Users' Privacy Concerns About Wearables:

impact of form factor, sensors and type of data collected

Vivian Genaro Motti and Kelly Caine

{vgenaro;caine@clemson.edu}
School of Computing
Clemson University
McAdams Hall – Clemson, S.C., USA

Abstract. Wearables have become popular in several application domains, including healthcare, entertainment and security. Their pervasiveness, small size and autonomy, enlarges the potential of these devices to be employed in different activities and scenarios. Wearable devices collect data ubiquitously and continuously, about the individual user and also her surroundings, which can pose many privacy challenges that neither users nor stakeholders are ready to deal with. Before designing effective solutions for developing privacy-enhanced wearables, we need first to identify and understand *what* are the potential privacy concerns that users have and *how* they are perceived. To contribute to that purpose, in this paper we present findings from a qualitative content analysis of online comments regarding privacy concerns of wearable device users. We also discuss how form factors, sensors employed, and the type of data collected impact the users' perception of privacy. Our results show that users have different levels and types of privacy concerns depending on the type of wearable they use. By better understanding the users' perspectives about wearable privacy, we aim at helping designers and researchers to develop effective solutions to create privacy-enhanced wearables.

Keywords. Privacy; Wearable Computing; Wearable Devices; Form Factors; Privacy Concerns; User studies; Human Factors

1 Introduction

The significant advances in technology in the past decades, characterized by the miniaturization of components, more efficient power sources, alternative network solutions, and novel sensors, boosted the development of wearable devices. As a consequence, a variety of form factors have been created, enabling wearable devices to be applied for multiple different purposes. Despite the large potential and known benefits of wearable devices, their spread usage entails several privacy concerns. Wearables, by continuously collecting, transmitting, and storing data, handle information that are often considered as personal, private, sensitive or confidential. This information can be publicly available or posted in social media, where it is shared with a network of friends of the individual user or even with unknown or untrusted parties. While the data collection and sharing brings many benefits for end users, it also brings novel privacy challenges for stakeholders involved in the creation of wearable devices and applications. Wearables enable the surveillance and sousveillance of individuals and their behaviors and surroundings as well, which can lead to severe privacy implications, threats and risks. These issues affect not only the individual user but also the society and organizations involved, for instance when the data collected are misused. Due to the novelty of the wearable field such implications are not yet fully understood.

The continuous use of wearables involves a variety of privacy concerns, however because the usage of these devices is relatively recent, users are not aware of the potential privacy implications of continuous data collection, storage and online sharing. To better understand how users actually perceive wearable privacy, and to identify what are their main concerns nowadays, we collected commentaries from users (end users and prospective users) from online sources (such as IT forums, websites, discussion lists and social medias) about several wearable devices (either commercially available or to be soon launched in the market) including head-mounted and wrist-mounted devices. With the analysis of the users' comments extracted from a set of online sources, we identified different concerns about wearable privacy, and we analyzed how they are related to specific form factors, sensors employed, and data collected.

The main contributions of this paper consist in identifying: i) what are the users' concerns for wearable privacy; ii) how form factors, data collected and sensors employed impact these privacy concerns (regarding their levels and nature); and iii) what concerns are specific to wearable devices, sensors and applications.

This paper is organized as follows: Section 2 motivates and contextualizes this research by presenting related works and the scope in which this research is inserted; Section 3 describes the method of the research; Section 4 presents the results obtained; Section 5 discusses them and Section 6 concludes.

2 Related Work

Privacy concerns are not exclusive from the technological domain, being discussed since 1890 [War90]. Despite being in discussion for a long time, privacy issues related to mobile technologies are relatively new, complex to study and still poorly understood [Man09]. Moreover, mobile and wearable devices continuously collect data, spreading the use of sensors, such as: cameras, GPS, and accelerometers, whose small size and invisibility adds novel challenges to ensure users' privacy.

Most of the previous works on user privacy has focused on mobile devices and their applications [Shk14], social networks [Ur13],[Gur13], web applications [Rei14], or other security concerns, as account hijacking [Sha14]. Little is known about wearable privacy [Tro08],[Hoy14] from a human-centered perspective. Existing solutions frame the privacy problems too narrowly and satisfactory general solutions remain elusive [Tro08], besides having a fragmented landscape [Gur13]. The nature of privacy concerns remains an open question, requiring a better understanding of privacy behaviors in technology [Cai09].

The following sections summarize related research findings, presenting and discussing privacy concerns and human perspectives in ubiquitous, mobile and wearable computing.

2.1 Privacy in Ubiquitous Computing

Characterized by the integration of computational solutions into the physical environment, ubiquitous computing enables inanimate objects to acquire intelligence, by sensing, processing and communicating data [Sch14]. These data concern the individual user and also her surroundings, and can imply in privacy issues. Despite the existence and importance of these issues, users have a limited understanding about those. By centering potential solutions for privacy-enhanced technologies on the users' perspectives and concerns, stakeholders can aid users to better understand and control their privacy in these systems [Kon13].

2.2 Privacy in Mobile Devices

Significant improvements in mobile computing in the past decades popularized the use of mobile devices, with smart phones and mobile apps playing nowadays a fundamental and intimate role in users' everyday life. Despite the continuous data collection and transmission with these devices and apps, previous research shows that users are not aware about *what* data are collected and *how* they are used [Shk14]. For [Man09], despite the importance of mobile privacy concerns, they still remain poorly understood.

2.3 Privacy in Wearable Devices

Similarly to ubiquitous and mobile computing, in wearable computing, privacy is one of the main challenges yet to be solved [Sta01a]. Not only because wearable computers are able to sense, process and store intimate information about the users, but also because wearables are able to do it continuously and discreetly [Sta01b]. Besides this, currently, users cannot fully understand the potential risks, threats and implications involved with data collection and tend to underestimate those. However the data collected often enable to infer private information, especially when combined with other data, which can result in significant risks to the users' privacy [Rai11].

As previous research identified, privacy became a key concern to users [Sta01b], being for instance among the top five concerns that users consider important in the wearability of HMD (head-mounted devices) [Mot14]. Despite its relevancy, wearable privacy is still an emergent topic and many questions remain open.

Previous works related to wearable privacy have focused on its different aspects, including: i) users' behaviors with wearable cameras, to identify the factors that impact how sensitive a photo is [Hoy14] and the privacy concerns in pictures illustrating eating behaviors of users [Edi13]; ii) requirements for remote communication in fashion garments [Jac14]; iii) perceptions of anklet wearers, to identify location-based privacy concerns [Tro08]; iv) privacy for augmented reality systems [Roe14]; and v) surveillance concerns of Google Glass users [Mcn14]. Although these works aid to understand how users perceive wearable privacy, they focus on specific wearable devices or applications.

2.4 Users' Perspectives on Privacy

Privacy behaviors across multiple technologies were identified and analyzed in [Cai09], aiding to understand the users' perspectives and concerns and to propose and devise novel solutions to ensure users' privacy. Despite extensive user studies, this work targets a general understanding of privacy concerns, regardless of the technology employed. User studies were also conducted by [Ber05], to better understand users' privacy concerns. This work, although focused on e-commerce applications, suggests a significant gap between reported concerns and actual users' behaviors, reinforcing that users often sacrifice their privacy in exchange of benefits. For [Ngu02], considering current users' needs and their cognitive models is key to ensure privacy control. The users' understanding about privacy was also analyzed in [Rei14], but mainly regarding their interaction with web sites.

Despite previous works focusing on ubiquitous, mobile and wearable computing, it is still not clear what are the users' concerns about wearable privacy and how these are related to specific devices, sensors and applications. However, without understanding what the privacy problems are, privacy cannot be addressed in a meaningful way [Sol08].

3 Methods

Because we were interested in assessing the privacy perceptions of a broad range of people who already had interest or experience in using wearable devices, and we wanted to gather a geographically and demographically diverse sample, we chose to conduct an observational study of online comments posted by wearable users. To identify concerns, we extracted comments from a series of online sources (described below). First, we selected a set of devices and data sources, then we identified, selected and analyzed the users' concerns about privacy in wearable devices. Further details about the methodology of this work are described in the following sections.

3.1 IRB Approval

To ensure the protection of human subjects, before data collection started, the Clemson University Institutional Review Board (IRB) approved this study as exempt.

3.2 Data Selection, Extraction and Analysis

Due to the fact the head-mounted and wrist-mounted devices are the most popular form factors available and in use today, we considered both form factors for data collection. To minimize bias in the data collected we selected a set of 59 different online sources, including popular websites for discussion and reviews of technology and e-commerce pages for shopping, reviewing and recommending devices. The data collection process resulted in more than 2,000 commentaries extracted for analysis. This process was conducted in April and May 2014 and consisted in visiting the online sources previously selected, searching for the users' comments regarding specific devices, and manually extracting the contents of interest to compose a report.

For the analysis, we filtered and selected the commentaries related to privacy concerns. For that a member of our research team read and analyzed each comment, to identify and annotate those related to privacy. Then, the annotated comments were analyzed again to identify the nature of the privacy concern regarding its motivations and rationale behind it. For example, a user who fears the consequences of his/her location being posted online in a live feed through social media apps concerns the *Implications of Location Disclosure*). In order to identify the relationships between the privacy concerns and respective data collected and sensors, we analyzed the nature of the concerns identified and assessed whether they were specific to a given form factor and/or application or generic to mobile devices. The results of this analysis are graphically presented in a Venn diagram (Figure 1).

3.3 Devices, Online Data Sources and Figures

The users' commentaries collected were generated at latest in May 2014. The date when a commentary was posted was not always available in the web sources selected, however users start commenting about a new device usually when a vendor announce it, launch it for sale or when a new release is made available. The comments collected were related to six wrist-mounted devices with different purposes, including:

- 27 privacy comments about six armbands and smart watches: Sony SWR10 (Core) Smartwear and Thalmic Labs Myo, Basis, Qualcomm Toq, LG Lifeband Touch, Razer Nabu.

The users' commentaries about the 32 head-mounted devices analyzed, included:

- 11 privacy comments about 19 earpieces, headbands and headphones: Looxcie, LG Lifeband Earphones, Intel Smart Earbuds, Microsoft Septimu, Avegant glyph, the Immersion headset, The Vigo, iRiver On, The Voyager Legend, NeuronOn, Recon's Snow 2, The Cynaps Enhance, iWinks Aurora Dreamband, Life Beam's Sports Headband, Emotiv Insight, Axio EEG Headband, InteraXon Muse, Muzik, Neurowear Zen tune Headphones;
- 34 privacy comments about 13 glasses: EmoPulse Nano Glass, Epson Moverio BT-200, Google Glass, Google Smart Contact Lenses, ICIS, K-Glass, Laster See Tru,

Meta Pro, Oculus Rift, Olympus MEG4.0, Second Sight's Argus II, Sony HMz-T1, The Atheer One, Vuzix Smart Sun Glasses.

The 59 online sources used for data collection included 15 forums, 34 technical websites, 6 e-commerce websites, and 4 social medias, e.g.: Amazon, Ars Technica, BestBuy, CNET, ComputerWorld, DigitalTrends, ExpertReviews, Engadget, eWeek, Geek, GizMag, GizModo, Overstock, PCAdvisor, PCMag, PCPro, PCWorld, PhoneArena, Popular Science, Mashable, MIT Technology Review, Reddit, Slate, TechCrunch, TechRadar, TheInquirer, TheNextWeb, TheVerge, T3, TrustedReviews, Wearable Computing Review, Wearable Technologies, Wired, ZDNet. With a diversity of sources, we aimed at more representativeness in the data collected and minimizing the potential bias of commentaries that were not posted by actual users. The main differences among the comments consisted in: more extensive, detailed and formal comments produced by reviewers (posted in IT forums), and shorter, more informal and objective comments produced by end users and posted in e-commerce websites. By gathering comments from heterogeneous sources, we ensure a diversity of user profiles, and still focus on the study goals, covering a set of specific wearable devices and privacy concerns of users for different wearable applications.

The analysis of online reviews has some drawbacks, for instance, little is known about the profile of the user who posted a comment and we cannot ensure whether the comment was in fact generated by an individual user or by a bot, a spammer or even a competitor company, which can introduce bias in the study. In our analysis, to minimize this risk, we selected heterogeneous online sources (59 websites with high popularity) and an extensive list of comments (n>2,000). Despite these drawbacks, as previous research indicate [Hed13], [Iac13], [Fu13], [Kha14], the analysis of online reviews has several benefits as well, for instance: i) users are placed in a *wild* study, i.e. not constrained by laboratory settings, ii) the commentaries are self-reports of the users' opinions, without a standard format or pre-defined set of questions, and iii) a large sample of reviews can be analyzed covering heterogeneous user profiles.

4 Identifying user privacy concerns for wearable technologies

The analysis of the online comments, revealed 13 users' concerns about wearable privacy. These concerns are closely related to the type of data each device collects, stores, processes and shares. Embedded sensors, such as cameras and microphones, capture data about the individual user or people nearby, often without their awareness or consent. These data are oftentimes personal, confidential, and sensitive, which poses privacy challenges, for instance regarding surveillance. Other sensors, such as heart rate monitors, glucometers and activity trackers, are often considered by users as involving fewer privacy concerns.

By analyzing the users' commentaries, 13 privacy concerns emerged, six for wrist-mounted devices and seven for head-mounted devices. These concerns are presented in the following sections, ordered by form factor and the activity they are related to, respectively: data collection, data processing and data sharing (according to the three first groups of activities defined in the Solove's privacy taxonomy [Sol08]).

4.1 Privacy Concerns for Wrist-mounted Devices

Wrist-mounted devices collect data whose nature is less sensitive than head-mounted devices, at least in a first sight. Some HMDs are able to capture audio, image and videos, whose privacy implications tend to be more critical or at least apparent for users. WMDs, on the other hand, often include activity trackers and sense the user location, which is considered by users as less privacy-critical data. Actually, from our analysis, the GPS sensor is pointed as the most critical privacy concern for users of WMDs, as their location is sensed and stored, and sometimes even shared online in real time through live feeds of social media applications. Besides this, the form factors of wrist-mounted devices are similar to conventional accessories worn in a daily basis, such as watches and bracelets, so they fit seamlessly in conventional outfits of users, raising less attention or suspicion from other people. Among the six privacy concerns identified for WMDs and presented below, the two first ones are related to data collection and the other four refer to data sharing.

4.1.1 General Social Implications: Unawareness

An activity tracker that synchronizes data (e.g., location and photos) and relates it to the network of friends of an authenticated user, can also impact the privacy of other people (e.g., individuals belonging to the social network contacts of a given user):

> *'it does not just record your activities, but also activities of* ***people around you****, it can also connect to other devices'*

The people belonging to the social network of a user are not necessarily aware of and compliant with the data collected, stored, published or shared.

4.1.2 Right to Forget

When data are continuously collected, stored, published and shared, they can include information that users do want to recall later, but also events and facts that users were not willing to capture or to be reminded of later on:

> *'it gives a record of everything you've done, day in and day out, possibly even some* ***things you don't want to be reminded of****'*

4.1.3 Implications of Location Disclosure

The users' comments analyzed revealed that users were afraid that their location when tracked could be disclosed to malicious parties and criminals, such as thieves and stalkers. These malicious parties could then misuse the user location, for instance to better plan a crime or other harmful actions:

> *'It [wearable device] just knows when to take pictures of the epic moments, know if you're riding in your car so your friends and* ***stalkers know where you are at all times*** *of the day, know when you go to sleep, riding a car, or climbing a mountain'*

4.1.4 Discrete Display of Confidential Information: non-Disclosure

Wrist-worn devices, such as smart watches, often use a screen to display notifications. These notifications can include sensitive or confidential information, which is also accessible to people located close to the end user. Being able to hide this information from co-located individuals is considered good for some users:

> *'the second screen will act as sort of a privacy screen,* ***keeping folks from reading your texts*** *by glancing at your wrist'*

4.1.5 Lack of Access Control

Users who are aware about data storage in the cloud, fear that organizations or even the government will use their personal data without their awareness or consent, for instance for abusive or malicious purposes:

> *'[wearable devices are] the* ***NSA's new best friend****'*

4.1.6 Users' Fears: Surveillance and Sousveillance

While most wearable device users acknowledge the many benefits of collecting and tracking their personal information, they fear the continuous surveillance and sousveillance and potential implications that this can bring them in the future:

> *'I'm not sure if I should be totally excited or* ***totally frightened*** *about this Sony band logging my every move. I can't help but think it could be good ole big brother in disguise'*

4.2 Privacy Concerns for Head-mounted Devices

Head-mounted devices that focus on augmented and virtual reality and gaming experiences did not raise as many privacy concerns for users (e.g., Oculus Rift and Sony HMz-T1), because less sensitive data are collected, and also because the device does not store or share information, keeping it protected from social media and other online applications with networks of online users. On the other hand, head-worn computers, such as Google Glass, which are equipped with cameras and microphones, are often synchronized with a smart phone, allowing users to connect to social media applications. This results in several privacy concerns, as indicated our analysis of the users' commentaries. The next sections detail specific users' concerns with HMD. Among the seven users' concerns, the four first are related to data collection, one to data processing, and the last two refer to data sharing.

4.2.1 Speech Disclosure

Using speech recognition enables users to have a hands-free interaction, however when users are not alone and need to handle confidential information, audio as a unique input modality poses serious privacy concerns:

> *'though you can't mind people* ***overhearing*** *what you are saying'*

4.2.2 Surveillance, Sousveillance and Criminal Abuse

By capturing data without any consent or awareness, users reported that they were concerned about a potential for criminal abuse:

> *'There are a lot of concerns about privacy invasion, **spying** and situations where people are more concerned with recording an event than actually engaging with it'*

4.2.3 Surreptitious Audio and Video Recording: Unawareness

Although smart phones and mobile computers such as tablet PCs also include cameras and microphones, a HMD allows users to start recording content discreetly:

> *'the video camera that is even easier to use than a smartphone's ... **privacy issues are indeed huge** with that'*
>
> *'Placing a tiny wearable device on someone's eye could potentially be **a lot more discreet**, though some privacy advocates might see that as a downside'*
>
> *'I do believe there is a difference between snapping pictures with something which is obviously a camera, and **recording video surreptitiously**. Social norms already frown on making surreptitious audio recordings (though it isn't illegal, it is done only infrequently and with an air of "secret agency" about it); **video is much more of an intrusion**.'*
>
> *'**the more subtle** and high tech augmented vision gets, **the more dangerous** it gets as well. Basically, we're teetering on a slippery slope here unless we find a solution for the **privacy/harassment concern** that **is growing**'*

4.2.4 Surveillance, Sousveillance and Social Implications: Unawareness

The fact that the device captures information from the users' surrounding extends the privacy issues to the social environment, as people nearby are often unaware or not compliant with the data collection:

> *'There's also another challenge that affects not only those who wear Glass, but everyone else around: **privacy**'*

Users may not feel comfortable to wear a device with a camera on their heads, at least nowadays and especially in environments in which this is not a common practice:

> *'The privacy concerns may very well be overblown, but I think **it'll take a while for people to get comfortable with the idea** of others walking around with camera-equipped devices strapped to their faces'*

4.2.5 Facial Recognition: Identifiability

Users acknowledge the benefits of facial recognition to augment their memory, however, they are also aware that privacy concerns will likely emerge in the near future, as previously pointed out by [Acq11]:

'…totally needs a camera. I want to be able to look at people and it have them tell me their names, limit it to my personal database of contacts if you must, but I'm terrible with names, if it wants to give me an immersive world experience, then ***it needs to be able to see what I see regardless of privacy worries****.'*

'Privacy officials understand that Google won't include facial recognition in Glass for now, but raised concerns about Google's future facial recognition plans'

'…image analysis. ***This of course raises all sorts of new privacy concerns*** *with things like identifying people through facial recognition associated with Facebook pictures… '*

4.2.6 Automatic Synchronization with Social Media: Linkability

Some users do not like the idea of their devices to immediately synchronize with social media applications and share their data without being able to control it:

'Why in the HELL would I ever want to tweet or facebook from a pair of headphones. Isn't there enough horror in the world without these in it?'

'Oh, how nice! Another unsubscribe factor to add to my unsubscribe rule list. ***Tweets from headphones? Unsubscribed!****'*

'Can't wait for the trend when not having a Facebook integration is a big thing…'

4.2.7 Visual Occlusion: non-Disclosure

HMDs that cover the field of view of the user, e.g., Oculus Rift and Sony HMz-T1, allow users to interact privately because their vision is occluded:

'Not as a primary display but ***for those times when I really need some privacy****'*

'watch what they want in the privacy of their own rooms.'

'covered design will enable complete privacy for the viewer.'

'What I want is a head-mounted replacement for my laptop screen. So I don't have to have its size, weight, fragility, power consumption, and ***lack of privacy*** *when I'm traveling'*

'provide you some privacy for your augmented-reality browsing.'

4.3 Privacy Concerns across Form Factors

The analysis of the users' comments collected resulted in 13 privacy concerns for wearable devices, some of them existing regardless of the form factor. By analyzing these concerns we noticed that some concerns (4) are device-specific, others (3) are sensor-specific, few (2) depend on the data collected, or (2) are both device/application- and data-specific:

- **Device-specific privacy concerns:** social implications (in general, devices that collect data that does not belong solely to an individual user, impact social aspects of privacy), criminal abuse (collecting personal data can facilitate criminal abuse), facial recognition can take place if the appropriate algorithms are available in the device, social media synchronization are not necessarily a user wish for wearables;

- **Sensor-specific privacy concerns:** location disclosure is associated with GPS usage, speech disclosure depends on the ability of using audio as input modality (HMD with a microphone), and surreptitious audio and video recording (HMD with cameras) depend on how invisible the sensors are embedded in a device, as data can be captured without it being noticeable;
- **Data-specific privacy concerns:** right to forget (all data that are collected without the consent, awareness or users' will should be able to be deleted after collection), users fear that certain data types when combined could have critical implications;
- **Device/Application and Data-specific privacy concerns:** discrete display and visual occlusion depends on devices with a screen available which should enable users to decide *what*, *when* and even *if* information can be displayed.

Most of the users' concerns, although identified in the analysis of one specific form factor, can also relate to different devices, depending usually on the availability of a specific sensor, feature or application. The location disclosure for instance depends mainly on a GPS to track users location, which is usually embedded in a wrist-mounted device, but can be also found in an anklet or a helmet. Besides the GPS, other sensors or data sources can also be used to track the users' location. Figure 1 illustrates how the privacy concerns identified can be placed regarding their influencing factors.

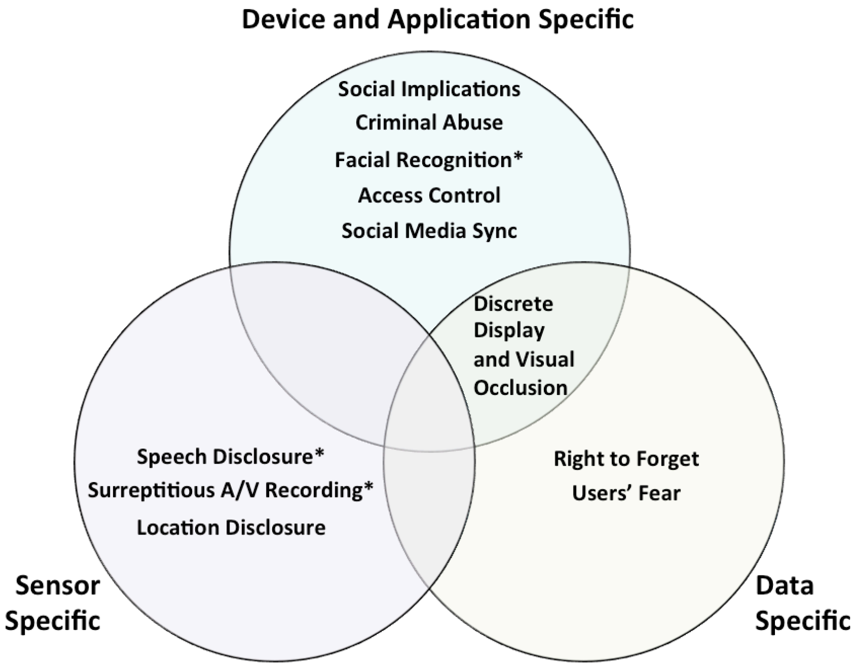

Fig. 1. Privacy Concerns per form factor (* concerns identified particularly for head-mounted devices), and according to their influencing factors: device, application, sensor or data.

5 Discussion

From the analysis of the users' concerns in wearable privacy we note that several factors affect the privacy concerns among users. These include: the nature of the data collected, their respective levels of confidentiality and sensitiveness, ability to share and disclose the information, and also potential implications (social, criminal, etc.).

The findings indicate that privacy concerns are not necessarily unique to one specific device or form factor, but are intimately related to the sensors embedded in the device and the respective data collected. We found that devices that include cameras and microphones resulted in more and more extreme privacy concerns, followed by devices with GPS and displays. Activity trackers that monitor heart rate, steps, and pulse for instance, are usually seen as inoffensive to the users' privacy, however it is likely that users are not aware of how such data could be misused by third-parties or potential privacy implications when the data are collected in a long term or associated with complementary information.

We also note a significant overlap between the users' concerns about mobile privacy and wearable privacy, mostly because the tasks that users can perform with wearables are also possible with alternative devices, which were previously used in a large scale (including cameras, pedometers, and tablet PCs). However from the analysis of the users' comments we do notice that specific characteristics of wearables strengthen these concerns. For example, while cameras and microphones were already employed in mobile devices, wearables make it easier to record data without other people noticing, so their lack of awareness, compliance and consent becomes more critical for privacy in the wearable context. Similarly, users have privacy concerns about location information, primarily because wrist-mounted devices are able to track their position and immediately publish it online in social media applications to a network of contacts. Users worry that this group can include malicious users and people that the individual user does not know or trust.

5.1 Limitations

An extensive list of 38 devices has been covered in the analysis of online comments, however, because the landscape of wearable devices is shifting very rapidly, obviously this list did not include every wearable device possible. For example, our analysis of wrist-mounted devices included six devices, mainly armbands and smart watches. In future work, to complement our research findings, we plan to analyze fitness trackers as well, as we hypothesize that this specific type of WMD may pose more privacy concerns than smart watches and armbands currently do.

Although this work focuses mainly on head and wrist-mounted devices, we believe that chest and back-mounted devices, such as the Polar band for heart rate monitoring and Lumo back band for posture tracking could also raise privacy concerns. To observe this, in future work, we plan to verify potential privacy implications that such devices could involve, and identify potential users' concerns.

Collecting and analyzing online data is a relatively new research method, and despite enabling the analysis of large amounts of contents, it involves two main limitations: first, no well-established and validated protocol is available regarding data collection and analysis, so the method employed in this research is both exploratory and empirical. Second, little is known about the users' profiles, as all data collected is anonymous. However, we can assume that users who post online comments access frequently the web (forums, IT websites) and are interested in technology (to follow new trends and news in the domain). Despite being a niche of users, which limits the generalization of the research findings, they also correspond to actual or potential users interested in wearable technologies.

6 Conclusion

The analysis of the users' comments shows that the privacy concerns about wearables are similar, but in some cases more specific than privacy concerns about mobile devices. It also shows that users are aware about potential privacy implications, but mainly during data collection and sharing. The privacy concerns of users are related to the ability of the wearable device to sense, collect, and store data, which are often private, personal, confidential or sensitive, and then share these data with unknown or untrusted parties.

Users' concerns about wearable privacy cover different aspects of the user interaction with a wearable, including: disclosure of sensitive information, subtle data collection (of audio and video), public posts in social media apps (sharing), and lack of control and awareness regarding who has access to the data collected.

Although the level of privacy concerns of users is similar to that of mobile devices, the nature of their concerns is critical, showing that because users are somewhat unaware about potential privacy implications, vendors should alert them about possible problems, enabling them to apply a fine-grained control about *what* is collected, *when*, and *how*, and also *how* data are shared (*who* has access).

While there is a long way to go to build wearable devices and applications that are actually privacy-enhanced, this work brings insight in clarifying the users' concerns about wearable privacy, aiding to devise better solutions in the future.

7 Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 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.

8 References

1. Acquisti, A., Gross, R., and Stutzman, F. (2011). Faces of facebook: Privacy in the age of augmented reality. *BlackHat USA,* 2011.

2. Berendt, B., Günther, O. and Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. Communications of ACM 48, 4 (April 2005), 101-106. DOI=10.1145/1053291.1053295
3. Caine, K. (2009). Exploring Everyday Privacy Behaviors and Misclosures. PhD Thesis. Georgia Institute of Technology.
4. Thomaz, E., Parnami, A., Bidwell, J., Essa, I., and Abowd, G. D. (2013). Technological approaches for addressing privacy concerns when recognizing eating behaviors with wearable cameras. In UbiComp'2013, pp. 739–748. Retrieved from http://dl.acm.org/citation.cfm?id=2493509
5. Fu, B., Lin, J., Li, L., & Faloutsos, C. (2013). Why people hate your app: Making sense of user feedback in a mobile app store. In Proceedings of KDD'13. Retrieved from http://dl.acm.org/citation.cfm?id=2488202
6. Gürses, S. and Diaz, C. (2013). Two Tales of Pivacy in Online Social Networks. IEEE Security & Privacy, 11(3), 29–37. Retrieved from http://ijeee.in/wp-content/uploads/2014/05/IJEEE-131-134.pdf
7. Hoyle, R. et al. (2014). "Privacy Behaviors of Lifeloggers using Wearable Cameras". In UbiComp '14, Seattle, WA, USA, September 13–17, 2014.
8. Hedegaard, S., and Simonsen, J. (2013). Extracting usability and user experience information from online user reviews. In Proceedings of CHI'2013 (pp. 2089–2098). Retrieved from http://dl.acm.org/citation.cfm?id=2481286
9. Iacob, C., Veerappa, V., & Harrison, R. (2013). What are you complaining about?: a study of online reviews of mobile applications. In Proceedings of the 27th International BCS Human Computer Interaction Conference (p. 6). Retrieved from http://dl.acm.org/citation.cfm?id=2578086
10. Jacob, C., and Dumas, B. (2014) Designing for Intimacy: How Fashion Design Can Address Privacy Issues in Wearable Computing. In *ISWC'14*, Seattle, USA, Sep 2014. ACM.
11. Khalid, H.; Shihab, E.; Nagappan, M.; Hassan, A., (2014) What Do Mobile App Users Complain About? A Study on Free iOS Apps, Software, IEEE , vol.PP, no.99, pp.1,1 DOI: 10.1109/MS.2014.50
12. Könings, B., Schaub, F., and Weber, M. (2013). Who , How , and Why ? Enhancing Privacy Awareness in Ubiquitous Computing. In PerCom'2013, March, 364–367, 2013.
13. Mancini, C., Thomas, K., Rogers, Y., Price, B. A., Jedrzejczyk, L., Bandara, A. K., Joinson, A. N., and Nuseibeh, B. (2009). From Spaces to Places: Emerging Contexts in Mobile Privacy, In: UbiComp'2009, 1–10.
14. Mcnaney, R., Vines, J., Roggen, D., Balaam, M., Zhang, P., Poliakov, I., and Olivier, P. (2014). Exploring t he Acceptability of Google Glass as an Everyday Assistive Device for People with Parkinson, in Proceedings of CHI'2014, 1–4.
15. Motti, V. G. and Caine, K. (2014). Understanding the wearability of head-mounted devices from a human-centered perspective. In *Proceedings of the 2014 ACM International Symposium on Wearable Computers* (ISWC '14). ACM, New York, NY, USA, 83-86. DOI=10.1145/2634317.2634340 http://doi.acm.org/10.1145/2634317.2634340
16. Nguyen, D., and Mynatt, E. (2002) Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems. In Georgia Institute of Technology GVU Technical Report (GIT-GVU-02-16), 2002.
17. Raij, A., Ghosh, A., Kumar, S., and Srivastava, M. (2011). Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11, 11. doi:10.1145/1978942.1978945

18. Reidenberg, J. R. et al., (2014) Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding (August 15, 2014). Fordham Law Legal Studies. At: http://ssrn.com/abstract=2418297
19. Roesner, F., Kohno, T., and Molnar, D. (2014). Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (April 2014), 88-96. DOI=10.1145/2580723.2580730 http://doi.acm.org/10.1145/2580723.2580730
20. Shay, R., Ion, I., Reeder, R. W. and Consolvo, S. (2014). "My religious aunt asked why I was trying to sell her viagra": experiences with account hijacking. In CHI '14. ACM, New York, NY, USA, 2657-2666. DOI=10.1145/2556288.2557330
21. Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., and Borgthorsson, H. (2014). Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use, In CHI '14. ACM, New York, NY, USA, 2647- 2656. http://doi.acm.org/10.1145/2556288.2557421
22. Solove, D. J., (2008) Understanding Privacy, Harvard University Press, May 2008; GWU Legal Studies Research Paper No. 420; GWU Law School Public Law Research Paper No. 420. Available at SSRN: http://ssrn.com/abstract=1127888
23. Starner, T. (2001). The Challenges of Wearable Computing: Part 1. *IEEE Micro* 21, 4 (July 2001), 44- 52. DOI=10.1109/40.946681 http://dx.doi.org/10.1109/40.946681
24. Troshynski, E., Lee, C., and Dourish, P. (2008). Accountabilities of Presence: Reframing Location- Based Systems. In *CHI'2008* Proceedings, 487–496.
25. Ur, B., and Wang, Y. (2013). "A cross-cultural framework for protecting user privacy in online social media." Proc. of the 22nd Int. Conf. on WWW. Steering Committee
26. Warren, S. D. and Brandeis, L. D., (1890) "Right to privacy," Harvard Law Review, vol. 4, pp. 193–220, 1890