Wearable Devices: Privacy Concerns

Shalby Hazem (10596243)

February 2023

Abstract

The popularity of wearable devices is growing, especially in the context of the metaverse. Wearables offer a means for users to interact and navigate in the virtual world. They also collect data on the user's physical and physiological state to create a more personalized virtual experience. However, with the increased use of wearables, privacy concerns arise. The purpose of this paper is to analyze these concerns with the purpose of highlighting the importance of prioritizing privacy in wearable devices for customers, companies, and society, as existing solutions are inadequate to preserve privacy.

Keywords: *Wearable; Privacy; Surveillance; Discrimination; Metaverse;*

Contents

1 Introduction 1

2 Background 2

2.1 Wearable devices . . . 2

2.2 Privacy . . . 2

3 Relevant Ethical Issues 3

3.1 Data type . . . 3

3.2 Lack of security . . . 3

3.3 Extracted information . . . 4

3.4 Surveillance . . . 4

3.5 Discrimination and bias . . . 4

4 Responsibility 5

4.1 Customers . . . 5

4.2 Companies . . . 5

4.3 Society . . . 6

5 Conclusions 6

6 Relevant future issues 6

1. Introduction

The popularity of wearable devices (devices that are worn on the body) is growing, especially in the context of the metaverse (virtual reality, augmented reality, and internet). Wearables offer a means for users to interact and navigate in the virtual world. They also collect data on the user's physical and physiological state to create a more personalized virtual experience. However, with the increased use of wearables, privacy concerns arise.

This paper aims to highlight the importance of prioritizing privacy in wearable devices for customers, companies, and society, as existing solutions are inadequate to preserve privacy.

To meet the proposed goal, the paper will first provide an overview of the central arguments regarding wearables and privacy. Then, it will focus on the primary privacy risks posed by wearables [1] and examine the responsibilities of users, companies, and society. Finally, the paper will conclude with some reflections over the proposed goal.

In this paper, the main focus is to evaluate some of the proposed solutions to privacy preservation issues to highlight their weakness. This is mainly done by using examples that demonstrate the inadequacy of these solutions in protecting privacy.

2. Background

In this section, a background about the two main arguments discussed in this paper (wearable and privacy) will be given.

2.1. Wearable devices

Wearable devices are technologies designed to be used while worn on the body and they combine the basic functionality of wearables (e.g. time for watches) with a lot of other innovative functionality (e.g. health monitoring). These kinds of devices are mainly characterized by some communication mechanisms (e.g. wireless, Bluetooth) that allow them to exchange information with other devices (e.g. smartphone) and a set of sensors that allow them to collect data about the environment around them (e.g. location, compass, and altimeter) and the user wearing them (e.g. heart rate and sleep patterns). Wearable devices have the potential to revolutionize healthcare, by providing doctors and researchers with real-time data about an individual's health and fitness.[2]

Wearable devices have become a topic of interest recently due to the development of technologies that increase their durability in terms of battery life, and due to the development of novel solutions capable of performing on-device analytics [2] (Machine learning techniques) at extremely low power consumption; The possibility of elaborating a lot of data (mainly generated by sensors) on the device, allows the implementation of applications which are aware of the user's context, including their environment, sensations, and perceptions.

The importance of wearable devices is also highlighted by reports that show that the number of wearable devices connected in 2020 was approximately 835 million, 929 million in 2021, and 1105 million in 2022, and current trends predict the number to increase. [3]

Due to the growth of usage of such devices, we are dramatically increasing the amount of personal data that can be collected by service providers. The expansion of such systems brought to light problems related to privacy preservation, which will be discussed later in this paper.

2.2. Privacy

Privacy is a fundamental right that is essential for maintaining personal autonomy and freedom. It refers to the ability of individuals or groups to control the access to and dissemination of their personal information, behavior, and communication.[4] Privacy can be protected by laws, social norms, and technical means.

One of the main ways in which privacy is threatened is through data breaches, where sensitive personal information is accessed or stolen by unauthorized individuals or organizations. An example of this type of threat is the PumpUp app which in 2018 leaked health data, private messages, and full credit card data in some cases.[5]

Another major threat to privacy is government surveillance; this type of threat is particularly concerning in countries with weak human rights respect, where surveillance may be used to target certain individuals or groups based on their political thoughts. Surveillance issues may not seem important in countries where human rights are respected but this is not always the case. Indeed, an example of this issue is discussed in [6], where a worker, who worked remotely, had been ordered to pay back the equivalent of £1500 in wages to her ex-employer, after tracking software deemed she had "misrepresented" hours of work.

The previously explained threats are only two of the major ones, that are used to highlight the importance of preserving privacy. The importance of privacy has been treated also by James Rachels in [7], where the main topic is to answer the question: *why privacy is important?* In particular, James Rachels gave some of the reasons (four) for which privacy preservation should be emphasized.

The first one is that Privacy is sometimes necessary to protect people's interests in competitive situations (e.g. if a chess player is not able to analyze an adjourned position in private, without his opponent learning his results, it would put him in an unfair disadvantage).

The second one is that sometimes people want to hide some aspects or behaviors of their life just because it would be embarrassing for other people to know about them (e.g. A person with something such as a mental health disorder or a sexually transmitted infection, may not want others to know about it).

The third reason is confidentiality (e.g. Revealing a pattern of alcoholism or drug abuse can result in a man's losing his job).

The last reason is that people don't want to be judged with unrelated facts (e.g. When people apply for credit, they are often investigated and the result is a fat file of information about them, but they may not want to be judged with information regarding sex-life, political view, etc.).

The analysis done by James Rachels in [7] is more complex than what has just been reported but for the purpose of this paper, these four points can be used to evaluate the privacy preservation in wearable devices. Although the presented reasons are not explicitly linked to any part of the paper, readers can easily connect them to some of the presented cases.

Nowadays privacy is a relevant aspect in the development of any application where some data about the user's context are collected. In particular, the main issues to consider are related to how sensitive data are collected, elaborated, stored, and shared by companies. To meet this need of protecting privacy, some laws have been put in place such as the General Data Protection Regulation (GDPR) in the European Union, and California Consumer Privacy Act (CCPA) in California.

3. Relevant Ethical Issues

In this section, a discussion regarding the main factors that raise privacy concerns in wearable devices will be carried out. In particular, the main goal is to demonstrate that the current solutions for privacy preservation in wearable devices are inadequate in solving or mitigating these problems.

The unifying theme across the next subsections will be that Wearable technology collects and elaborates a significant amount of sensitive data, and this in different ways raises concerns about privacy preservation that are needed to be considered.

3.1. Data type

In wearable devices, it is not often a matter of how much data are collected, even if it's a huge amount of data (335PB of data per month in 2020 [8]), but it is a matter of the type of information we can collect, in fact, information about physical activity, sleep patterns, and location can be collected by wearables. This type of data can for sure be used to improve the user experience (e.g. health monitoring applications can track a patient's condition and detect or predict medical issues that are reported to a humans agent which acts accordingly in the best way possible for the patient) but can be used to also obtain the user's sensations and perceptions of the environment around them.

The relevance of this issue came out also because these data are often transmitted to the device's manufacturer, and can also be shared with third parties for research or marketing purposes. An example that allows to understand the importance of this issue can be given by a fitness tracker (e.g. Fitbit), that could be hacked (not a hard task due to a lack of security) and used to track the user's location, and this could be seen as a violation of privacy, as it allows others to monitor user movements and activities without their knowledge or consent.

3.2. Lack of security

Another factor that creates concerns is the lack of security in wearable devices, which is due to their hardware constraints (i.e. limited computation power, memory capacity, and battery life) which don't allow the implementation of the most robust security measures. This means that the data collected by the device could be vulnerable to hacking or other forms of cyberattacks, which could have serious consequences for the affected user.

To mitigate these risks, companies can design and develop their products in such a way that robust security measures such as encryption, secure communications, and strong authentication are implemented. These techniques can be used to at least mitigate the risks of undesired intrusions but usually, they are not implementable in the wearables, due to the hardware constraints, or implementing them cause a huge drop in the application's performances (e.g. encrypting all the communications between the device and the external environment requires time and energy and this can be in contrast with the real-time and energy efficiency requirements of a certain application).

An example of this issue is what happend in 2016 when some fitness bands used a key exchange protocol that was created specifically for communicating over Bluetooth in an energy-efficient way. This protocol meets the design goals of using very little energy and running in a small amount of time, but it can be easily compromised. Indeed, it has been proved that using a normal processor (core i7), all the possible combinations of key pairs can be guessed in a single second.[9] This seems an isolated instance but in wearable devices, the hardware constraints often shape the way in which the security measures are implemented. As a result, less secure measures are favored over more secure ones as the latter often require hardware capabilities beyond what is available on the device.

3.3. Extracted information

A significant concern with wearable technology is the extraction of sensitive information from the device sensor data, potentially revealing details about the user's activities. This seems an irrelevant problem but usually the type of information leaked in this case is more sensitive since it is external to the device.

This is a complex concept and the best way to explain it is using an example: Imagine a user wearing a smartwatch and digiting the PIN code on his smartphone; If a hacker can track the user's movements and actions, they could try to infer information about the user's typing habits, such as the length of time between key presses, which could be used to make guesses about the user's PIN code. This task seems technically unrealizable but a team from the Stevens Institute of Technology has proved that by using collected key entry traces it's possible to infer the PIN code with an accuracy that is more than 90%.[10] The just described is just an example of what this issue is about but more complex ways in which external to the device information can be leaked are available.

3.4. Surveillance

Another major threat to privacy is the usage of wearables for surveillance purposes. This is due to the fact that a good portion of wearable devices contains cameras and microphones that can be used to capture images or videos or to record audio without the knowledge or consent of the users.

The problem becomes more relevant with the presence inside the device of other types of sensors, that allow capturing the user's movement and location. Indeed, an unauthorized agent or simply someone who has access to the data generated by the device can have complete sight of what the user is doing (camera and microphone), where the user is (GPS), and how the user is doing it (movement capture). An example of this issue is the usage of smartwatches to monitor employee movements. This happened in China in 2019, where Street cleaners were forced to wear GPS-tracking smartwatches so employers can monitor how hard they work.[11]

A misconception about surveillance is that it becomes an issue only if the device is compromised by an unauthorized agent (such as a hacker intercepting the data) and that in normal circumstances, companies are not monitoring the users. This is not always the case, as proved by the case of the Street cleaners just mentioned[11]. Indeed, Surveillance is an issue even with the not compromised devices, because there is a lack of regulation specifically addressing the use of wearables for surveillance. To solve this problem governments should make laws that prohibit the use of wearables for surveillance purposes but creating laws to preserve privacy is often a challenging task. This is due to the rapid growth of this type of technology, in fact sometimes emerging products can easily neglect existing regulations for privacy matters. The task is made harder also because usually privacy is negligible compared to the benefits that the product offers.

3.5. Discrimination and bias

Wearable technology has the potential to generate discrimination and bias. This is because the data collected by wearables may be used to make decisions about a user's health or fitness or to judge him, but this data may be not accurate or may be unrelated to the taken decision. Additionally, data collected by wearables may be used to make decisions about users' employment or insurance, which could lead to discrimination based on factors such as age, gender, or ethnicity.

An example of this issue is the usage of a wearable in the workplace to monitor employee productivity, in fact, the extracted data can be used to make an evaluation of the employee's performance and to decide about a possible promotion, and this can lead to possible discrimination in the work environment. The collected data may have not taken into account the employee's circumstances, such as disabilities, family, or medical conditions at that moment, and this may lead to discrimination based on factors such as gender (e.g. pregnant woman's productivity is reduced due to her unique condition).

4. Responsibility

When it comes to responsibilities, there are two types: active responsibility and passive responsibility. Active responsibility refers to the actions and duties one takes to prevent negative events from occurring, such as taking care of a certain person or situation. Passive responsibility, on the other hand, is focused on addressing and mitigating the consequences of negative events that have already occurred [12]. In summary, active responsibility is about taking steps to prevent negative events from happening, while passive responsibility is about addressing the consequences of negative events that have already occurred. In [13], the author has presented some suggestions to solve the problem of preserving privacy in the wearable framework. In particular, what the author has presented are the responsibilities that customers, companies, and society must fulfill to tackle the problem of privacy preservation regarding wearable devices. For sure the responsibilities of these three subjects is both passive and active but the most important is the active one since when talking about privacy the foremost priority is taking steps to prevent negative events (i.e. privacy invasion) from happening.

In the following sections, this paper will focus on presenting the responsibilities of the three subjects discussed in [13] and will present some limits to what the author suggests that prevents the three subjects from fulfilling their responsibilities.

4.1. Customers

In [13] the author say that it's crucial for customers to increase their knowledge of privacy and to be cautious when uploading personal information. For instance, many customers fail to pay attention to the authorization for data access when installing a new application. It's essential for customers to prioritize privacy when granting access or privileges to any third party.

The declaration of the author sounds good at first glance, but when a user downloads and installs a certain application, he may be asked to grant certain permissions (e.g. camera or location) but he may not fully understand the implications of granting these permissions and he will end granting them because of the need to use the services that this application is offering. This issue can be solved by being more selective about which applications to download and only granting permissions to applications from trusted sources.

What has just been suggested as a solution to a problem, raises another concern: *how to select a trustworthy source?* It can be challenging for a customer to determine which source is reliable. This task becomes even more complex because it is not only a matter of trusting enough the source of the application but also a matter of trusting the way in which this application manages and shares the data the customers are granting the application access. What happened with the Cambridge Analytica scandal in 2014 [14], even if is not a wearable-related example, can be used to clarify this issue. Although Facebook is often considered a trusted source or at least a common customer trusts it because of the need for its service, the way in which they used to share the customer's personal data, resulted in sensitive information of tens of millions of users being harvested without their knowledge or consent.

4.2. Companies

In [13] the author says that companies should take on more responsibilities rather than producing devices only, and suggests to consider the eight principles about private information set by OECD.[15]

The most interesting principle for privacy preservation tasks is the limitation principle which states that companies should not share the data without the authorization of customers or sell data for commercial profits. This principle is more or less equivalent to the definition of Privacy reported at the beginning of this paper, in fact controlling the access to and dissemination of personal information is the same as authorizing the company to share personal data with a certain agent. This looks like gold for the privacy preservation issues, but an analysis from the point of view of the companies is needed. Thus a comparison of the benefits in terms of profit between selling data with and without user authorization is needed. As easily deducible, the average user will not authorize the companies to share data with other companies, therefore the profit will be reduced, and consequently also the company's interest in asking for the user's consent to share data.

Here only the most interesting of the eight principles has been analyzed but also the other seven have some limits that make them not beneficial to implement for the companies.

4.3. Society

In [13] the author say that stronger supervision must be carried out by organizations. Food and Drug Administration has released regulations on wearables and guaranteed digital health (Dolan, 2015). The supervision task is however a hard task because due to the rapid growth of this field, sometimes emerging products can easily neglect existing regulations for privacy matters.

5. Conclusions

The paper demonstrates that under certain conditions, the justifications for privacy as outlined by James Rachels [7] can be completely disregarded. Additionally, the use of wearable devices raises privacy concerns due to their inherent lack of security, which is a consequence of their hardware constraints. Even in instances where no security breaches occur, wearable devices may still be utilized in a manner that violates privacy, specifically in this paper the case of wearable devices used for surveillance purposes has been analyzed.

In conclusion, privacy for wearable devices is a vital aspect for everyone and users shouldn't get used to a world in which they have zero privacy but they should attempt to protect it. As Snowden said, "Privacy is not something that I'm merely entitled to, it's an absolute prerequisite". Therefore customers should opt for devices that prioritize privacy, companies should make privacy a priority when creating new products, and society should regulate these products and establish laws to protect privacy.

6. Relevant future issues

This section is devoted to present some cases in which wearable devices are used in a way that is ethically relevant. This section is reported after the conclusions on purpose since the cases that will be reported are only a hint for future discussion about wearable devices.[1] As these examples (mainly from [2]) will not be the subject of other analysis, here is a list of them:

- Using the acceleration data on the watch, a classifier that can recognize the characters written can be built.
- Using wearables to detect smoking gestures;
- Wearable device used to detect the activation of skeletal muscles;
- Wearable used to detect activities such as chewing, drinking and talking with an accelerometer and classify the activities as the users move teeth differently

[1] For sure these examples can be related to privacy issues but for the purpose of the paper other examples have been used

References

[1] Holger Regenbrecht, Sander Zwanenburg, and Tobias Langlotz. Pervasive Augmented Reality—Technology and Ethics. *IEEE Pervasive Computing*, 21(3):84–91, July 2022.

[2] Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, and Aruna Seneviratne. A Survey of Wearable Devices and Challenges. *IEEE Communications Surveys & Tutorials*, 19(4):2573–2620, 2017.

[3] Global connected wearable devices 2016-2022.

[4] Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, and Martijn Warnier. Privacy and Information Technology. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University, summer 2020 edition, 2020.

[5] A popular fitness app leaked health data and private messages.

[6] Ethical issues arise as tracking software gets employee sacked.

[7] James Rachels. Why Privacy is Important. *Philosophy and Public Affairs*, 4(4):323–333, 1975.

[8] Storage in the Exabyte Era.

[9] Are Fitness Bands Secure? There's More to It Than Just the Clasp!

[10] Chen Wang, Xiaonan Guo, Yan Wang, Yingying Chen, and Bo Liu. Friend or Foe? Your Wearable Devices Reveal Your Personal PIN. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 189–200, New York, NY, USA, May 2016. Association for Computing Machinery.

[11] 'Work harder! Work harder!': Backlash over Chinese street workers forced to wear monitoring devices. *ABC News*, April 2019.

[12] Ibo van de Poel and Lamber M. M. Royakkers. *Ethics, Technology, and Engineering: an Introduction.* Wiley-Blackwell, Malden, Mass, 2011.

[13] Victor Chang, Xin Xu, Barbara Wong, and Victor Mendez. Ethical problems of smart wearable devices: 4th International Conference on Complexity, Future Information Systems and Risk. *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, pages 121–129, May 2019.

[14] Alvin Chang. The Facebook and Cambridge Analytica scandal, explained with a simple diagram, March 2018.

[15] OECD Privacy Principles.