Privacy Implications of Smart Wearable Devices

Gautam Worah, Jubeen Shah, Sujal
{gworah, jnshah2, ssujal}@ncsu.edu

1. Project Description & Motivation

Wearable Technology refers to the category of gadgets worn by the user to provide user-specific information to the device it pairs. Wearables have become popular in several high-impact domains such as healthcare, security, and entertainment. This effect is due to their autonomy, small size, and increasingly long battery life.

Wearables are essentially sensor nodes collecting data for the master server (the smartphone). Smartwatches, glasses, clothing, and even jewelry are some of the examples. On the one hand, they provide the opportunity to enhance efficiency across industries by continuously monitoring human activity. However, they also pose security concerns in comparison to other computing devices, because these wearable technologies are so much more personal. The ability of these devices to ubiquitously and continuously collect and transmit data to their sister devices (smartphones, other IoT devices) poses many privacy risks [1]. Their sensitive nature accentuates these privacy risks as they can often reveal vital information about an individual's health, their daily routine, and the people they interact with. Moreover, since the mass adoption of these devices is recent, most users are still unaware of the potential implications of continuous monitoring, storage, profiling, and analysis of health and personal data [2].

The amount and type of data collected by these devices may be used to reveal one's identity, and therefore security challenges are critical to their usage. Thus, the primary motivation of this project is to identify what are the privacy concerns of users, how they perceive the data collection, and what is their level of awareness with regards to the data usage and privacy policies of these devices. The answers to these questions will help us understand what the current mentality of users in the context of smart wearable privacy is, what is their level of understanding concerning the types and extent of data that can be collected and what would be the best means to educate them to protect their sensitive information.

We will be studying the implications caused by a broad category of these devices, in terms of security and privacy vulnerabilities. We will also discuss how the type of data collected, frequency of data collection, and the privacy risks posed depending on the type of wearable used.

2. Related Work: Background & Literature Review

Privacy and security concerns have been discussed for a long time, but the implications with respect to wearable devices are still relatively new [3]. In general, smart devices continuously collect data via sensors and their complex designs accrue various challenges in providing user privacy. Although many studies have been focused on mobile devices, applications etc. , there is still a vast scope in understanding the privacy behaviours of wearable technology[4,5]. This is mainly due to the fact that these sensors are able to store and process user's sensitive information. And this information could infer potential risks especially when combined with any kind of auxiliary data from other sources [6].

In [7,8] the authors have determined some key psychological factor that affect the adoption of smartwatches, we leverage the analysis from the paper to underscore the fact that privacy concerns are not

key amongst the people adopting smartwatches, or smart wearable devices. This combined with other related work we would be working towards the hypothesis that if given enough information, consumers would change their mind about adopting new smart wearable devices, if there are privacy concerns.

3. Approach

For this study, we have divided the wearable smart devices space into three broad categories:

1. Glasses
2. Watches and Trackers
3. Clothing

Each category is unique because of the various types of data collected (such as smart glasses collect data about location and images, whereas smartwatches collect more data on health metrics, usage patterns, frequent services used).

For each of these categories and their related products, we will be studying their privacy policies to understand the information collected by the respective devices, at the same time, also realizing if the data collected is in line with the product category. We also intend to look for possible vulnerabilities in their policies which might compromise the user's identity in some scenarios. Additionally, we will be creating a user study covering the various aspects of the policies and how the data collected could be used by brands for their businesses. The user study may include user awareness and acceptance of data sharing and storage practices, anonymization steps, sensitive data encryption measures, and transmission security. We will also analyze how easy it is for users to be able to modify or opt out of these settings. We will understand the relevance of the information collected by the devices and verify their importance under their respective scopes. This analysis will include activities to determine whether an application needs permission for a particular feature and are users aware of these "hidden" features.

Finally, we plan to design user surveys in correspondence with the results of our study of their privacy policies. For example: First, we will be describing the product and ask the user if he/she will buy it or not. Next, we will uncover some information to the user taking the survey, from the privacy documents for the chosen products. Further, we will describe its implications (if any) and ask the same question again. We hypothesize that once the users are aware, their outlook might change, change their minds about buying a particular product which might give us useful responses to gauge user awareness as well.

4. Evaluation Plans and Milestones:

- Milestone 1: Feasibility study and User analysis
    - Reading about the different types of devices and studying the kind of data they collect.
    - Based on the above, construct a user study to be conducted.
- Milestone 2: Data acquisition
    - Conduct user studies to collect information on user's knowledge of the type of data being collected, devices which collect data, awareness about the data sharing practices of the device and application developers, privacy policies etc.
    - Collect data from the devices and their companion mobile applications (if possible)
- Milestone 3: Data Analysis & Inference
    - Analyse the implications on the basis of the study and understand the user's concerns for wearable privacy, what types of concerns are prevalent among which specific types of devices.
    - Conclusion

5. Timeline

Milestone	Start	End
Milestone 1: Feasibility study and User analysis	09-30-19	10-13-19
Milestone 2: Data acquisition	10-14-19	10-31-19
Milestone 3: Data Analysis & Inference	11-1-19	11-28-19

6. References

1. Greig Paul and James Irvine. 2014. Privacy Implications of Wearable Health Devices. In *Proceedings of the 7th International Conference on Security of Information and Networks* (SIN '14). ACM, New York, NY, USA, Pages 117, 5 pages. DOI: https://doi.org/10.1145/2659651.2659683
2. Motti, Vivian Genaro, and Kelly Caine. "Users' privacy concerns about wearables." In *International Conference on Financial Cryptography and Data Security*, pp. 231-244. Springer, Berlin, Heidelberg, 2015.
3. Mancini, C., Thomas, K., Rogers, Y., Price, B.A., Jedrzejczyk, L., Bandara, A.K., Joinson, A.N., Nuseibeh, B.: *From spaces to places: emerging contexts in mobile privacy*. In: Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp 2009), pp. 1–10. ACM, New York (2009). doi: 10.1145/1620545.1620547, http://doi.acm.org/10.1145/1620545.1620547
4. Troshynski, E., Lee, C., Dourish, P.: *Accountabilities of presence: reframing location-based systems*. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2008), pp. 487–496. ACM, New York (2008). doi: 10.1145/1357054.1357133, http://doi.acm.org/10.1145/1357054.1357133
5. Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., Kapadia, A.: *Privacy behaviors of lifeloggers using wearable cameras.* In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2014), pp. 571–582. ACM, New York (2014). doi: 10.1145/2632048.2632079, http://doi.acm.org/10.1145/2632048.2632079
6. Raij, A., Ghosh, A., Kumar, S., Srivastava, M.: *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 (CHI 2011), pp. 11–20. ACM, New York (2011). doi: 10.1145/1978942.1978945, http://doi.acm.org/10.1145/1978942.1978945
7. Apurva Adapa, Fiona Fui-Hoon Nah, Richard H. Hall, Keng Siau & Samuel N. Smith (2018) *Factors Influencing the Adoption of Smart Wearable Devices*, International Journal of Human–Computer Interaction, 34:5, 399-409, DOI: 10.1080/10447318.2017.1357902
8. Kim, K. and Shin, D. (2015), *"An acceptance model for smart watches"*, Internet Research, Vol. 25 No. 4, pp. 527-541. https://doi.org/10.1108/IntR-05-2014-0126