Wearable Privacy: Skeletons in The Data Closet

Byron Lowens
School of Computing
Clemson University
Clemson, SC
blowens@g.clemson.edu

Vivian Genaro Motti
Volgenau School of Engineering
George Mason University
Fairfax, VA
vmotti@gmu.edu

Kelly Caine
School of Computing
Clemson University
Clemson, SC
caine@clemson.edu

***Abstract*—Equipped with sensors that are capable of collecting physiological and environmental data continuously, wearable technologies have the potential to become a valuable component of personalized healthcare and health management. However, in addition to the potential benefits of wearable devices, the widespread and continuous use of wearables also poses many privacy challenges. In some instances, users may not be aware of the risks associated with wearable devices, while in other cases, users may be aware of the privacy-related risks, but may be unable to negotiate complicated privacy settings to meet their needs and preferences. This lack of awareness could have an adverse impact on users in the future, even becoming a "skeleton in the closet." In this work, we conducted 32 semi-structured interviews to understand how users perceive privacy in wearable computing. Results suggest that user concerns toward wearable privacy have different levels of variety ranging from no concern to highly concerned. In addition, while user concerns and benefits are similar among participants in our study, these variables should be investigated more extensively for the development of privacy enhanced wearable technologies.**

I. Introduction

The popularization of wearable technology has enabled many of the original ideas of pervasive computing to come to fruition [1]. Wearables allow the usage of a variety of sensors into multiple environments, facilitating continuous data collection to offer immense benefits to consumers [2]. These technologies and their robust set of features also have the potential to assist researchers with early detection of diseases and personalized treatment of medical conditions [3]. Piwek et. al [4] mentioned that 15% of the consumers in the United States currently use wearable technologies, such as smartwatches and fitness bands. From a commercial perspective, based on results from International Data Corporation (IDC) 72.1 million wearable devices were shipped in 2015, a growing trend if compared to 2014 when 26.4 million devices were shipped. By 2019, wearable sales are expected to reach 155.7 million units [5]. This widespread adoption of wearable technologies has the potential to provide immense benefits to individual consumers and the society as well [6].

Available in a myriad of form factors that support several applications, including fitness and healthcare domains, wearables have revolutionized the life of "quantifiers" or those users interested in systematically tracking and analyzing their everyday habits in detail and "non-quantifiers" alike. Quantifiers are finally able to track themselves in a more automated and affordable fashion [7], [8] and non-quantifiers can promptly get feedback, alerts, and notifications, especially with wrist-worn devices (WWDs).

Fitness trackers and smartwatches were among the top selling consumer-grade wearable devices of 2016, showing promise for use in health-related applications in daily life [9]. These devices and their related applications and services enable users to collect personalized data about location, steps taken, food intake and sleep patterns, among others. In addition to these affordances, wearables are also able to monitor physiological parameters, including heart rate and blood pressure [10]. Consumers are enthusiastic about the ability to visualize and analyze their health-related data, and improve their overall behavioral patterns and quality of life [11], [12], [13], [14], [15], [16].

Traditionally, an individual's health information has always been considered as private. Data have also been traditionally stored in health care provider's databases, and by law, through Health Insurance Portability and Accountability Act (HIPPA) compliance, these offer some privacy protection. Due to the proliferation of commercial wearable devices, health information is now able to be collected, stored, and handled by multiple services that do not offer as strong privacy protections [4].

By collecting personal data continuously and sharing it online, digitally and/or with third-parties, users become more vulnerable to criminal abuses, including the misuse of their personal data to adjust healthcare insurance policies and premiums according to daily behaviors, activities and pre-existing medical conditions. Much personal health data collected by existing wearable applications is not HIPPA-compliant [17] unless the technology was designed and subject to Federal Trade Commission (FTC) jurisdiction about access and storage of information on devices [18]. Most user personal health data is transferred to external entities (e.g. the device manufacturer or a third party) outside the control of the user who is generating this data [19]. Users are not always aware of the threats, risks and implications involved and in some instances, they may even have difficulties in understanding the imposed risks. In other cases, users feel they have no other choice than to sacrifice their privacy to obtain the benefits and more personalized services provided by their devices [20].

To gain further insight into users' perceptions, current understanding, and potential concerns about wearable privacy we conducted 32 semi-structured interviews asking participants

978-1-5090-4881-6/17 $31.00 © 2017 IEEE
DOI 10.1109/ICHI.2017.29

about their privacy concerns, sharing preferences, and their understanding and current usage of privacy controls on their wearable devices. This paper consolidates our findings and identifies key concerns, benefits, misconceptions, trade-offs, and solutions that users' have about the collection, use, and sharing of their wearable data. Better understanding users' perceptions and behaviors help stakeholders to implement privacy-enhanced solutions and can lead to solutions that allow users to manage their privacy [21], [22].

A. Research Questions

While the complexity of privacy requires context-specific studies, a holistic understanding of privacy concerns enables an integrated view of related problems, abstraction and prioritization of concerns. In this context, this work seeks to answer the following research questions: (i) How do users understand privacy in the context of wearables, specifically WWDs?; (ii) What are the benefits and concerns related the collection and sharing of health data collected via WWDs and when do these concerns arise?; (iii) What are common misconceptions users' share about health related data on WWDs?

B. Contribution

The primary contribution of this work shows that concerning wearable privacy: (i) there is variety in the levels of user concern about it ranging from almost no concern to highly concerned. For users who are concerned about wearable privacy, it is not always clear the actual risks, and potential implications of privacy violation; (ii) several factors define the users' concerns, including the unintended usage of their data and the lack of control over their data; these concerns are linked to the collection and use of wearable data. Identifying and understanding these factors will allow us to identify unexplored design alternatives that enable users to have more control over their health-related data which can facilitate toward the implementation of privacy-enhanced solutions that may allow users to better manage their privacy on WWDs [21], [22].

II. Related Work

Private information belonging to an individual or a group of individuals should be protected and not disclosed to third parties without that individual's intention and consent [23]. The concept of contextual integrity [24] was introduced as an alternative benchmark for privacy, demanding that data collection and distribution be suitable to that context and observe governing norms of distribution within it. Private data should have a corresponding degree of confidentiality that aligns with specific user needs. Privacy is one of the most persistent social issues connected to information technology [24] and is a complex concept that can take on various definitions in different contexts [25]; in the scientific [26], industrial domains [27] and standardization bodies [28]. No privacy consensus exists [27], as users perceive it differently, due to personal [29], [30] or cultural [31] aspects. Sharing information can be critical or trivial depending on individual perceptions and involving circumstances. In the context of this work, privacy refers to the ability to not exhibit information, to prevent external access or observation by the society when unintended.

In this section, we present and discuss related work, highlighting privacy in wearable computing, and privacy with regards to health information.

A. Privacy in Wearable Computing

While the widespread adoption of wearable devices is expanding rapidly [32], the emergent risks associated with the collection and sharing of data using such devices is still poorly understood by users [33] and not adequately addressed by stakeholders [2], [34]. Prior work has cited privacy as key user concern for users in their adoption of pervasive computing technologies [35], [36] and has been cited as a key concern specifically in wearable computing [37], [16]. Wearable devices have potential to collect and transmit large amounts of physiological, and environmental data that some users consider innocuous [16], [33], [38], [6], [19]. Wearables can sense, process, and store information continuously and discreetly [39] and users do not thoroughly comprehend, and may underestimate, the sensitivity of the information collected by wearable devices and the privacy risks involved [16].

Physiological and environmental data produced by WWDs can comprise sensitive information that can impart itself as emergent medical records [3]. This data can indicate records of one's activity levels that could be potentially used by a third party to evaluate an individual's health and well-being, possibly impacting insurance benefits, costs or health premiums [3], [38], [6]. Wearable devices are also often synchronized with social media sites for sharing information, which presents additional privacy risks [3]. Criminal actions can be planned using location information collected by wearable devices that is shared on social media sites. For example, a theft can be planned according to the analysis of displacement patterns of individual users [40]. Previous works have also identified privacy as a key concern associated with wearable devices from the user stand point [35], [41], [37]. Because of these unique concerns, previous research has investigated user perspectives and concerns related to the privacy of wearables devices.

Lee et. al investigated the perception of the general public linked to the risk of information disclosure which was associated with wearables [41]. The findings from this work reveal that privacy and security are at the top of users' overall concerns. The results from this study also show that users self-reported privacy preferences are related to how they may react, even in situations that they are unfamiliar with. While this work provides insight into user acceptability in reference to data disclosure and general user concerns about wearable devices, 83% of participants from this study reported they did not own a wearable device. As the researchers mentioned, participants may not have a clear sense of the technology and may be underestimating the risk associated with the use of wearable devices. Our study focuses specifically on

current users of wearable devices who may have a better understanding of wearables and their capabilities. Prior work by [42] explored privacy about wearable health technologies in the workplace and challenges the assumption that users are becoming comfortable with perceived risks with wearable technologies. In this work, the researchers conducted a study of a workplace health campaign that depended on the use of step counting technologies and daily self-reporting of steps over the course of three weeks. This research explored the types of concerns employees express about the disclosure of step counts, and how they change over time. The main findings from this work show that there is a difference in concerns toward data disclosure to organizations that support health campaigns between people who chose to participate, versus those who do not. The results from this study also illustrate that concerns over data disclosure to employees, bosses or friends change over time. Although these results offer insight into privacy concerns toward wearable health technologies in the workplace, being held responsible for tracking physical activity at work can be unwelcoming for users and is quickly abandoned when the intervention is complete [43]. Participants in our study had owned their wearable devices on average for about nine months prior to the study.

Prior work also shows that user levels and types of privacy concerns vary based on the type of wearable device. Using a qualitative content analysis of online comments from wearable device users, [16] identified the privacy concerns of wearable users who commented online. The findings from this work indicate that privacy concerns about wearables are similar, but some cases are more specific than privacy concerns for mobile devices in general. The results from this work also illustrate that users have a keen awareness of impending privacy implications of wearable devices, but mainly during data collection and sharing. This work also claims that users' concerns about wearable privacy cover different facets of user interaction with wearables and in some instances, users are somewhat oblivious to potential privacy implications associated with using wearables. While this work offered valuable contributions to research on wearable privacy and provided general insights on users' concerns about it, this work collected data anonymously from online comments, and we do not know much about the user's profiles and demographics from this study population sample. Also, the methods in this study employ a relatively new research approach that is both exploratory and empirical and does not have a well-established and validated protocol concerning data collection and analysis.

Data from another exploratory study by [3] shows how user intent to avoid privacy issues by sharing sensitive information conflicts with the social propensity to share wearable data, generating undesirable behavior. The objective of this research was to address the gap between users' privacy concerns from using wearable devices and their actual behavior to identify a potential model for how this concept could be extended. This work suggested a theory based on a cognitive model that combines current theories with the Construal Level Theory (CLT). This theory illustrates how choices individuals make every day are based unconsciously on discounting purposes [44], [45], [46]. The results of this study demonstrate that behavior is driven more by actual short-term rewarding intentions, than by the general long-term risk-avoiding intentions. Although this work was the first that applied CLT to address the gaps between intentions and online behavior with wearable devices, only 60% of participants used a wearable device. In addition, the model in this work is suggested to be more appropriate for general online behaviors.

To better understand why people use wearables despite the privacy risks [40] conducted a qualitative study, that examined the perceived values of wearables that drive individuals' usage and disclosure of their data and the reasons why these values outweigh the privacy risk of wearable usage. The findings of this study reveal eight values that individuals perceive through the use of wearable devices. The researchers claim that these values indicate that respondents use wearables for activities that are intrinsically motivating and provide satisfaction. This research also shows that users have limited knowledge about the privacy consequences of using wearable devices and suggest that many users do not want to invest time and effort to understand how their personal data can be used and potentially exploited by stakeholders. The findings of this study only refer to the use of bracelets and watches in the particular context of self-tracking. This sample also only included wearable users from Switzerland, which does not make the results generalizable on a global scale.

While prior works have investigated and provided insight to these concepts, wearable computing faces dynamic changes and widespread adoption. There is a need to better understand current users' behaviors and concerns in what regards privacy risks, concerns and wearable technologies [17], [2], [47], [40], [48] which motivates our research.

B. Privacy and Health Information

Contemporary trends and advances in technology have led to patients and consumers becoming more involved in their personal health care through wearable devices and related services. Physicians have found these mobile health applications to be beneficial in increasing the access to healthcare and facilitating the communication between patient and medical provider [49]. While these advances offer conveniences to users, they also raise significant privacy concerns [33]. Whittaker [49] cited privacy and security as the main concern in a survey of 27 respondents from across the health and mobile health sections in the United States .

Concerns in reference to health related data have also been often raised in prior work [50], [51], [38], [52], [53], [33]. A user study conducted by [54] demonstrated that patients desire granular privacy control over which health information should be shared with individual recipients. This work also illustrated that for privacy to have any meaning, this type of control is necessary. All the popular health and wellness apps analyzed in [53] presented some risk to the consumer, and the privacy policies do not describe those risks. This work found that the biggest risks to the information privacy of users of

mobile health and fitness apps were technical in nature, usually due to unencrypted connections to third-party advertisers and analytics services, which often disclose personal information. It is imperative that the user becomes aware of the increasing privacy risk surrounding data collected by wearable devices [52]. This work also noted that these privacy risks comprise the collection of data without users' consent, transferring private health information to advertisers and data brokers, besides also presenting inadequate privacy policies and sending private health data via unencrypted networks. In addition to that, the data collected from wearable devices are not protected by Federal Agencies, and many users believe that because these mobile health applications collect health data, the data is protected by HIPAA [17]. While HIPPA has a restricted scope of protection with consumer health data, the expansion of wearable technologies moves too quickly for these federal agencies to update policies accordingly [52].

C. Existing Solutions

Existing solutions to address privacy issues vary. Schaub [25] proposed control mechanisms with a context model and privacy decision engine, focusing on Ubiquitous Computing in general. Ur [55] proposed a theoretical framework to handle cross-cultural issues in social media. The Privacy Mirrors Framework was created to ensure history, feedback, awareness, accountability, and change, concerning social, technical and physical environments [29]. This framework focuses on understanding the system. However, purely technical solutions for protection and control have been considered inappropriate [56] when users' actual behaviors are taken into account.

The National Health Service (NHS) in the United Kingdom adopted an approach with their regulatory framework for mobile apps, which can be classified as "medical devices" by the Medicines and Healthcare Products Regulatory Agency [57]. In fact, if this type of solution is applied to consumer wearables devices used for health-related purposes, this could persuade the private sector to provide access to their data collection practices, analysis, and measurement concerns [4].

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

III. Method

In this work, rather than proposing a technical solution, we focused on further investigating user behavior as it relates to wearable privacy. To identify key benefits, drawbacks, misconceptions, trade-offs, and solutions about the collection, use, and sharing of WWD data, we conducted 32 semi-structured interviews with existing users of wearable devices.

A. Recruitment

We recruited participants by: (1) posting flyer's with a call for participants around the campus of Clemson University; (2) digitally advertising the call for participation in the sports center at the University on TV screens located at the entrance of the building; and (3) publishing messages in online forums, (e.g. Meetup) communication channels, (e.g. LinkedIn) and email lists (e.g. to student athletes).

B. Interviews

We conducted semi-structured interviews with 32 participants to identify their concerns, common misconceptions, and perceptions about the costs and benefits of collecting and sharing information via wearable devices. After giving informed consent, participants completed a brief demographic survey and face-to-face interviews, via phone or video chat (via Google Hang Outs or Skype). Each interview lasted around 40 minutes. The entire study was IRB approved, and participants received a US $25 gift card as compensation.

C. Interview Script

The full script of the interview included a range of questions, and the following five are focused on this paper:

1) What are your privacy concerns, if any?
2) Would you share your device and/or the data? Why? With who?
3) Do you sync/view data? How?
4) How often do you access it?
5) Do you access it for healthcare purposes?

D. Data Preparation and Analysis

Interviews were audio-recorded and transcribed verbatim. For the content analysis, one member of the research team first read and analyzed all transcripts, generating codes for the contents; then, each segment was assigned to a category. Then each segment was coded in specific categories (e.g., perceptions were identified as self, social and actions were defined as none, variable, extreme). In the third phase we extracted and summarized the results to answer the the research questions mentioned in Section I-A. Our results emerged from a bottom-up approach using a focused analysis, with a method inspired in grounded theory [59]. This method allowed us to capture the rationale of WWD users, showing the benefits and drawbacks they share and at what step during their interaction with their WWD due concerns occur. This approach also allowed us to identify similarities, and differences while detecting emerging concepts, which helped us derive design guidelines.

IV. Results

Of the 32 participants we interviewed we excluded data from four participants because they did not own wearable devices and from eight participants who reported they primarily used Head-Mounted Devices (HMDs) for general purposes. These exclusions resulted in a final sample size of 20 (62% of 32) interview participants as shown in Table I.

A. WWW Device Ownership

All participants used WWDs. Participants reported using nine different fitness trackers, including: FitBit (10), Nike + Fuel band (2), Pebble (2), Basis (1), JawBone Up (1), Gear (1), Body Media (1), Garmin forerunner (1) and Misfit Shine

TABLE I
PARTICIPANT DEMOGRAPHICS AND TECHNOLOGY EXPERIENCE

	N = 20
Age (SD)	36 (11)
Gender	
Male	6 (30%)
Female	14 (70%)
Education	
High School	1 (5%)
Bachelors	9 (45%)
Masters	5 (24%)
PhD/Post-doctoral	5 (24%)
Ethnicity	
White	14 (70%)
African American	2 (10%)
Other	4 (20%)
Technology Experience	
Intermediate	4 (20%)
Advanced	7(35%)
Professional	9 (45%)

(1). For participants with more than one device, we instructed them to provide answers about the device they wore most frequently.

B. Level of Concern for Privacy

Participants' perceptions and actions vary depending on their expertise and level of privacy concern. Based on their comments about privacy concerns around WWDs, we categorized participants as: unconcerned, somewhat concerned and highly concerned (Table II). These three groups had different understandings not only around privacy but also about data collection. While some interviewees had some prior knowledge about privacy, in practice they seemed to be unconcerned about the potential threats. For example, some participants who were unconcerned (n=12) thought none of the data that was collected from their WWD was significant enough to cause any potential threats their privacy:

"None of the data that I'm logging I think is significant enough to cause any grief." (P2) "As a technology person, I don't really mind sharing data like this. To me, that doesn't really quantify anything about me nor from my private life." (P6)

Others realized sensitive information was collected, but they would not mind sharing it:

"I have no problem to make this kind of information public [jogging information]." (P28)

All the participants who reported some concern (n=5) were aware that risks were involved or that control was needed:

"This is super interesting because right now I don't have any. But I can see if this information was somehow accessed by let's say a health insurance company or someone else who could use it in order to determine what kind of care I received. That's a little big brotherish." (P23)

TABLE II
LEVEL OF CONCERN FOR PRIVACY AMONG WEARABLE USERS.

Level of Concern	N = 20 (100%)
Unconcerned	12 (60%)
Somewhat Concerned	5 (25%)
Highly Concerned	3 (15%)

Highly concerned participants (n=3) reported being conscious about the potential threats and were aware that their health related data could be used against them:

"I have more privacy concerns about the fact that there will be some vast analytics running on it... maybe there are some aspects which could be derived that somewhere in the future I'll be sick... I'm more worried about the fact that it can be used against me." (P12)

C. Concerns Toward Health Related Data on WWD

Users' concerns in relation to the collection and sharing of their health related data on WWD were mainly related to the unintended use of data. Our results indicate that these concerns arise mainly in the data collection state. Participants also shared concerns about control over their data and data ownership. Table III shows annotated concerns by type as described next.

1) Unintended Use: Some users' privacy concerns centered around the unintended use of the information captured by their WWD. For example, P23 was concerned that an insurance company might be able to access their health data and use this data to determine what type of care they would receive (See Table III). We categorized this concern as "unintended use" because the users' initial reason for purchasing the device was to improve their quality of life and use data that was being collected by the device to be aware of the changes they were making. The inadvertent use of this data for predictive modeling to determine health care was not how the user intended their data to be used.

P16 and P9 noted concerns more immediate, centering on the potential unintentional revelation of data to colleagues. These two participants shared similar thoughts on the unintended use of their data if it is revealed to co-workers. P16's concerns were related to data being collected on their health status to indicate whether they had an illness, but needed to be at work. P9 worried that if she called in sick, but her coworkers or boss might see her hiking which could present a potential privacy concern in the future.

2) Control: Some participants' concerns were related to the idea of not having control or owning the data on their WWD. For example, P12 mentioned that data collected about them from their WWD and being uploaded somewhere, but they do not have control over how this is done, nor do they have access to this data. P3 mentioned they would prefer to not share or sync their data online and the data should only be stored directly on their cell phone.

TABLE III
USER CONCERN TOWARD SHARING OF HEALTH RELATED DATA ON WWD

	Type of Privacy Concern
Unintended Use	*"But, if after the fact someone were to gain this access to this data and use it to prove why I shouldnt be eligible for something or exclude from a health program that would be concerning." (P23)*
	"If it was collecting,information about like "oh, he's feeling sick today" and maybe if there's a conflict in terms of well he's sick, but he's supposed to be at work." (P16)
	"I have more privacy concerns about the fact that there will be some of the vast analytics running on it,maybe there are some aspects which could be derived that somewhere in the future Ill be sick, and then some insurance company may say we already have this core for 60 years old or something. So Im more worried about the fact that it can be used against me without my knowledge, without my confidence." (P12)
	"Oh, you know if I were connected to coworkers or my boss and I called in sick one day and she sees that I am completing these hikes...that could be an issue. Like I said it's a hypothetical, potential privacy concern right now." (P9)
	"If someone wants to know my weight I guess. Depends on how they use that information." (P1)
Control	*"That I am forgetting it, and it keeps measuring unobtrusively, without me thinking about it. And its uploading data somewhere. Okay, so the bad thing, maybe also, I don't own the data yet. They say they're still working on the data sharing, so I cannot pull up any data, I can just see them as graphs on the website. So that's a bad thing still." (P12)*
	"I dont know how practical it is but it seems like a nice thing would be it doesnt necessarily need to be shared with anybody or synced online or anything. It just needs to talk directly to...lets say your cell phone and keep it stored on your cell phone but it doesn't need to sync those settings or with anything else." (P3)

D. Benefits

In addition to concerns about privacy, many participants also felt positive about the data sharing and collection capacity of their WWD. For example, one participant (P30) noted that is was a good thing to share data with others because it can make one feel good about themselves. In general, the study participants tended to believe that analysis of data collected via WWDs could eventually result in a better understanding of human behavior and improvement of the devices. For example, P23 noted that understanding the type of data collected could be used to provide more insights to a larger population, which was a positive aspect of using WWDs.

P26 mentioned having a WWD device is very interesting because it provides insights about their health and well-being and gives them an alternative mechanism to supplement their healthcare. P12 noted that they are very satisfied with their WWD because it allows them to see patterns and improvements in their health. Overall the device has influenced them to adopt a healthier lifestyle:

"The basis watch, I very much like it, I would say I'm even more addicted to see the patterns, to see also the improvements in me changing some behaviors, and I'll tell you in a moment what have I changed. And then, seeing the effect of this." (P12)

P23 and P30 also noted that sharing data with their doctors and family members could result in positive outcomes. For example, P23 indicated that sharing their data with their doctor could be a really good idea and this would hold them accountable for staying healthy. P2 mentioned sharing their data with friends who have different devices to compare the results is very beneficial and they have no problem sharing this information.

"I've shared my data with the study over there as well as Fitbit also has a friends feature to make you more accountable to your peer group. So, I have several Fitbit friends in there and if they wanted to they could see it." (P2)

The main benefits mentioned about sharing information captured from wearables include: encouragement, cheering, comparison (of performance for instance) and analysis of their behavior and confirmation within their group:

"Yeah, I had my husband, my boss, we're all on this together and we always with my coworkers. We are part of each other's little social circle and we'll chat back and forth. look how many calories I burn, come with me, join me!" (P23)

"It actually does make a difference when you know who your friends are on it and you are all motivating each other to not eat above a certain level or not eat below a certain level. So it helps sometimes." (P6)

"Yeah, it's funny I actually use in it presentations at work. Because what I do is often talk about motivation and I'll use as a real world example to help people understand how I am personally motivated by data in my own life." (P23)

E. Misconceptions

Among participants, there seems to be a misunderstanding about the definition of privacy, as often it is confused with security. Some participants immediately associate privacy with security. For others, the data or profile was not *interesting* (or important) enough to warrant concern:
"Daily activity is not something private... I mean, if people are around you, they... figure out whether you're lazy or not." (P6)

For one interviewee, the users' knowledge and experience was enough to ameliorate any concerns about sharing data:

"Most people that are technology savvy wouldn't mind

sharing data." (P6)

Finally, the *"lack of input device"* led some users to feel that they should not have to be concerned about the privacy of the data collected by their WWD:

"Yeah, there weren't any passwords or anything like that I put into the device. And also, that specific device doesn't have a keyboard, so you can't type in any sensitive information." (P20)

F. Solutions

During the interviews some participants brainstormed potential solutions to issues they detected with wearable privacy. These unprompted responses were grouped in three main categories: authentication, policies, and network of friends, being defined as follows:

- **Authentication:** For *authentication*, one user suggested biometrics:
  "You could only have your biometrics be private to you, they would be shared with someone other online account or anything." (P3)
- **Policies:** For policies, one participant realized that all permissions, terms and conditions must be clear for users: *"I was not aware of this before, but apparently, now, if you go download an app, these things need to be clear in there." (P6)*
- **Network of Friends:** Concerning the network of friends, participants mentioned limiting sharing to prevent issues: *"I haven't really thought about my privacy concerns, but I do try to limit them by just limiting how much information I share and how many friends I have." (P9)*

G. Privacy Settings

Users like to be in control of their privacy *"I like to control it, I wouldn't want a lot of strange people see it so I would only share it with my friends." (P14)*, but adjusting these settings can be confusing for users. In some instances users are not even aware of their privacy settings *"I may have had to change it."; "I don't think so, no I don't think I really ever thought about it that deeply. I don't really remember actually... let me just double check. That's crazy, I am looking at the app right now, and I can't tell" (P24).*

Among the participants who did not change their privacy settings, they either have no concerns *"personally, I wasn't too concerned about it." (P20)* or assume all data is set as private by default *"they came private from the get-go" (P6).*

Among the participants who changed their privacy settings, they want control over their their sharing *"Yes, I have changed it. I've gone into settings to say what kind of information do you want to report. I've actually done that more often" (P9)*, in an easy way, *"Yeah, it was very easy. You just go in there and click I think it's like go through in advanced settings or something and hit "privacy or something like that." (P21)* and having it all private by default, *"it's default is privacy and then if you want to share it then you make changes to that" (P2).*

H. Tradeoffs

For the participants who are aware of risks involved with collecting and sharing data from WWD's, some mentioned being willing to sacrifice their confidentiality for services offered by some devices. P8 noted distinct trade-offs for using WWDs and understands that in some instances you have to make a choice between two unpleasant choices. Clearly this user understands the risks associated with the sharing and collection of their personal data, but believes there are no alternatives and is willing to take the risk of compromising their privacy to use services offered by their devices.

"there's a price I pay for having it convenient and nice but I've kind of accepted that's, you know, pick your poison, and that's just something I run the risk of to use these applications...I don't trust them but I go ahead and use their products anyways." (P12)

I. Emerging Concerns

Interestingly, in spite of most (60%) participants mentioning at a first moment that no privacy concerns were involved, in a second thought, they started to think about privacy implications after we posed questions from their responses. For example:

"I don't care much about if people are looking at my performance as a runner.....I'm just running for fun, so I feel like... I'm less concerned about my running tracks than about features about myself, for instance. I have no problem to make this kind of information public, but of course, nobody's interested in these things as well." (P28)

We followed this question by asking if the participant considered this information not as confidential or sensitive and they said:

"No, I yeah, I of course, it's sensitive because you can figure out where I've been, in a specific, in which city I'm living." (P28)

One participant mentioned not having any privacy concerns, but when asked if they accepted the privacy settings by default, they indicated that changes were made:

"Well, I may have had to change it. I changed it so the privacy would be just the people that I said." (P4)

J. Key Findings

From this study we note four main findings concerning users' perceptions and actions toward wearable privacy:

- There is variety in concern among users. Most participants (60%) reported being unconcerned about their health-related data collected from their WWDs. They are unsure whether sensitive data are collected, shared, and it is hard for them to perceive *who* can access *what* and *when*. Participants who did show concern (40%) were

aware of risks associated with the collection of their related data and understood how this data could be used against them;
- Users have a *partial understanding* about privacy; its implications, threats, risks and solutions are unclear, poorly understood, and oftentimes underestimated and confusing;
- Users' concerns in relation to the collection and sharing of their health related data on WWD were mainly related to *Unintended Use* and *Control* over data collected from WWDs. Conversely, some participants also felt positive about the data collection and sharing capacity on their WWD;
- The *"lack of input device"* led some users to feel that they should not be concerned about the privacy of the data collected by their WWD.

V. Design Implications

For stakeholders, as wearable developers and designers, a clear understanding of how users perceive privacy, may help them to propose solutions that support involving actions, preferably matching interest of both *users* and *vendors.* The primary solutions consist of defining control mechanisms to enable users to control their privacy settings whenever necessary (i.e. sharing of personal, sensitive, or confidential data with unknown or untrusted parties). These mechanisms need to be made clear to users because as our results show, they are either unaware or just partially aware of practical solutions (similar findings have been noted for account hijacking [21]). As our results show, privacy preferences and perceptions vary among users which indicate a need for granular privacy control over wearable data [54] and personalized solutions.

From the analysis of the data collected with user studies, three key requirements for privacy-enhanced wearable systems emerge:

Transparency. Users must be aware of what type of data is collected, when, how this data is collected, who owns the data, whether the data is shared, how it is shared, when it is shared, and with who it is shared. Transparency can prevent misuse of health-related data, for instance, if a health insurance provider exploits sensitive information collected by a users' activity tracker to modify the health care services provided or to increase insurance premiums based on the user physical activities. Transparency may also help in preventing criminal abuse, e.g. if a thief exploits user data (i.e. location data produced from a fitness tracker) for malicious aims (such as: stalking, robbery, sexual assault).

Reliability. To ensure trust on wearables, the data collection, transmission and sharing must be as precise and reliable as possible. Critical consequences can result from mishandling of personal data, especially in health care.

Granular Control. Users want control over what is shared, *how, when,* and *with who* as demonstrated in [54]. Users' should be able to fill out forms that can be modified according to the users' preferences before data collection starts. If the user can immediately interrupt any data collection or sharing before it starts, this gives them more control over their data. As mentioned in [24] with reference to contextual integrity, there should be adequate protection for privacy to standards of particular contexts, demanding that data collection and distribution be appropriate to that context.

In our analyses, the users' concerns were identified by two aspects. To provide support for each corresponding action, we indicate three design implications to be implemented in wearable applications:

- **None (users without concerns and/or public data):** the lack of concern occurs either when users have no sharing options, and all the data are kept private, or when no sensitive information is handled, enabling users to have it publicly available without any implications. In both cases the data are by default not shared or fully shared (public). Despite the lack of implications, it is recommendable to make users aware of the solution adopted, providing them with the respective feedback on some instructive guidance contents to make information clear and understandable to user.
- **Moderated (users with some privacy concerns):** the control mechanisms needed to ensure that users select the data they want to be shared, with who they want to share it, and how. Fine-grained solutions are preferred (allowing a flexible and detailed control level).
- **Extreme:** users with high levels of concerns do not want anything to be shared, so the systems need to either have everything private by default (preferred by users) or enable them to set everything as private. In both cases, the status of the system needs to be presented in a clear and reliable format to users seeking to ensure transparency.

While these implications may seem pretty obvious in principle, the users' claims gathered during this study show that WWD applications that collect health-related data are not yet able to properly support them, urging for further improvements.

VI. Discussion

Our results show that users have a basic understanding of privacy, and also variability in their levels of concern about wearable privacy – ranging from unconcerned to highly concerned. We find that although there is variability in the level of concern across users, the majority of participants (60%) were not very concerned about wearable privacy believing that the data collected by their WWD was not cause for concern. Despite these beliefs, data produced by WWDs collects and stores sensitive information that could eventually become a "skeleton in the closet"; if revealed or used inappropriately it could have a negative impact on users [3]. This result could also indicate that many existing privacy controls are lacking or limited in WWDs.

Participants show concern toward the unintended use of data collected and desire more control over their wearable data as mentioned in section IV-G – when the user indicated they like to control their data, and they do not want people to see

their data. As we mentioned in the related work section, the unintended use of data collected from WWD could disclose users' activity without their awareness or consent [41]. These implications suggest the need for granular privacy control over data collected on WWD. Granular control over privacy and sharing of health information has existed [54], even if that control has been applied by different means (e.g. patient limiting the type of information seen by non-primary physicians). Participants also mentioned that settings on WWDs could sometimes be confusing despite users desiring more control over their own data. Unintended use and control were mentioned in prior work by [60], which gives external validity to the privacy concerns indicated in our study. Although participants showed privacy concern, they also felt positive about data sharing and collection from their wearable device due to the potential benefits involved.

The participants who showed concern identified solutions on how to enhance their privacy, for instance through biometric authentication, clear, transparent and better defined policies when downloading third-party fitness apps, and limiting the sharing of data.

To complement the results of this study in future work, we plan to refine our understanding of the users' sharing preferences, especially with certain devices, applications, and recipients. We also plan to use this information to elicit privacy solutions that address the user need for granular privacy control [54] and personalization over data generated from WWDs.

VII. Limitations

While this research sheds light on understanding wearable privacy from a user-centered perspective, the results need to be carefully understood before any generalization.

First, because the study focused on a sample of 20 users (mostly American), which may not significantly reflect the overall population, special consideration should be taken before generalizing the cultural aspects of privacy perceptions. Further studies are necessary to broaden and refine the research findings to other cultural groups.

Similar to the experiences of other privacy researchers (e.g., [61], [62]), during the interview, we found that participants became increasingly concerned about privacy as they had the time to reflect. In our study, these concerns primarily emerged when we asked participants about changing their privacy settings and their current sharing practices for online services. We tried to avoid biasing and skewing participants about privacy concerns by focusing our questions on concerns that they already had before the start of the interview.

VIII. Conclusion

The analysis of the users comments shows that the privacy concerns towards WWDs can be investigated from several perspectives, with personal, cultural and social aspects impacting crosscutting concerns in the physical and virtual world. New threats, risks, and implications involving wearable privacy emerged with the popularization of wearable devices, however they are still recent and unclear for most users and stakeholders, who tend to underestimate, or ignore potential risks. While many open challenges remain, this work sheds light on how users perceive wearable privacy, demonstrating that (i) user concerns of wearable privacy are variable, (ii) user concerns and benefits are similar and should be investigated more rigorously for the development of privacy enhanced WWDs (iii) users desire granular privacy control on WWDs and (iv) several misconceptions and trade-offs exist in users understanding of wearable privacy. By better understanding users' needs and behaviors, we seek to define solutions that effectively help users to understand and better control their privacy on wearable devices, especially for healthcare-related purposes.

IX. Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant Numbers 1619950 and 1314342. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] M. Weiser, "The computer for the 21st century," *Scientific american*, vol. 265, no. 3, pp. 94–104, 1991.

[2] V. Genaro Motti and K. Caine, "An overview of wearable applications for healthcare: requirements and challenges," in *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*. ACM, 2015, pp. 635–641.

[3] C. Hallam and G. Zanella, "Wearable device data and privacy: A study of perception and behavior," *World*, vol. 7, no. 1, 2016.

[4] L. Piwek, D. Ellis, S. Andrews, and A. Joinson, "The rise of consumer health wearables: promises and barriers," *PLos Med*, vol. 13, p. e1001953, Feb. 2016.

[5] "Wearable device unit sales worldwide by region in 2015 and 2020," https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/.

[6] F. of Privacy Forum, https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf, 2016.

[7] M. Swan, "Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking," *International journal of environmental research and public health*, vol. 6, no. 2, pp. 492–525, 2009.

[8] ——, "Health 2050: The realization of personalized medicine through crowdsourcing, the quantified self, and the participatory biocitizen," *Journal of personalized medicine*, vol. 2, pp. 93–118, 2012.

[9] "Health at hand: A systematic review of smart watch uses for health and wellness."

[10] R. S. Istepanian, E. Jovanov, and Y. Zhang, "Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity," *IEEE Transactions on information technology in biomedicine*, vol. 8, no. 4, pp. 405–414, 2004.

[11] D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner, "Privacy and security in mobile health: A research agenda," *Computer*, vol. 49, no. 6, pp. 22–30, 2016.

[12] S. Park and S. Jayaraman, "Enhancing the quality of life through wearable technology," *IEEE Engineering in medicine and biology magazine*, vol. 22, no. 3, pp. 41–48, 2003.

[13] B. Schwartz and A. Baca, "Wearables and apps for health promotion."

[14] N. Eagle and A. Pentland, "Wearables in the workplace: Sensing interactions at the office." in *ISWC*, 2003, pp. 256–257.

[15] S. Ajami and F. Teimouri, "Features and application of wearable biosensors in medical care," *Journal of research in medical sciences: the official journal of Isfahan University of Medical Sciences*, vol. 20, no. 12, p. 1208, 2015.

[16] V. G. Motti and K. Caine, "Users' privacy concerns about wearables," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 231–244.

[17] K. Caine, "Privacy is healthy," *IEEE Pervasive Computing*, vol. 15, no. 4, pp. 14–19, 2016.

[18] U. F. T. Commission *et al.*, "Complying with the ftc's health breach notification rule, 2010."

[19] S. R. Peppet, "Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent," *Tex. L. Rev.*, vol. 93, p. 85, 2014.

[20] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, no. 4, pp. 101–106, 2005.

[21] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, "My religious aunt asked why i was trying to sell her viagra: experiences with account hijacking," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2657–2666.

[22] R. Hoyle, R. Templeman, S. Armes, D. Anthony, D. Crandall, and A. Kapadia, "Privacy behaviors of lifeloggers using wearable cameras," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2014, pp. 571–582.

[23] O. for Econ. Co-operation & Dev., "Oecd guidelines on the protection of privacy and transborder flows of personal data," 1980.

[24] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[25] F. M. Schaub, "Dynamic privacy adaptation in ubiquitous computing," Ph.D. dissertation, Universität Ulm, 2014.

[26] J. DeCew, "Privacy," in *The Stanford Encyclopedia of Philosophy*, spring 2015 ed., E. N. Zalta, Ed. Metaphysics Research Lab, Stanford University, 2015.

[27] M. Langheinrich, "Privacy by design- principles of privacy-aware ubiquitous systems," in *International conference on Ubiquitous Computing*. Springer, 2001, pp. 273–291.

[28] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith, "Privacy considerations for internet protocols," Tech. Rep., 2013.

[29] D. H. Nguyen and E. D. Mynatt, "Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems," 2002.

[30] K. E. Caine, "Exploring everyday privacy behaviors and misclosures," 2009.

[31] B. Ur and Y. Wang, "A cross-cultural framework for protecting user privacy in online social media," in *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 2013, pp. 755–762.

[32] BusinessWire. (2015) Worldwide wearables market forecast to grow 173.3% in 2015 with 72.1 million units to be shipped, according to idc. [Online]. Available: http://www.businesswire.com/news/home/20150618005154/en/Worldwide-Wearables-Market-Forecast-Grow-173.3-2015

[33] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava, "Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 11–20.

[34] V. G. Motti and K. Caine, "Towards a visual vocabulary for privacy concepts," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2016, pp. 1078–1082.

[35] T. Starner, "The challenges of wearable computing: Part 2," *Ieee Micro*, vol. 21, no. 4, pp. 54–67, 2001.

[36] R. Want, B. N. Schilit, N. I. Adams, R. Gold, K. Petersen, D. Goldberg, J. R. Ellis, and M. Weiser, "An overview of the parctab ubiquitous computing experiment," *IEEE personal communications*, vol. 2, no. 6, pp. 28–43, 1995.

[37] V. G. Motti and K. Caine, "Understanding the wearability of head-mounted devices from a human-centered perspective," in *Proceedings of the 2014 ACM International Symposium on Wearable Computers*. ACM, 2014, pp. 83–86.

[38] S. Spann, "Wearable fitness devices: Personal health data privacy in washington state," *Seattle UL Rev.*, vol. 39, p. 1411, 2015.

[39] T. Starner, "The challenges of wearable computing: Part 1," *Ieee Micro*, vol. 21, no. 4, pp. 44–52, 2001.

[40] A. Wieneke, C. Lehrer, R. Zeder, and R. Jung, "Privacy-related decision-making in the context of wearable use," in *Proceeding of the 20th Pacific Asia Conference on Information Systems (PACIS 2016)*, 2016.

[41] L. Lee, J. Lee, S. Egelman, and D. Wagner, "Information disclosure concerns in the age of wearable computing," Working paper University of California, Berkeley. Retrieved from https://blues. cs. berkeley. edu/wp-content/uploads/2016/02/camera-ready. pdf, Tech. Rep., 2016.

[42] N. Gorm and I. Shklovski, "Sharing steps in the workplace: Changing privacy concerns over time," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 4315–4319.

[43] ——, "Steps, choices and moral accounting: Observations from a step-counting campaign in the workplace," in *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 2016, pp. 148–159.

[44] N. Liberman, Y. Trope, S. M. McCrea, and S. J. Sherman, "The effect of level of construal on the temporal distance of activity enactment," *Journal of Experimental Social Psychology*, vol. 43, no. 1, pp. 143–149, 2007.

[45] N. Liberman, M. D. Sagristano, and Y. Trope, "The effect of temporal distance on level of mental construal," *Journal of experimental social psychology*, vol. 38, no. 6, pp. 523–534, 2002.

[46] Y. Trope and N. Liberman, "Construal-level theory of psychological distance." *Psychological review*, vol. 117, no. 2, p. 440, 2010.

[47] D. Kerr, K. Butler-Henderson, and T. Sahama, "Security, privacy, and ownership issues with the use of wearable health technologies," *Managing Security Issues and the Hidden Dangers of Wearable Technologies*, p. 161, 2016.

[48] M. De Mooy and S. Yuen, "Towards privacy-aware research and development in wearable health," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[49] R. Whittaker, "Issues in mhealth: findings from key informant interviews," *Journal of medical Internet research*, vol. 14, no. 5, p. e129, 2012.

[50] L. Hanna and S. Hailes, "Privacy and wireless sensor networks. university college, london," 2010.

[51] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93–101, 2012.

[52] G. Addonizio, "The privacy risks surrounding consumer health and fitness apps, associated wearable devices, and hippa's limitations," 2016.

[53] C. M. L. Njie, "Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications," *Research Performed For: Privacy Rights Clearinghouse*, 2013.

[54] K. Caine and R. Hanania, "Patients want granular privacy control over health information in electronic medical records," *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 7–15, 2013.

[55] B. Ur and Y. Wang, "A cross-cultural framework for protecting user privacy in online social media," in *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 2013, pp. 755–762.

[56] P. Dourish, "Culture and control in a media space," in *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW93*. Springer, 1993, pp. 125–137.

[57] M. McCartney, "How do we know whether medical apps work?" *BMJ*, vol. 346, p. f1811, 2013.

[58] M. Chan, D. Estève, J.-Y. Fourniols, C. Escriba, and E. Campo, "Smart wearable systems: Current status and future challenges," *Artificial intelligence in medicine*, vol. 56, no. 3, pp. 137–156, 2012.

[59] B. G. Glaser, A. L. Strauss, and E. Strutzel, "The discovery of grounded theory; strategies for qualitative research." *Nursing research*, vol. 17, no. 4, p. 364, 1968.

[60] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model," *Information systems research*, vol. 15, no. 4, pp. 336–355, 2004.

[61] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011, p. 15.

[62] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2347–2356.