are ambivalent about their health (Anderson & Agarwal, 2011; Gao et al., 2015). In addition, consumers are concerned about the reliability and accuracy of the health data collected by IoT devices. Consumers' tend to have a heightened sense of concern that the data collected by the device may be inaccurate and cause the user to make erroneous health decisions (Marakhimov & Joo, 2017). Nevertheless, although their perceived risk may be heightened, people still recognize that medical wearable devices can improve their overall well-being, again illustrating the risk-benefit analysis.

Finally, with whom data is shared plays a major factor in users' privacy concerns. Interestingly, users tend to feel more concerned about sharing data publicly, which includes sharing with friends, co-workers or the general public, versus sharing with companies' servers. (Felt et al., 2012; Lee et al., 2015). In other words, users claim to not mind sharing data with companies. However, a disparity occurs between the included studies, as additional studies suggest that users expressed a strong desire to understand the intended use of the shared data as

well as maintain control of who gains access to their data (Atienza et al., 2015; Lopez et al., 2016; Lowens et al., 2017; Williams et al., 2017). For example, one interviewee stated "But, if after the fact someone were to gain this access to this data and use it to prove why I shouldn't be eligible for something or excluded from a health program that would be concerning" (Lowens et al., 2017, p. 300). Therefore, more research is needed to determine with who and for what reasons users would be comfortable sharing data.

Due to the high variability of privacy concerns, a "one-size-fits-all" approach to data privacy may not be adequate (Atienza et al., 2015). Consequently, device manufacturers should be transparent about their use of data and allow users' "granular control" of how, when and with who data is shared (Sunyaev et al., 2015). Furthermore, policy makers should begin exploration into regulations that allow for innovative growth of the IoT industry while still addressing consumer's specific concerns.

Users' Understanding of Privacy

Although people claim to value their privacy, often device users engage in behavior that dismisses privacy and puts their data at risk, a phenomenon known as the "privacy paradox" (Jensen et al., 2005; Talebi et al., 2016; Williams et al., 2017). This, in large part, is due to users' lack of awareness about privacy options. To determine peoples understanding of privacy and determine if users are in fact trying to take actions to protect their privacy, many studies have conducted device usability tests and interviews (Felt et al., 2012; Jensen et al., 2005; Williams et al., 2017). Figure 3 summarizes device users' understanding of data privacy and establishes the privacy paradox within IoT device users.

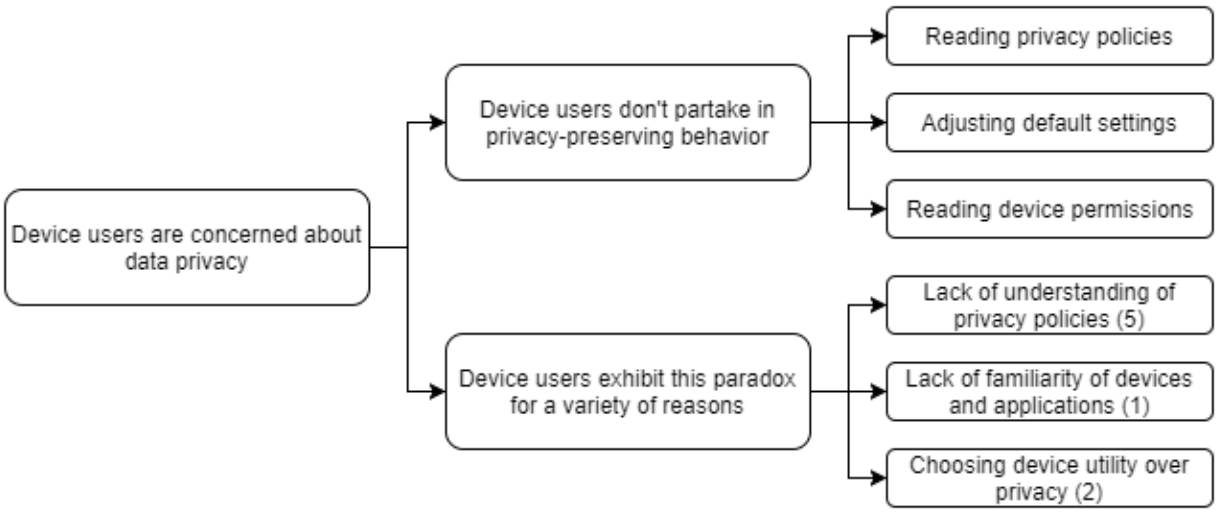

Figure 3: Prevalence and reasoning for the privacy paradox within IoT device users. Numbers in parentheses represent how many studies identified these characteristics as important to consumers.

In general, consumers *are* concerned about their data privacy (Cheung et al., 2016; Jensen et al., 2005; Williams et al, 2017). Studies have found that both Internet users and device users express a desire to retain their privacy and many users also claim to understand how to protect their data (Jensen et al., 2005; Williams et al., 2017). The theory of the privacy paradox maintains that although users understand their privacy options, they do not partake in behavior that reflect this understanding. To measure the prevalence of this paradox within IoT device users, usability tests are often performed in order to gauge how users interact with a device. Specific observable actions can include whether device users consult privacy policies, read device permissions or change default privacy settings. However, many studies have found that IoT device users fail to adopt these protective behaviors, hence reinforcing the privacy paradox, which may be due to a lack of understanding of privacy policies, a lack of familiarity with devices, or a desire to choose convenience over privacy (Felt et al., 2012; Jensen et al., 2005).

Privacy policies tend to be filled with an abundance of legal jargon that is incomprehensible to the average consumer (Felt et al., 2012; Sunyaev et al., 2015). Often privacy

policies are over generalized and do not address the specific device or application in question. This leads consumers to believe that policies lack transparency and consequently, they do not bother to find or read privacy polices (Felt et al., 2012; Sunyaev et al., 2015). In contrast, other consumers simply assume that all data is set to private by default, meaning there is no need seek out specific privacy policies. This suggests a large disconnect between what consumers perceive is happening to their data and how it is actually being used (Lowens et al., 2017).

Additionally, wearable devices are a new technology and this unfamiliarity can often lead to lack of knowledge within consumers. This may include lack of knowledge about potential risks the device poses or lack of knowledge about how to protect one's data. Consumers are significantly less familiar with wearable devices as compared to laptops and desktops, which could lead to consumers being less aware of how to protect their data (Williams et al., 2017). In other words, consumers may *want* to protect themselves, but are unsure of how to do so.

Finally, the paradox may exist simply because users choose device utility over data privacy. For example, many device users are aware that they can change privacy settings, but do not want to spend the time to do so and therefore, choose to keep the default settings (Motti et al., 2015; Williams et al., 2017). In addition, consumers may determine that the benefits of using the device outweigh the potential risk. As one article puts it, "While privacy can still be aspired to as a principle, it is often sacrificed through practical necessity" (Williams et al., 2017, p. 9).

Relevance to Research

Since IoT is a relatively new area of technology, there is still a large opportunity available for continued research, specifically within the wearable device sector and health data privacy. Many previous studies either did not analyze health data specifically or included health data in a comparison against blatantly high-risk data, such as bank account or social media

information (Lee et al., 2015). Consequently, there is an opportunity for more work to be done in which health data is the only type of data studied; therefore, discounting possible effects of including other data types. As such, one would be able to quantify which health data consumers' are particularly aware of or concerned about.

Secondly, many consumers may not be aware of the risks involved with sharing health data collected by a wearable device, thereby decreasing their perceived concern as shown in past literature (Lee et al., 2015; Lopez et al., 2016). For example, although a wearable device may only measure primary data, such as heart rate, certain analytics can be performed in order to estimate secondary data, such as sleep patterns, which consumers may not be aware of occurring. As such, there is an opportunity for additional work in which users are presented with all possible risks associated with one piece of health data in order to determine if this affects users' level of concern.

Finally, past research has previously identified that privacy policies, which are used as a means of informing consumers, are too long, hard to read and use an abundance of legal jargon (Sunyaev et al., 2015; Jensen et al., 2005; & Felt et al., 2012). However, no research has endeavored to determine how consumers react to the contents of privacy policies. Therefore, additional research may seek to control for these shortcomings by presenting consumers with short, easy-to-understand excerpts from current privacy policies and determining consumers' feelings towards the contents of the policy.

Research Questions

This research seeks to quantitatively answer the following three questions:

1. *Are consumers aware and concerned about their health data privacy, specifically when presented with the implications of sharing their health data?*

   The majority of this research will focus on quantifying wearable device users' awareness of risk and level of concern for data privacy. As discussed above, past literature has failed to inform research participants of the risks involved in sharing health information; and, as such, health data privacy has generally been quantified as unimportant to consumers. Therefore, this research seeks to openly address these risks and determine if informing consumers about these possible risks correlates to an increase in data privacy concerns.

2. *Are privacy policies an effective method of informing consumers about current data privacy practices?*

   Device manufacturers tend to rely on detailed privacy policies as a catch-all for informing consumers about how their data is used. Past research has previously identified that these policies are long, hard to read and use an abundance of legal jargon (Sunyaev et al., 2015; Jensen et al., 2005; & Felt et al., 2012). This research seeks to controls for these shortcomings by presenting participants with brief excerpts from various policies, which do not contain the characteristics of full privacy policies (i.e. long, hard to read, legal jargon) to determine their emotions towards the collection and use of their data.

3. *To what extent do consumers believe that the wearable device industry, which is currently self-regulated, should comply with additional data privacy regulations?*

   Using the results of the first two research questions, a comprehensive thematic analysis will be performed to determine if the privacy practices used by wearable companies is informing

consumers to their satisfaction. Ultimately, the purpose of this research is to determine if self-regulation within the wearable industry is sufficiently protecting consumers' data privacy concerns. These results will help to guide policy makers in determining how to approach data privacy within the new technological age of IoT.

Methodology

For this study, multiple methodologies were employed to (1) gain initial insight into consumers' understanding of privacy, (2) extract device companies' approach to protecting privacy, and (3) perform a more comprehensive analysis of consumers' understanding and actions towards protecting their privacy.

Initial Consumer Insights Survey

To gain initial consumer insights on wearable devices, we conducted a large-scale, crowdsourced online survey of 400 participants ("Survey 1"). Both wearable device users and non-users were included in this initial survey to gain a broad sense of privacy practices across the population. The survey was designed to gauge (1) consumers' awareness of privacy risks, (2) consumers' concern for their health data privacy, and (3) what, if any, preventative actions consumers are taking to protect their privacy. Many past research studies pertaining to privacy have utilized surveys as the primary mode of data collection as surveys provide a large sample size, and standardized data that can be analyzed statistically.

Ultimately, the survey consisted of 17 questions, with 15 multiple choice and 2 open-ended questions. The breakdown of the questions was as follows:

- Comprehension and Background (3)
- Consumer Awareness (1)
- Consumer Concern (5)
- Consumer Actions (4)
- Demographics (4)

A reading comprehension question was included in order to ensure participants were fully engaging with the survey rather than simply clicking answers. Additionally, demographics questions were included in order to eliminate responses from children under the age of 13 and to

determine the effects various demographics have on data privacy concerns. The full text of the survey can be found in Appendix A.

The survey was generated and advertised on Amazon's Mechanical Turk (MTurk), a platform used by previous researchers to learn insight into the general population (Felt et al., 2012; Lee et al., 2015). It was posted on October 27, 2017 and remained active until 400 participants had completed it. All MTurk users were able to participate. Participants who incorrectly answered the reading comprehension question were rejected and the survey was again opened until the participant quota was reached. Each accepted participant was paid $0.70 and all answers remained anonymous.

Privacy Policy Analysis

From Survey 1, the most commonly used wearable devices within the sample population were identified and their respective privacy policies were analyzed. Privacy policies for Fitbit, Apple, Samsung and Garmin were coded and thematically analyzed. Specifically, the privacy policies were analyzed in order to extract the types of data collected by each company, what the data was used for, how and with whom the data was shared and what measures were implemented to protect consumer privacy. This information was then used to generate more detailed questions included in the secondary survey.

Comprehensive Consumer Insights Survey

Following analysis of Survey 1, a second, more thorough survey was conducted to further gauge consumer insights ("Survey 2"). Survey 2 was designed similarly to Survey 1 in that questions fell into three categories, including (1) consumers' awareness of privacy risks, (2) consumers' concern for their health data privacy, and (3) what, if any, preventative actions consumers are taking to protect their privacy. However, Survey 2 included both follow-up

questions to interesting results of Survey 1, and new questions that emerged as a result of the privacy policy analysis. Furthermore, Survey 2 included more open-ended response questions to encourage participants to explain why they felt or acted a certain way. Finally, survey participants were limited to wearable device users, only, allowing for a more focused analysis.

Survey 2 consisted of 27 questions, with 16 multiple choice and 11 open-ended questions. The breakdown of the questions was as follows:

- Comprehension and Background (3)
- User Awareness (6)
- User Concern (6)
- User Actions (8)
- Demographics (4)

More stringent rejection criteria were maintained during Survey 2. Again, a reading comprehension question was included to ensure participant engagement. In addition to this, however, a lower bound time limit of two minutes was required of all participants. Incomplete or incomprehensible survey responses were also rejected. Finally, only MTurk users with a "Masters" status, meaning the quality of users' responses had been verified by past MTurk requesters, were able to participate.

Survey 2 was posted to Amazon's Mechanical Turk on February 3, 2017 and remained active until 300 participants had been approved. Each accepted participant was paid $1.50 and all responses remained anonymous.

Findings

Survey Participants

Survey 1

Upon completion of Survey 1, 412 survey responses were collected; after filtering incomplete or incomprehensible answers, 396 responses were accepted. In total, 61% of participants were male while 39% were female and the majority (79%) of participants fell within the 20-39 age group. Additionally, 92% of respondents had completed further education past a high school diploma, indicating a well-educated participant pool. This reflects the target consumer wearable device market.

Respondents were divided into current or previous wearable device users and non-device users. 63% of participants (250 people) were considered device users, while the remaining 37% (146 people) either did not use or did not know if they currently or previously used a device. Unless otherwise indicated, the Survey 1 analyses was separated into device users and non-users.

Survey 2

Upon completion of Survey 2, 309 survey responses were collected. Using the rejection criteria described within the Methods section to filter all responses, 287 total responses were accepted for analysis. In total, 57% of participants were male while 43% were female, suggesting a slightly more even gender distribution than Survey 1, and the majority (75%) of participants fell within the 20-39 age group. Further, 85% of respondents had completed higher education past a high school diploma, indicating a well-educated participant pool. This, again, reflects the target consumer wearable device market and a good, representative sample population. Finally, in contrast to Survey 1, all participants were current wearable device users.

Consumer Awareness and Concern for Health Data Privacy

Privacy Normalization

Often when conducting privacy studies, especially ones involving interviews and surveys, participants become more privacy-conscious throughout the duration of the study (Lowens et al., 2017). As participants are asked more questions, or presented with more privacy-concerning scenarios, their awareness and sensitivity to privacy risks increases. This may skew the results of the survey, with responses to questions asked later in the study reflecting a heightened sense of concern than responses to earlier questions.

To determine if this bias was apparent within our research, an identical question was included at the beginning and end of each survey which asked participants to rank their health data privacy concerns on a 1-5 Likert-scale (see Appendix A). Results for Survey 1 and 2 were nearly identical, however, Survey 2 included a more representative sample and therefore, are described in more detail here. Of all included responses, initial concerns totaled 2.87 ± 1.26 on the Likert scale while ending concerns were 3.07 ± 1.18 This suggests there was no significant difference between pre and post-survey privacy concerns and the results of each survey should not be biased ($p = 0.0532$).

The results of this question were also analyzed for varying groups and demographics within the sample. Results are summarized in Table 1. In summary, the male population exhibited a higher concern for privacy than females, but not with statistical significance, which agrees with previous literature ($p = 0.0588$) (Jensen et al., 2005; Lee et al., 2015; Williams et al, 2017). However, both surveys showed a significant difference ($p < 0.0001$) in privacy concerns between age groups, with younger generations ($\leq$ 39 years old) tending to be more privacy-conscious than older generations, This finding is highly disputed within literature, with some

studies showing older generations being more concerned (Lee et al., 2015; Williams et al., 2017) while others show younger generations being more concerned (Lopez et al., 2016), as agrees with this research. This is most likely an effect of younger people growing up with technology highly integrated into their daily lives and; therefore, they have a better understanding the risks associated with IoT devices. Finally, survey results indicated a statistically significant relationship ($p < 0.0001$) between education level and privacy concerns. Namely, those who had obtained education past a high school diploma were significantly more concerned than those who had not. This relationship has only been explored in one previous work and was not found to be significant (Lee et al. 2015). The results of this research, however, suggest that through education, consumers have learned to question technology, rather than accepting it at face value.

Table 1: Level of Privacy Concerns for Varying Groups within Survey 2 Population

Group/Demographic	***Privacy Concern****
Gender	
Female	2.71 ± 1.30
Male	3.00 ± 1.23
Education	
HS Grad or Lower	2.23 ± 0.96
Higher Education	2.97 ± 1.28
Age	
Younger (≤ 39 years old)	3.04 ± 1.28
Older (≥ 40 years old)	2.35 ± 0.98
Total Participants	2.87 ± 1.27

**Data reflects a 1-5 Likert scale, with 1 being "Not at All Concerned" and 5 being "Very Concerned."*

Data Awareness

Survey 1 aimed to gauge consumers' awareness about how their data could potentially be used by wearable device companies or hackers. To accomplish this, participants were presented with a type of primary data collected by a wearable and asked if they were aware of the secondary data capable of being estimated from the data. In analyzing *all* the responses as one,

meaning responses were not separated into various data types, it was found that 38.4% of device users and 44.5% of non-users were aware of possible analytics that can be performed on primary data. These results demonstrate a large lack of knowledge by both device users and non-users alike.

Survey 2 attempted to better quantify this unawareness by determining if participants are more aware of the implications of *specific* data types. Again, participants were presented with a type of primary data collected by a device (e.g. heart rate, calories burned) and asked if they were aware of the secondary data that was able to be estimated from this information (e.g. sleep patterns, risk of obesity). The type of data presented was randomized for each participant. For example, participant A received the question, "Are you aware that when a wearable device measures your *heart rate variability*, it is possible for your *stress levels* to be estimated?"; while participant B received the question, "Are you aware that when a wearable device measures your *sweat*, it is possible for your *emotions* to be estimated?". The type of data each participant was asked about was recorded and each primary/secondary data type received approximately 15 responses each. Table 2 displays the percentage of participants aware of each risk and the corresponding level of concern, as measured on a 1-5 Likert scale, that participants had for each risk. The table is structured so that risks are ordered from least to most amount of awareness. Furthermore, the level of concern is highlighted so that risks rated less than 2.5 are green (little concern), between 2.5 and 3.5 are yellow (moderate concern), and greater than 3.5 are red (high concern).

Table 2: Awareness* and Concern** for Specific Primary/Secondary Health Data Types

Primary Data/Secondary Data	***Participants Aware of Risk (%)***	***Level of Concern (1-5 Likert)***
Heart Rate/Sex Patterns	6.67	2.87 ± 1.36
Sweat/Risk of Neurological Disorders	12.50	2.75 ± 1.29
Force per Step/Risk of Neuro. Disorders	13.33	3.07 ± 1.39
Body Temperature/Female Period Cycles	25.00	2.44 ± 1.26
Respiration Rate/Risk of Respiratory Disease	26.67	2.93 ± 0.88
Blood Oxygen (SpO2)/Risk of Heart Disease	28.57	3.21 ± 1.19
Sweat/Emotions	30.77	3.31 ± 1.18
Sun Exposure/Risk of Skin Cancer	33.33	3.07 ± 1.39
Brain Activity (EEG)/Stress Levels	40.00	2.33 ± 0.98
Body Temperature/Female Fertility Cycles	41.67	2.43 ± 1.09
Heart Rate/Respiration Rate	42.86	3.00 ± 1.36
Respiration Rate/Sex Patterns	42.86	2.38 ± 1.26
Heart Rate/Risk of Heart Disease	46.15	3.20 ± 1.47
Eye Movement/Sleep Patterns	46.67	3.13 ± 1.50
Step Rate/Risk of Obesity	50.00	3.31 ± 1.03
Calories Burned/Sex Patterns	53.85	4.17 ± 0.94
Calories Burned/Risk of Obesity	58.88	2.81 ± 1.23
Heart Rate Variability/Stress Levels	61.54	2.40 ± 1.12
Heart Rate/Sleep Patterns	73.33	2.40 ± 1.12

**Data types are listed in order of least to most awareness.*
***Level of Concern data reflects a 1-5 Likert scale, with 1 being "Not at All Concerned" and 5 being "Very Concerned."*
Green < 2.5, 2.5 ≤ Yellow ≤ 3.5, Red > 3.5

From Table 2 it can be inferred that there is no correlation between consumers' awareness about a specific risk and how concerned they feel about that risk. In other words, a low awareness about a specific data type does not correlate to a high level of concern, as may have been expected. However, insight can be gathered about awareness and concern, separately. As expected, participants were most aware about the risks associated with common primary data types, such as heart rate, calories burned and step rate. Furthermore, they were least aware of risks associated with more obscure primary data types, such as sweat, force per step, and body temperature. The most common wearable devices, including Fitbit and Apple Watch, do not currently measure these metrics, so naturally participants would be unaware of these. Finally,

many of the "moderate concerns" (highlighted yellow) involve secondary data in which a users' risk of a disease can be extracted, suggesting that consumers may be concerned about insurance companies getting ahold of this data.

Regulatory Awareness

While the above section tested participants' awareness regarding risks involved with collecting specific data types, this section evaluated participants' knowledge of current regulations in place to protect data privacy. To start, Survey 1 participants were asked about their knowledge of the Health Insurance Portability and Accountability Act (HIPAA) to evaluate consumers' understanding of the most well-known federal health data regulation. Participants were given a brief statement explaining why HIPAA was created, then asked if they believed that the data collected by wearable devices is regulated by HIPAA. Although many stated that they did not believe (43.4%) or were unsure (34.1%) if data collected by wearable devices was regulated by HIPAA, nearly a quarter of participants (22.5%) said that they *did* consider this statement to be true, which suggests that some people have a false understanding of regulations in place to protect consumers' privacy (Figure 4).

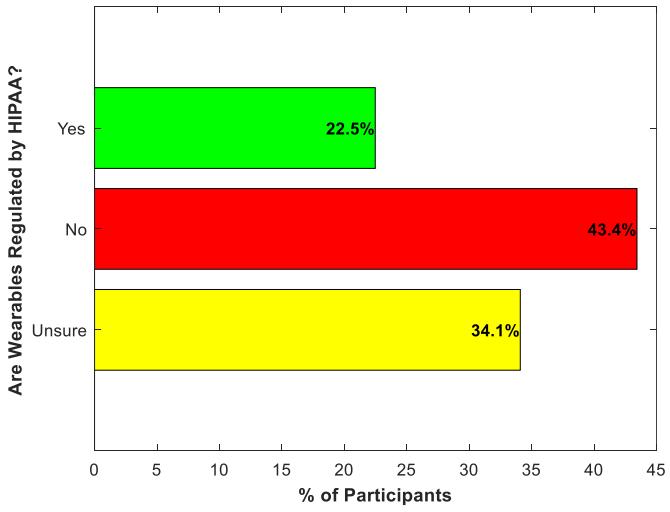

Figure 4: Percentage of participants that believe wearable devices and the data they collect are regulated by HIPAA.

While Survey 1 demonstrated a lack of understanding about the authority and applicability of HIPAA to wearable device data, Survey 2 sought to further investigate this misunderstanding, and determine if consumers felt as if there should be more regulations in place. Participants were asked if they believed there were *any* regulations currently in place to regulate the health data collected by wearable devices. Nearly three-quarters of participants stated that they were unsure of (27.5%) or did believe (39.7%) that there are current regulations in place that protect wearable data privacy, which is incorrect (Figure 5).

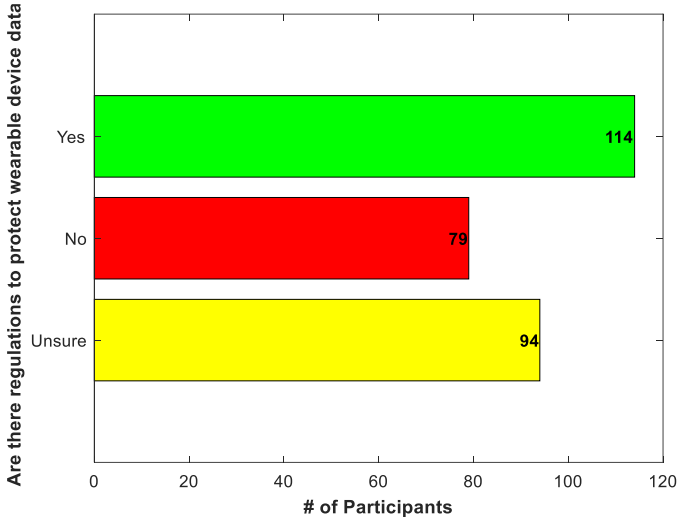

Figure 5: Number of participants that believe there are current regulations in place that protect the privacy of health data collected by a wearable device.

To elaborate on this finding, those that indicated that they believed there are current wearable device data privacy regulations were then asked if they were able to name any of those regulations. Interestingly, most people could not name any, but stated that "[data privacy is] something so obvious there have to be regulations on it." Others couldn't think of specific policies, but rather, stated that there were general policies to protect "the safety of our data" or "regulate how [device manufacturers] can share or sell your data."

Table 3 further elaborates on participant responses to this question.

Table 3: Data Privacy Regulations Listed by Survey Participants*

Can you name any regulations?	***Example Responses***
No (52)	"I can't name any, but I know there should be."
	"...I can't, actually, I just feel like that's something so obvious there have to be regulations on it."
General privacy and security regulations (9)	"The prevention of release of any personal information such as GPS location."
	"I think it is about the safety of our data."
HIPAA (9)	"Health Insurance Portability and Accountability Act"
	"Covered entities"
General data sharing regulations (5)	"Terms of service regulate how they can share or sell your data."
	"They don't share it with any 3rd parties."
FDA regulations (3)	"FDA regulations"
MDR (2)	"MDR"

**Numbers in parentheses reflect how many participants mentioned this "regulation".*

User Actions

The previous three sections analyzed consumers concern for data privacy and their understanding of regulations in place to protect this privacy, however, it was desired to determine if these elicited concerns translate into similar actions, such as limiting the amount data shared with others. In other words, participants were asked pointed questions about how they interact with their devices and mobile applications in order to elicit what, if any, privacy-preserving behaviors consumers engage in. Questions revolved around three categories, including (1) sharing data with third-party apps, (2) inputting information when prompted during application installation, and (3) inputting additional information during normal application usage. While Survey 1 sought to simply understand *how* consumers interact with their devices, Survey 2 attempted to rationalize *why* users perform certain actions.

For the purpose of this research, "third-party apps" were categorized as apps provided by a vendor other than the device manufacturer. Results of Survey 1 showed that the majority of

device users (66.0%) either do not or are unsure if they connect their device to any third-party apps. Survey 2 verified this result, but also explored the reasoning of those who choose to not use third-party apps. Most commonly, people indicated that they do not need the services of additional applications, suggesting that the Fitbit or Apple Fitness apps, for example, are sufficiently satisfying consumers' needs. However, 38.0% of respondents indicated that they did not connect to third-party applications due to privacy-related concerns, such as fear of sharing too much data. Figure 6 further elaborates on these reasonings and shows privacy-related concerns in red.

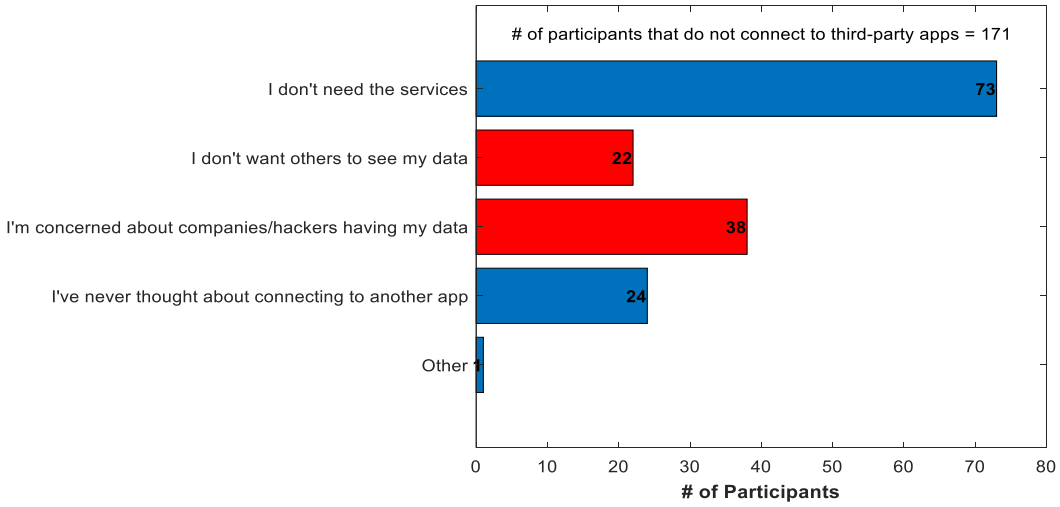

Figure 6: Reasons why participants do not connect to third-party applications. Bars in red indicate reasons pertaining to privacy concerns.

When installing a mobile application, such as the Fitbit app, Apple Workout, or Samsung Health, users are often asked optional, personal questions during the installation process, such as height, weight, current activity level, alcohol intake, etc. Results of Survey 1 indicate that nearly all device users (91.6%) will share any personal data *if it was asked of them* during installation. In other words, if the user was prompted to input information during installation, then they would comply. The results of Survey 2 verify this action; however, the few participants that did not enter their information (n = 14) were asked to give reasoning as to why they chose not to

input some information. The majority of responses (n=11) indicated that they did not input information due to privacy-related concerns. Again, Figure 7 further elaborates on these reasonings and shows privacy-related concerns in red.

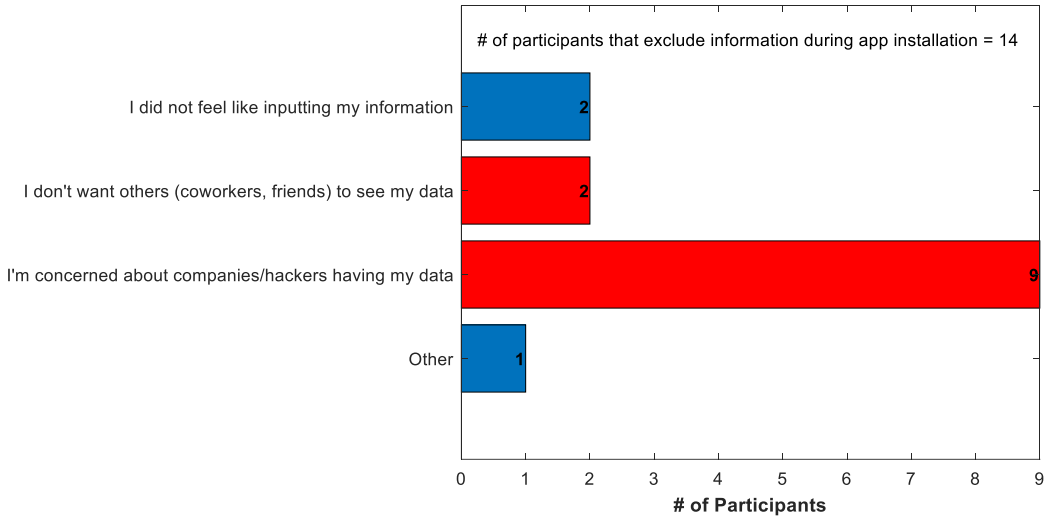

Figure 7: Reasons why participants do not input all personal information during mobile application installation. Bars in red indicate reasons pertaining to privacy concerns.

Finally, users were questioned about the opportunity to input additional health data, such as medication, glucose levels and blood pressure during normal application usage. Interestingly, almost all Survey 1 participants (84.8%) responded negatively to this question, suggesting that if people aren't *prompted* to input personal information, then they will abstain from doing so. Survey 2, again, verified this inaction, and participants were asked for their reasoning. Although most indicated that they simply do not track any other information, some (18.5%) suggested that they do not enter information due to privacy concerns, as shown in red in Figure 8.

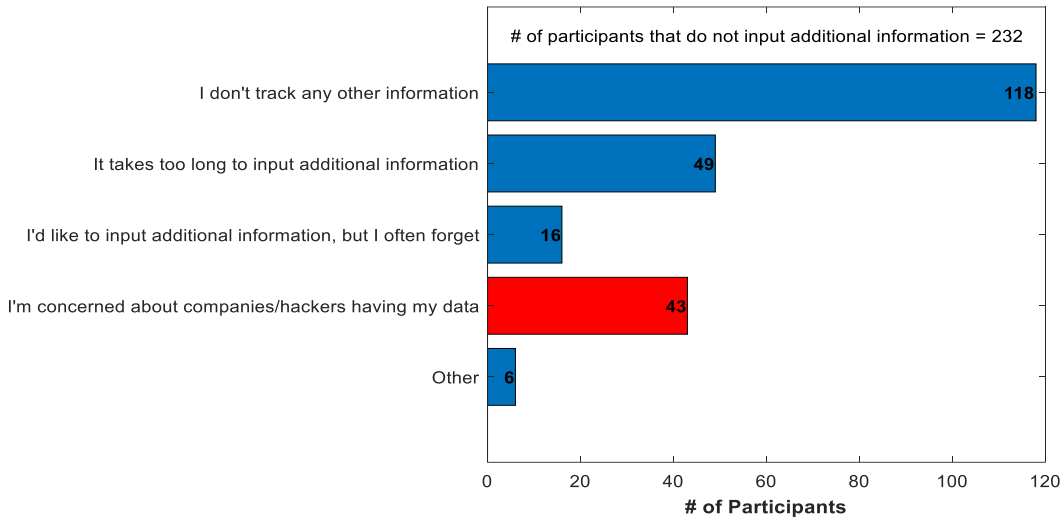

Figure 8: Reasons why participants do not input additional health information during normal application usage. The bar in red indicates a reason pertaining to privacy concerns.

Privacy Policy Effectiveness

Privacy Policy Analysis

From Survey 1, it was found that the most commonly used devices among participants were sold by Fitbit (62.4%), Apple (14.4%), Samsung (4.0%) and Garmin (2.8%). Consequently, the privacy policies of these four companies were chosen to be analyzed. The most up-to-date privacy policies were gathered, read and thematically analyzed. Table 4 presents some general observations about each privacy policy.

Overall, the most important considerations for each policy were nearly identical across the policies. Specifically, the types of data collected, with whom and how data is shared, and the permissions granted to each company were consistent for all privacy policies. Furthermore, these are the aspects that most affect the consumer.

Table 4: General Privacy Policy Attributes

Point of Interest	***Fitbit Privacy Policy***	***Apple Privacy Policy***	***Samsung Privacy Policy***	***Garmin Privacy Policy***
Last updated?	09/28/2017	01/19/2018	12/21/2017	07/11/2017
Separate policy for wearable devices?	N/A	No	Yes	Yes
Specifically references "health data"?	Yes	No	Yes	No
Profile is set to "private" by default?	Doesn't say	Doesn't say	Doesn't say	Yes
Defines the term "personal information"?	No	Yes	No	Yes
Mentions data security protocols?	Yes	Yes	Yes	No

All wearable device companies collect information about the user, and much of this information is considered "personal" or "identifiable" information. Apple and Garmin explicitly define the term "personal information" within their policies as "information that, either alone or in combination with other information collected, identifies an individual" (Privacy Statement for Garmin, 2017). Fitbit and Samsung, however, simply give examples of the type of information they collect; this may wrongly lead consumers to believe the only personal information collected is that of the examples given. Moreover, almost all policies analyzed, excluding Fitbit, include a statement within their policies asserting that if a user chooses to not input their personal information, then the user will not have access to all the device features. For example, within the first paragraph of Apple's Privacy Policy, the policy states "you are not required to provide the personal information that we have requested, but, if you choose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have" (Apple Privacy Policy, 2017). This prompted a question within Survey 2 in which participants were asked if they chose not to read privacy policies simply because they felt as if they had no choice in their privacy settings.

All privacy policies analyzed stated that de-identified, aggregated data is able to be shared with third-parties for the purposes of public reports or advertising. Although the terms "de-identified" and "aggregated" are well-known within the health data privacy industry, the everyday consumer may be confused or misunderstand the meaning of such terms; this may lead to consumers unknowingly engaging in risky behavior. Therefore, a question was developed for Survey 2 to test if the inclusion of legalese jargon within privacy policies affected consumers' overall understanding of the major concepts.

Finally, each privacy policy included a section titled "How We Use Information", in which companies stated the purposes of collecting personal information. Within each policy, a broad, blanket statement was included that allowed companies to perform various types of analytics on the data. For example, Fitbit claims:

> Using the information we collect, we are able to deliver the Services, improve them, and research and develop new ones. For example, we use the information to provide you with the Services you request; understand how you and other users interact with the Services; track exercise, activity, and other trends; provide customer support; troubleshoot and protect against errors; perform data analysis and testing; conduct research and surveys; and develop new features and Services (Fitbit Privacy Policy, 2017).

Vague wording, such as in the statement above, could allow Fitbit to use the primary health data measured by its wearable devices and "perform data analysis" in order to extract secondary data. This, however, may not be fully understood by common device users; and, consequently, Survey 2 asked participants to explain how this statement made them feel.

Privacy Policy Understanding

Following the Privacy Policy analysis, it was desired to determine *why* people fail to read privacy policies, and if they were to read them, how would they *feel* about their data privacy. Participants were first asked if they had ever read a privacy policy, and surprisingly, 25.8% of responses indicated that they had. The three-quarters of participants who stated that they had not, however, were asked to justify why they chose not to. As expected from past literature, 87.3% reasoned that they chose not to read privacy policies due to failures on the part of the device manufacturers, as shown in red in Figure 9 below (Felt et al., 2012; Sunyaev et al., 2015). For example, the policies are too long (56.8%), too difficult to understand (11.7%) or users simply felt that they had no choice in their privacy settings, so reading the policy was not worthwhile (18.8%).

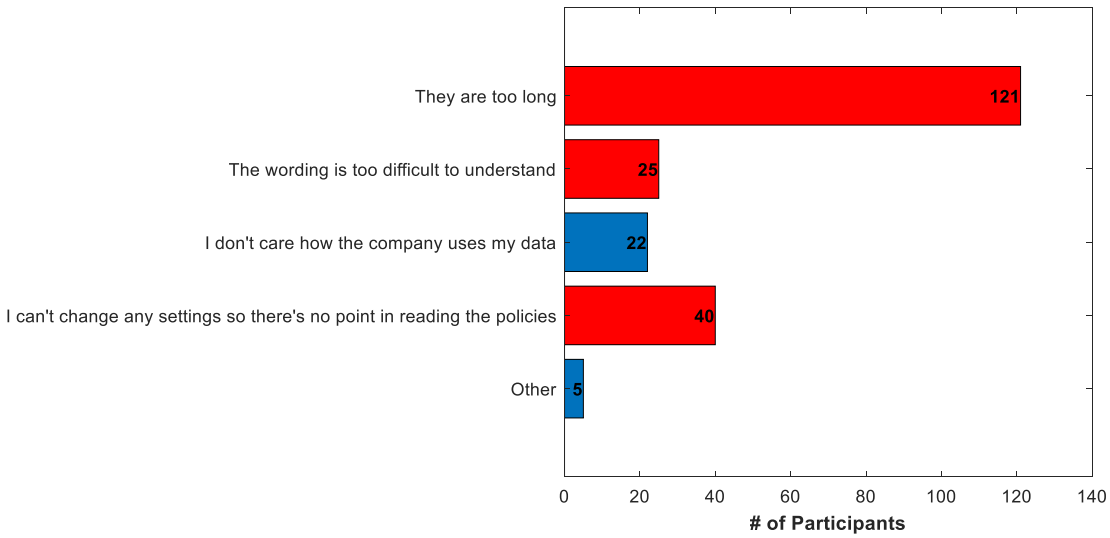

Figure 9:Reasons why participants fail to read privacy policies. Bars in red indicated failures on the part of the device manufacturers.

Following this, participants were presented with an excerpt from the Fitbit Privacy Policy pertaining to how the company uses collected data (see Appendix B). Participants were then asked how this statement made them feel. While half of participants (54.7%) responded that they felt “good” or “safe” after reading the statement, another 28.7% stated that they felt “concerned”,

"surprised", or "confused". Positive responses included justifications such as, "nothing listed seems to be outside the domain of appropriate use", indicating an awareness about what companies are allowed to do with data. In contrast, negative responses, such as "this leaves a great deal open to interpretation…" shows skepticism within some consumers. Table 5 provides more examples of participants' feelings.

Table 5: Feelings towards Fitbit Privacy Policy Excerpt

Feelings Toward Privacy Policy Statement	***Example Responses***
Good (117)	"…I have no problem sharing basic information to help them with their studies and developing new features and such. I have everything to gain if the product they produce gets better."
	"Nothing listed seems to be outside the domain of appropriate use."
Concerned (58)	"I am somewhat concerned about the testing and analysis that the company is using my data for. I'd like to know more of what they are analyzing."
	"The language used is tactical and at times does not seem genuine from the perspective of the user/customer."
Safe (40)	"I feel like this is a proper and comprehensive disclosure."
	"I feel the information above does not leave me at risk for anything significant."
Surprised (12)	"I am surprised at how much they do with the data they collect."
	"This leaves a great deal open to interpretation as far as what they use my data for, I mean developing features and services could literally mean anything."
Confused (12)	"Written by lawyers most likely, vague."
	"'Conduct research and surveys' is confusing to me."
Other (40)	"Indifferent because it is just words to satisfy the readers, the users, the products makers, the brands, the legal requirements."
	"Unconcerned, because I kind of expect such things now days."

**Numbers in parentheses reflect how many participants mentioned this concern.*

Wearable Industry Self-Regulation

The above results will be further analyzed within the Discussion section in order to further elaborate on the question of self-regulation. However, the effectiveness of self-regulation not only depends on the success of data privacy practices, but rather, the overall satisfaction of consumers. This is described in more detail below.

Open-Ended Questions

Both Survey 1 and 2 concluded with an open-ended question in which participants were asked if they held any other concerns about wearable devices or health data. Responses were systematically coded and analyzed to determine any responses that were of especially high concern. Of the 79 participants that answered this question with additional concerns, 66 were able to be coded.

Six major concerns emerged. Listed in the order of most mentioned, concerns included (1) intended use of the data, (2) unauthorized access to data, (3) location tracking, (4) comfort, battery life and wearability of the device, (5) accuracy of the data, and (6) additional security concerns. Table 6 provides example responses regarding these concerns.

Table 6: Additional Concerns regarding Wearable Devices and Health Data*

Type of Concern	***Example Responses***
Intended Use of Data (17)	"I'm concerned if my insurance company could ever use the information from my Fitbit against me, like by charging me more."
	"used to implicate someone in a crime (i.e. why was your blood pressure so high at this moment in time, you should have been in bed)"
Unauthorized Access to Data (17)	"I'm worried that information the collect will be sold to 3rd parties without my knowledge"
	"just a normal hacker getting to it and pretending to be me if asked too much personal questions"
Location Tracking (11)	"I am more concerned with location tracking and information about my running routes/locations being stored than my actual health data"
	"GPS data tracked worries me more"
Comfort, battery life, wearability of device (7)	"the battery should last long for 24 hours"
	"I'm a little concerned if the wearable device itself which uses wireless technology harms our body in anyway"
Accuracy of Data (6)	"I am sometimes concerned with the accuracy of the health data it is collecting"
	"My main concern is really about accuracy of data collected"
Additional Security Concerns (5)	"Just because some sites/service is secure now does not mean that they will never be compromised or sell out down the road"
	"How its stored on their end. Is it anonymized or not?"

**Numbers in parentheses reflect how many participants mentioned this concern.*

Discussion & Significance

The purpose of this research was to determine (1) consumers' awareness or and concern for health data privacy, (2) how device manufacturers are informing consumers of current privacy practices, and ultimately, (3) if the data privacy practices adopted by the wearable industry align with consumer interactions with and understanding of wearable devices and the data they collect. Through the implementation of two consumer surveys, various findings regarding users' awareness of, concern for, and actions towards data privacy were able to be extracted. This information can be used to drive policy change within the wearable industry to better inform consumers and protect their health data.

Consumer Awareness and Concern for Health Data Privacy

In total, survey participants rated their health data privacy concerns, when in relation to wearable devices, as approximately a 3 ("neutral") on a 1-5 Likert scale. Some may argue a neutral response on a Likert scale simply means indifference towards a particular subject, however, one may also argue that the neutral option is made available as an "opt-out" option for participants that do not know enough about the subject. Another way to state the "neutral" option is to say the participant "neither agrees nor disagrees" and more information on the subject may sway a participant towards a particular polarity. Therefore, this "neutral" concern ("3" on a Likert scale) towards health data privacy, as expressed by survey participants, has been interpreted as a result of an uninformed consumer base. In other words, consumers lack the information necessary to make a polar decision regarding their health data privacy concerns. Furthermore, survey results indicated that those who had obtained education past that of a high school diploma had a significantly higher concern for privacy than those who had not ($p <$

0.0001); this further supports the notion that a "neutral" concern is largely due to an uninformed population.

Past research into wearable data privacy has tended to be concerned with all data types, including health, financial and social media data. As discussed in the literature review, when presented in this fashion, health data tends to be considered one of the least risky types of data to share (Lee et al., 2015). Therefore, this research sought to focus exclusively on health data in order to determine if specific data types, such as heart rate or emotional data, are of higher concern than others. Moreover, it was hypothesized that if consumers were aware of the possible risks (secondary data) associated with each collected data type (primary data) then concerns would be increased. Results, as shown in Table 2, demonstrate that consumers are least concerned about data that is familiar to them, such as heart rate and the number of calories burned. These data types have been integrated within wearable devices from their outset; therefore, consumers may have had time to understand the risks associated with collecting this data. In contrast, the data types of most concern were those in which a risk of a specific disease was able to be extracted from it as well as emotional data (concern: 3.21 ± 1.19 and 3.31 ± 1.18, respectively). Thus, collection of more familiar health data types is less concerning to device users; whereas, data that is less familiar, harder to measure and, ultimately, less quantifiable, such as emotions, raise a bigger flag to consumers. This may be for a variety of reasons, including (1) consumers feel device companies should not have access to this type of information, (2) consumers do not trust the accuracy of the algorithms or (3) because they understand the implications of certain types of data becoming public. Each of these possible hypotheses is supported within the "user actions" and "open-ended" sections discussed in more detail below.

It was hypothesized that some participants concern for data privacy may be lesser because they believe there are regulations already in place to protect their data. Although it is true that the Federal Trade Commission (FTC) has oversight over wearable device companies, there are currently no wearable-specific regulations in place. Rather, companies are encouraged to abide by the Fair Information Practices Principles (FIPPS), a group of guidelines for the use and sharing of electronic data (Privacy Online, 2000). It has been recognized, however, that some of these principles, specifically "notice and choice" and "data minimization" are no longer applicable in the world of big data (Internet of Things, 2015). Furthermore, more stringent regulations, such as the Health Insurance Portability and Accountability Act, which protect personal health information (PHI) when it is collected by a covered entity, do not apply to wearable device companies. This leaves health data collected by wearable devices to be regulated at the discretion of the wearable company. However, survey results indicate that many consumers falsely believe there are wearable-specific regulations currently in effect to protect their data. Specifically, 39.7% of participants stated that there are regulations to protect wearable data privacy, yet when asked to name any of those regulations most participants stated similar answers, such as "I can't name any, but I know there should be." Still, others considered HIPAA or the Medical Device Regulations ("MDR") to apply to wearable device data (Table 3). This should be a red flag for policy makers, as there is currently a large portion of wearable device users who may be engaging in riskier behavior than they otherwise would like to if they were more aware of the current wearable regulatory structure. When asked simply if there should be additional regulations, regardless of ones that may currently be in place, over three-quarters (79.4%) of participants responded affirmatively (Figure 10). This suggests that many consumers

perceive that wearable device companies today are not doing a good enough job of self-regulating, and would like for policy makers to step in.

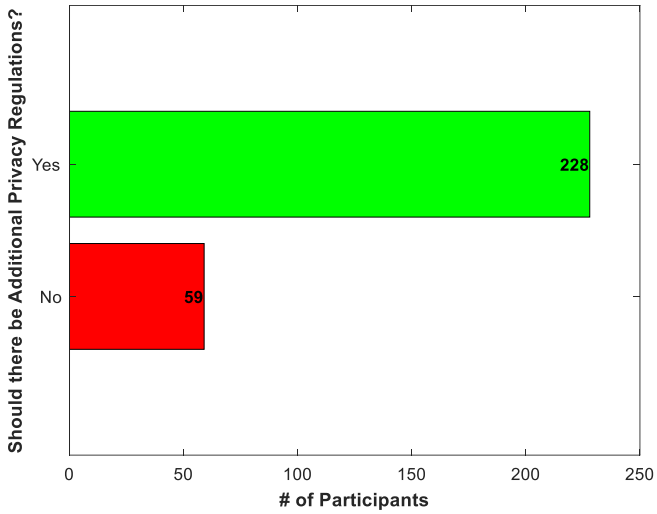

Figure 10: Number of participants that think there should be additional regulations to protect the privacy of health data collected by wearable devices.

Finally, device users' interactions with their devices and mobile applications were analyzed in order to determine if consumers' concerns for data privacy are reflected within their behaviors. Past research has analyzed some common user actions, such as changing default privacy settings and sharing data with friends; however, no past studies, to the best of the authors knowledge, have investigated *why* users act in a specific way (Cheung et al., 2016; Jensen et al., 2005; Williams et al, 2017). Consequently, this research attempted to determine if consumers do in fact engage in privacy-preserving behavior because they are concerned about their data or if they claim to be concerned, but their actions do not follow suit. Three actions were focused on within this study, including (1) sharing data with third-party apps, (2) inputting information when prompted during application installation, and (3) inputting additional information during normal application usage.

First, it was found that 131 participants (74%) do not connect to additional third-party apps; and, of these, 60 participants cited privacy concerns. Specifically, users were concerned

about others, such as friends, coworkers, companies and hackers, having access to their data. Similarly, the few number of participants (n = 14) that stated that they do not input all their information when installing an application most commonly cited concerns with sharing data with others as their reasoning. Finally, most participants (n = 232) did not enter additional information, such as blood pressure or glucose, during normal application usage. While the majority stated this was because they did not track any other information, 43 participants cited privacy-related concerns.

Thus, assuming some of the same participants chose privacy-related reasons for multiple of the actions above, at minimum 60 participants have some form of privacy concern, which correlates to 21% of the total sample population. This, again, suggests that data privacy needs to be better addressed by device manufacturers and policy makers. Moreover, consumers' may be more likely to download or fully utilize the functionalities of a mobile application if they felt their data was more protected.

Privacy Policy Effectiveness

Privacy policies serve as a means for wearable device companies to explicitly convey to consumers what data they collect, how they use said data, and with whom it is shared. However, as device functionalities have increased, the complexity of privacy policies has increased as well. Consequently, nearly three-quarters of survey participants stated that they had never read a privacy policy before. Of more interest, however, is the reasoning behind this inaction. Of the 213 participants that have never read a privacy policy, 87% cited reasons that indicate a failure on the part of the privacy policy maker. Specifically, people think the policies are too long or too difficult to understand, or, perhaps most concerning, is that people feel as if they are unable to change *any* of their privacy settings so, reading the policy is pointless.

The notion that privacy policies are too difficult to understand was tested when participants were given an excerpt from the Fitbit policy regarding how the collected data may be used and participants were asked to state how they felt. Over one-quarter of participants stated that they felt "concerned", "surprised" or "confused," most commonly because the wording was "vague" and "left a lot open to interpretation" (Table 5). This further demonstrates that privacy policies are doing a poor job of conveying information to the users and; therefore, should not be the primary mode of communication between companies and device users. An alternate suggestion, explained in more detail within the "Policy Recommendations" section below, would be to allow manufacturers' to implement various tiers of privacy and apply for product-certification, therefore, decreasing consumer confusion.

Wearable Industry Self-Regulation

To reiterate, the purpose of this research was to determine (1) consumers awareness and concern for their health data privacy, (2) how device manufacturers' address and inform consumers about current data privacy practices, and finally (3) if the data privacy practices currently employed by the wearable device industry aligned with how consumers interact with their devices and understand health data privacy. From research questions one and two, it was determined that consumers are largely unaware of the possible risks associated with sharing data collected by wearable devices; and, approximately three-fourths consumers misunderstand the current regulatory structure in place to protect data privacy. Additionally, approximately one-fifth of the population chooses to not partake in certain actions in order to limit who (e.g. friends, companies, hackers) has access to their data. Finally, privacy policies, which are primarily utilized as a means of informing consumers, tend to instead leave approximately one-third of consumers skeptical of current data practices. Therefore, although privacy concerns are highly

variable, as supported by past literature, this research was able to quantify that between 20-33% of the population is highly concerned about the data privacy practices currently employed by wearable device companies. In conclusion, self-regulation within the wearable device industry has not been satisfactory thus far.

To further this conclusion, it was found that data privacy practices are not the only concern to wearable device users, rather there are also many other risks associated with wearable devices that may be more apparent to individuals. As such, participants were given the opportunity to describe any additional concerns that they may have. Responses were able to be broken into six categories, including (1) intended use of the data, (2) unauthorized access to data, (3) location tracking, (4) comfort, battery life and wearability of the device, (5) accuracy of the data, and (6) additional security concerns. Interestingly, the top two concerns were in fact privacy-related. For example, there were multiple instances of participants being concerned about "insurance companies", or the "government" using the data against them. This is especially relevant as multiple recent news reports have cited wearable data being used to convict people of crimes (Watts, 2017). Furthermore, location tracking, especially regarding running routes, was of high importance to some users, while others were concerned about the wearability of the device and accuracy of the data. For example, one participant stated, "I'm a little concerned if the wearable device itself which uses wireless technology harms our body in anyway." Therefore, it is inferred that wearable device users *are* concerned about the current regulatory state of the wearable device industry, from both a data privacy and device hardware perspective.

Policy Recommendations

As suggested from this research, federal privacy and security regulations currently in effect, such as HIPAA, are insufficient in protecting wearable device users' health data. However, new, recommended regulations may face many issues, including, (1) difficulty passing through Congress, (2) inability to enforce, and (3) quickly becoming outdated and insufficient. To elaborate, wearable device companies generally consist of major technology players, such as Apple, that have a vested interest in maintaining self-regulation; and, furthermore, these companies have the funds available to lobby policy makers and key government officials. As such, more stringent data privacy regulations would be extremely slow and difficult to pass through Congress. Secondly, the government, specifically agencies such as the Federal Trade Commission, lack the man-power necessary to effectively regulate the wearable technology industry. Regulations are often thought of as limiting the capabilities of companies, and, therefore, companies will seek out loopholes in order to continue their current practices. Finally, as demonstrated by the Fair Information Practices Principles, even when policies are able to be adopted by the federal government, they often quickly become outdated and insufficient. For example, the FIPPS, which were developed in 1974 and are still encouraged today, identify "data minimization," or collecting a minimal amount of data, as a main pillar to data privacy, which is in direct opposition to IoT technology. Because of these limitations, it is not recommended that a federally-mandated privacy and security policy be introduced to Congress.

Rather, it is suggested that a non-government, yet widely-respected organization, such as the Institute of Electrical and Electronics Engineers (IEEE), develop a three-tier privacy certification that wearable device companies are able to apply for, but are not forced to adhere to. As shown above, the federal government lacks the speed, bandwidth and education to properly

regulate the data collected by wearable devices. However, a third-party organization, such as IEEE, has a large, informed and voluntary population that does not need to jump through loopholes to recommend standards. A three-tier system would consist of bronze, silver and gold certifications which correlate to increasingly stringent privacy and security requirements. For example, the bronze certification would consist of the minimum requirements currently enforced by the federal government, such as adhering to the regulations currently set forth within the FTC Act and Children's Online Privacy Protection Act ("Statutes Enforced…", 2018). In contrast, the gold certification would be given to companies that, for example, ensure that absolutely no data, whether deidentified or not, will be shared or sold to third parties. Other gold characteristics may involve abstaining from using data for any purpose other than displaying to the user, clearing all data servers after an allotted amount of time and voluntarily reporting to IEEE any privacy breaches, regardless of how insignificant. As such, wearable device companies will be able to decide for themselves which level of privacy they would like to implement into their products, apply for said certification, and undergo an IEEE review in order to be able to advertise it on their products.

As opposed to a federal government regulation or law, a system such as this would be voluntary for wearable device companies. Some may argue that in not forcing companies to participate, there will be no incentive to do so. However, as more research, such as the one above, illustrates that consumers are becoming increasingly privacy-conscious, consumer demand will force companies to participate in these programs. Furthermore, a three-tier certification system is concise, and easy for consumers to understand. Consumers will no longer need to read complex privacy policies to infer how their data is being collected and used. Rather, a simple, pyramid structure will indicate to them how their data is being handled. Therefore,

consumers can easily identify which tier of privacy they prefer and which products they trust with their personal data.

Limitations

The above study attempted to minimize bias as much as possible while reflecting the opinions of an evenly distributed sample. Despite this, limitations within the study occurred as a result of the chosen methodologies. For example, both Survey 1 and 2 were skewed slightly towards a male and highly educated (> high school diploma) population. Moreover, both populations were predominantly White and Asian, with other race being vastly underrepresented. This was a limitation of the chosen survey platform, which included advertising through the Internet, and could only have been improved through in-person recruitment. Finally, the privacy policy analysis only included policies from large, technology companies, and, as such, the results are biased to reflect the policies of the leading wearable companies, rather than smaller businesses.

Conclusion

This research, through an online, crowd-sourced survey platform, examined 683 individuals' awareness, concern and understanding of current data privacy practices within the wearable device industry. Though previous literature has utilized surveys to gauge consumers' perception of privacy, this research differed in that participants were presented *solely* with health data risks, rather than *all* data types, such as financial or social media data. Furthermore, rather than simply referring to the primary data collected by wearable devices, such as heart rate, participants were made aware of the secondary analytics that can be estimated from the primary data, such as stress levels. As such, survey participants were able to better understand the risks involved with sharing health data and make a more informed decision about whether they would be comfortable sharing said data.

Survey results suggest that there is a large lack of awareness regarding possible risks involved with sharing data collected by wearable devices. Most participants were unaware of the possible secondary information that can be estimated from primary data. Furthermore, nearly three-quarters of participants (67.2%) has a false understanding of current federal regulations in place to protect data privacy. Therefore, it was concluded that most wearable device consumers are uninformed about the risks, and, consequently, lack the necessary information to have an educated opinion about their concern for data privacy.

This lack of education is enhanced due to the mode of communication between companies and consumers – privacy policies. Many policies are long, difficult to understand and contain an abundance of legal jargon, which confuses and deters consumers from ever reading them. As such, this research attempted to omit some of the factors that prevent consumers from reading policies by simply giving participants a short excerpt with minimal difficult language.

Participants were asked how the information contained within the excerpt made them feel. Over one-quarter (28.7%) stated they felt “concerned”, “surprised” or “confused”, as the statement “leaves a great deal open to interpretation as far as what they use my data for” and was very “vague.” From these results, it was concluded that privacy policies, as they are written today, are not properly informing consumers about the collection and use of their data, and consequently, should not be primary mode of communication between companies and consumers.

Despite this lack of awareness and understanding about privacy, some consumers are still taking preemptive measures to control their data privacy. It was determined that approximately 1 in 5 people (21%) choose to limit their data sharing in fear of privacy-related concerns, such as hackers or companies having too much of their data. Furthermore, data privacy is not the only concerning feature of wearable devices. Although many participants suggested that the unintended use or unauthorized access of data was of highest concern, still others wondered about the physical safety of the device and the accuracy of the data. Many consumers are blindly wearing these devices, assuming there are no physical side-effects, or adjusting their daily routines as a result of the data, however, these devices are still in their infancy and, as such, have not had the life-span to be sufficiently tested.

Ultimately, it is suggested that a non-government body, such as IEEE, develop a three-tier data privacy certification that wearable companies may apply for. Consumer demand for increased privacy measures would drive companies to voluntarily apply for a specific privacy tier. Moreover, consumers would no longer need to read lengthy privacy policies to understand how their data is used. Overall, this solution would increase consumer knowledge, allowing them to more readily consider the risks and make informed decisions regarding their own personal health data.

References

Anderson, C. L., & Agarwal, R. (2011). The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. In *Information Systems Research, 22*(3), 469-490. doi:10.1287/isre.1100.0335

Atienza, A. A., Zarcadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W.-Y. S., & Pritts, J. (2015). Consumer Attitudes and Perceptions on mHealth Privacy and Security: Findings From a Mixed-Methods Study. In *Journal of Health Communication*, 20(6), 673–679. doi:10.1080/10810730.2015.1018560

Cheung, C., Bietz, M. J., Patrick, K., & Bloss C. S. (2016). Privacy Attitudes among Early Adopters of Emerging Health Technologies. In *PLoS ONE, 11*(11). doi:10.1371/journal.pone.0166389

Comstock, Jonah. (2015, December 01). ABI: 30M wearable sensors shipped in 2012. *HIMSS Media.* Retrieved October 09, 2017, from http://www.mobihealthnews.com/19448/abi-30m-wearable-sensors-shipped-in-2012

Felt, A. P., Engelman, S., & Wagner, D. (2012). I've Got 99 Problems, But Vibration Ain't One: A Survey of Smartphone Users' Concern. In *SPSM '12 Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, 33-44. doi:10.1145/2381934.2381943

Felt, A. P., et al. (2012). Android Permissions: User Attention, Comprehension, and Behavior. In *Symposium on Usable Privacy and Security (SOUPS).* doi:10.1145/2335356.2335360

Fitbit Privacy Policy (2017, September 28). *Fitbit, Inc.* Retrieved February 28, 2018 from https://www.fitbit.com/legal/privacy-policy

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

Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017. (2017, August 24). *Gartner, Inc.* Retrieved October 09, 2017, from http://www.gartner.com/newsroom/id/3790965

Global Wearable Sensors Market Development and Demand Forecast to 2020. (2015, May). *P&S Market Research.* Retrieved September 10, 2017, from https://www.psmarketresearch.com/market-analysis/wearable-sensors-market

Hoyle, R., et al. (2014). Privacy Behaviors of Lifeloggers using Wearable Cameras. In *Ubicomp '14*. doi:10.1145/2632048.2632079

Internet of Things: Privacy and Security in a Connected World (2015, Jan.) *FTC Staff Report*. Retrieved March 3, 2018 from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. In *International Journal of Human-Computer Studies, 63*(1-2), 203-227. doi:10.1016/j.ijhcs.2005.04.019

Lamb, K., Huang, H.-Y., Marturano, A., & Bashir, M. (2016). Users' Privacy Perceptions About Wearable Technology: Examining Influence of Personality, Trust, and Usability. In *Advances in Human Factors in Cybersecurity*, 55–68. doi:10.1007/978-3-319-41932-9_6

Lee, L., Egelman, S., Lee, J. H., & Wagner, D. (2015). Risk Perceptions for Wearable

Devices. In *ArXiv:1504.05694 [Cs]*. Retrieved from http://arxiv.org/abs/1504.05694

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

Loechner, Jack. (2016, December 22). 90% of Today's Data Created in Two Years. *The Center for Media Research.* Retrieved October 09, 2017, from https://www.mediapost.com/publications/article/291358/90-of-todays-data-created-in-two-years.html

Lopez, G., Marin, G., & Calderon, M. (2016). Human aspects of ubiquitous computing: a study addressing willingness to use and privacy issues. In *Journal of Ambient Intelligence and Humanized Computing*, *8*(4), 497-511. doi:10.1007/s12652-016-0438-4

Lowens, B., Motti, V. G., & Caine, K. (2017). Wearable Privacy: Skeletons in the Data Closet. In *2017 IEEE International Conference on Healthcare Informatics*. doi: 10.1109/ICHI.2017.29

Marakhimov, A. & Joo, J. (2017). Consumer adaptation and infusion of wearable devices for healthcare. In *Computers in Human Behavior, 76*, 135-148. doi:10.1016/j.chb.2017.07.016

Motti, V. G., & Caine, K. (2015). Users' Privacy Concerns About Wearables. In *International Financial Cryptography Association 2015.* doi:10.1007/978-3-662-48051-9_17

Privacy Online: Fair Information Practices in the Electronic Marketplace (2000, May). *Federal*

Trade Commission. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf

Privacy Policy (2018, Jan. 19). *Apple, Inc.* Retrieved March 3, 2018 from https://www.apple.com/legal/privacy/en-ww/

Privacy Statement for Garmin Connect and Compatible Garmin Devices (2017, July 11). *Garmin, Inc.* Retrieved February 28, 2018 from https://connect.garmin.com/en-US/privacy

Samsung Global Privacy Policy (2017, Dec. 21). *SAMSUNG,* Retrieved March 3, 2018 from https://www.samsung.com/us/account/privacy-policy/

Statutes Enforced or Administered by the Commission (2018). *Federal Trade Commission*, Retrieved May 8, 2018, from https://www.ftc.gov/enforcement/statutes

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. In *Journal of the American Medical Informatics Association,* 22(e1), e28–e33. doi:10.1136/amiajnl-2013-002605

Talebi, N., Hallam, C., & Zanella, G. (2016). The new wave of privacy concerns in the wearable devices era. In *2016 Portland International Conference on Management of Engineering and Technology (PICMET),* 3208–3214. doi:10.1109/PICMET.2016.7806826

The wearable future (2014, October). *PwC.* Retrieved October 09, 2017, from https://www.pwc.com/us/en/technology/publications/wearable-technology.html

Watts, Amanda (2017, Apr. 26). Cops use murdered woman's Fitbit to charge her husband. *CNN Newsource.* Retrieved March 5, 2018 from https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html

Williams, M., Nurse. J. R. C., Creese, S. (2017). "*Privacy is the Boring Bit"*: User Perceptions and Behaviour in the Internet-of-Things. In *15th International Conference on Privacy, Security and Trust (PST'2017).* http://www.cs.ox.ac.uk/files/9213/2017-pst-wnc-preprint.pdf

Yang, H., Yu, J., & Zo, H. (2016). User acceptance of wearable devices: An extended perspective of perceived value. In *Telematics and Informatics, 33*(4), 256-269. doi:10.1016/j.tele.2015.08.007

Zhang, M., Luo, M., Nie, R., & Zhang, Y. (2017). Technical attributes, health attribute, consumer attributes and their roles in adoption intention of healthcare wearable technology. In *International Journal of Medical Informatics, 108*, 97-109. doi:10.1016/j.ijmedinf.2017.09.016

Appendix

Appendix A: Survey 1

This survey focuses on any consumer wearable device ('wearables'), and their corresponding mobile applications, that contains sensors to measure individual health data. Examples may include, but are not limited to, the Apple Watch, Fitbit, Polar Chest Strap, or Nike+ Shoe Sensor. This survey is not concerned with *medical* wearable devices prescribed by physicians.

1. The questions within this survey are focused on consumer wearable devices that track health data.
    - True
    - False
    - I don't know

2. Have you previously used or currently use a consumer wearable device?
    - Yes, please specify which device:
    - No
    - I don't know

3. How concerned do you feel about your health data privacy when it is collected and stored by a wearable device?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

HIPAA is a federal regulation that limits the accessibility and availability of individual personal health information.

4. Do you think that health data collected by wearable devices is regulated by HIPAA?
    - Yes
    - No
    - I don't know

5. Are you *aware* that when a wearable device measures your <data>, it is possible for your <analytics> to be determined?
    - Yes
    - No

<data>	***<analytics>***
Heart rate	Sleep patterns, sex patterns, respiration rate, risk of heart disease

Heart rate variability	Stress levels, sleeps patterns
Steps	Risk of obesity
Calories burned	Sex patterns, risk of obesity
Floors climbed	Risk of obesity
Blood oxygen (SpO2)	Risk of heart disease
Respiration rate	Sleep patterns, risk of respiratory disease
Eye movement	Sleep patterns
Body temperature	Fertility cycles, period cycles
Sweat (galvanic skin response)	Emotions, risk of brain disorders
Sun exposure	Risk of cancer
Force per step	Risk of brain disorders
Brain patterns	Sleep patterns, stress levels

6. How *concerned* do you feel about your <analytics> being analyzed or tracked?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

7. How concerned would you feel if your wearable was able to measure your <future data>?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

<future data>
Blood pressure
Glucose
Nutritional intake
Hormone levels
Hydration level
Muscle movement (EMG)
Alcohol intake

Most wearable devices require users to download a mobile application in order to unlock all of the device features.

8. Many applications allow you to link data from other third-party applications, such as MyFitnessPal, or share your data with your friends. Have you ever purposefully shared your data with either of these third parties?
    - Yes, please specify which parties:
    - No
    - I don’t know

9. If yes, why did you choose to share your data?

10. During installation, many applications will ask for personal information such as height, weight, gender, or activity levels. When installing these applications, do you normally enter all your personal information?
    - Yes
    - No, please specify which information you choose to exclude:
    - I don't know

11. Many applications allow you to input additional data, such as glucose levels, medications and blood pressure into the application. Do you normally enter this information into your application?
    - Yes, please specify which information you choose to input:
    - No
    - I don't know

12. How concerned do you feel about your health data privacy when it is collected and stored by a wearable device?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

13. Do you have any other concerns regarding wearable devices and health data not addressed in this survey?

14. Please specify your gender.
    - Male
    - Female
    - Prefer not to answer

15. Please specify your race.
    - White
    - Latin American
    - Black or African American
    - Native American or American Indian
    - Asian or Pacific Islander
    - Other

- Prefer not to answer

16. Please specify your age.
    - Under 14 years old
    - 14-19 years old
    - 20-29 years old
    - 30-39 years old
    - 40-49 years old
    - 50-59 years old
    - 60-69 years old
    - Over 70 years old

17. Please specify your highest level of education achieved.
    - No schooling completed
    - 8th grade
    - Some high school, no diploma
    - High school graduate, diploma or the equivalent (e.g. GED)
    - Some college credit, no degree
    - Trade, technical or vocational training
    - Associate degree
    - Bachelor's degree
    - Master's degree
    - Professional degree
    - Doctorate degree
    - Other
    - Prefer not to answer

Appendix B: Survey 2

PLEASE NOTE:
All survey participants MUST currently use a wearable device. Please take your time in answering all questions. Incomplete or rushed surveys will be rejected.

This survey focuses on any consumer wearable device ('wearables'), and their corresponding mobile applications, that contains sensors to measure individual health data. Examples may include, but are not limited to, the Apple Watch, Fitbit, Polar Chest Strap, or Nike+ Shoe Sensor.

1. The questions within this survey are focused on consumer wearable devices that track health data.
    - True
    - False
    - I don't know

2. Do you currently use a consumer wearable device?
    - Yes
    - No
    - I don't know

3. Which device do you currently use?
    - Fitbit
    - Apple Watch
    - Garmin
    - Samsung
    - Jawbone
    - Xiaomi
    - Other: _____

4. How concerned do you feel about your health data privacy when it is collected and stored by a wearable device?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

5. Do you think that there are regulations in place to protect the privacy of health data collected by wearable devices?
    - Yes
    - No
    - I don't know

5.1. Can you name any of those regulations?

6. Are you aware of the federal regulation HIPAA (Health Insurance Portability and Accountability Act) and the purpose of this regulation?
    - Yes
    - No

6.1. Do you think that health data collected by wearable devices is regulated by HIPAA?
    - Yes
    - No
    - I don't know

7. Do you think there should be increased regulations to protect information collected by wearable devices?

8. Are you aware that when your wearable measures your <data>, it is possible for <analytics> to be extracted?
    - Yes
    - No

<data>	***<analytics>***
Heart rate	Sleep patterns, sex patterns, respiration rate, risk of heart disease
Heart rate variability	Stress levels, sleeps patterns
Steps	Risk of obesity
Calories burned	Sex patterns, risk of obesity
Floors climbed	Risk of obesity
Blood oxygen (SpO2)	Risk of heart disease
Respiration rate	Sleep patterns, risk of respiratory disease
Eye movement	Sleep patterns
Body temperature	Fertility cycles, period cycles
Sweat (galvanic skin response)	Emotions, risk of brain disorders
Sun exposure	Risk of cancer
Force per step	Risk of brain disorders
Brain patterns	Sleep patterns, stress levels

9. How concerned do you feel about your <analytics> being analyzed or tracked by a wearable device company?
    - Not at all concerned
    - Not very concerned
    - Neutral
    - Somewhat concerned
    - Very concerned

Most wearable devices require users to download a mobile application in order to unlock all of the device features.

10. Many applications allow you to link data to and from other third-party applications, such as MyFitnessPal or Endomondo. Have you ever purposefully shared your data with third party apps such as these?
    - Yes, please specify which apps: _____
    - No
    - I don't know

10.1. Why did you choose not to share your information?
    - I did not need the services that other third party apps provide
    - I did not want others (friends, coworkers, companies) to see my data
    - I am concerned about companies or hackers knowing too much of my personal information
    - I've never thought about connecting to another app or sharing my data
    - Other: _____

11. During installation, many applications will ask for personal information such as height, weight, gender, or activity levels. When installing these applications, do you normally enter all your personal information?
    - Yes
    - No, please specify which information you choose to exclude: _____
    - I don't know

11.1. Why did you choose to exclude some information?
    - I am concerned about companies or hackers knowing too much of my personal information
    - I did not want others (friends, coworkers, companies) to see my data
    - I did not feel like inputting all my information
    - It takes too long to input all my information
    - Other: ____

12. During normal use, many applications allow you to input additional data, such as glucose levels, medications and blood pressure into the application. Do you normally enter this information into your application?
    - Yes, please specify which information you choose to input: _____
    - No
    - I don't know

12.1. Why do you choose to not enter additional information?
    - I don't track any other information
    - It takes too long to input additional information
    - I'd like to input additional information, but I often forget
    - I am concerned about companies or hackers knowing too much of my personal information
    - Other: _____

13. Have you ever read the privacy policy for your wearable device or its mobile application (for example: Fitbit or Apple privacy policy)?
    - Yes
    - No

13.1. If not, why have you not read the privacy policy?
    - They are too long
    - The wording is too difficult to understand
    - I don't care how the company uses my data
    - I don't think I can change any privacy settings so there's no point to reading the privacy policy
    - Other: _____

The following section asks you to read an excerpt from the Fitbit privacy policy and then answer questions about the excerpt.

"We use the information [we collect] to provide you with the Services you request; understand how you and other users interact with the Services; track exercise, activity and other trends; provide customer support; troubleshoot and protect against errors; perform data analysis and testing; conduct research and surveys; and develop new features and Services."

14. How does the above statement make you feel? Please explain why you feel that way.
    - Good: _____
    - Safe: _____
    - Concerned: _____
    - Surprised: _____
    - Confused: _____
    - Other: _____

"We may share non-personal information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual. We may disclose such information publicly and to third parties…" (Fitbit Privacy Policy; Updated September 28, 2017)

15. What does the above statement mean?
    - Fitbit may share any information about you, including your name, to the public
    - Fitbit may only share information with whom the user (you) requests it to be shared with
    - Fitbit may share some information about you as long as personal identifiers, such as name, have been removed
    - Fitbit may share any information about you, including your name, with third parties, such as advertisers
    - I don't know

16. How concerned do you feel about your health data privacy when it is collected and stored by a wearable device?
    - Not at all concerned

- Not very concerned
- Neutral
- Somewhat concerned
- Very concerned

17. Do you have any other concerns regarding wearable devices and health data not addressed in this survey?

18. Please specify your gender.
    - Male
    - Female
    - Other

19. Please specify your race.
    - White
    - Latin American
    - Black or African American
    - American Indian or Alaska Native
    - Asian
    - Native Hawaiian or Pacific Islander
    - Other

20. Please specify your age.
    - Under 14 years old
    - 14-19 years old
    - 20-29 years old
    - 30-39 years old
    - 40-49 years old
    - 50-59 years old
    - Over 60 years old

21. Please specify your highest level of education achieved.
    - No schooling completed
    - 8^{th} grade
    - Some high school, no diploma
    - High school graduate, diploma or the equivalent
    - Trade, technical or vocational training
    - Associate degree
    - Bachelor's degree
    - Master's degree
    - Professional degree
    - Doctorate degree