Wearable Technology, Privacy Issues

Pablo Saa[1(✉)], Oswaldo Moscoso-Zea[1], and Sergio Lujan-Mora[2]

[1] Faculty of Engineering Sciences, Universidad Tecnológica Equinoccial, Quito, Ecuador
psaa@ute.etu.ec
[2] Department of Software and Computing Systems, University of Alicante, Alicante, Spain

Abstract. The market of wearable devices, which includes advanced devices such as smart watches, fitness trackers, augmented and virtual reality headsets, wearable cameras and other gadgets, is growing at a spectacularly fast pace thanks to the acceptance by users with open arms. However, there exist some concerns about how wearable devices could affect people's privacy. This paper presents a literature review of privacy issues related to wearable devices. Due to the novelty of this topic, there is a lack of legislation and most wearable manufacturers do not respect the privacy of their customers. The main concern is related to the potential incorrect use of health data collected by wearable devices. Finally, from the information reviewed, several implications to be considered by all stakeholders are drawn.

Keywords: Wearables · Wearable technology · Privacy issue
Wearables regulations · Wearable data

1 Introduction

Advances in science and technology and the proliferation of devices connected to the Internet, sensors and mobile apps are critical factors to an increase in smart devices that can be attached to the human body. These types of devices are called wearable devices. Wearable technology or wearable devices are "clothing and accessories incorporating computer and advanced electronic technologies" [14].

Wearables started its development with the main goal to enhance the functionality of clothing [11]. This development bridges the gap in making technology pervasive into people's daily life. Today, wearable technology is becoming popular and is growing and gaining momentum quickly for personal and business use. A forecast expects the market to grow from 84 million units of wearables in 2015 to 245 million units in 2019, with a market to be worth $25 billion [4].

Companies like Google and Apple are taking the lead on the wearable devices market and are offering people an infinity of newly and trendy devices. This

The original version of this chapter was revised: Affiliation of first and second authors has been updated. The erratum to this chapter is available at https://doi.org/10.1007/978-3-319-73450-7_110

Á. Rocha and T. Guarda (eds.), *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018)*, Advances in Intelligent Systems and Computing 721, https://doi.org/10.1007/978-3-319-73450-7_49

wearable market is forecast to grow by 78 % each year, until reaching 112 million in 2018 [2]. There are many reasons for an exponential adoption of these devices in the very near future. The most important reasons for these global adoption are: low prices, high customer perceived value and low perceived risk [28].

Despite the positive aspects, sound functionality and higher expectations of mass adoption of wearable devices, there is still some work to do. One of the fields which need much attention before these devices reach a mature stage of commercialization is information security, specifically risks concerning privacy issues. Privacy has been considered one of the biggest barriers to the mass uptake of this emerging technology, as it will be discussed along this paper. Legislation has to be created to protect users and restrict manufacturers and companies the use of personal and health information.

After introducing the topic of this paper in this section, the rest of the paper is structured as follows: Sect. 2 presents a literature review on the wearable topic; Sect. 3 summarizes an analysis about privacy violation by exploiting wearable devices; Sect. 4 describes existing legislation and regulation; Sect. 5 presents the implications for the adoption of this technology; finally, Sect. 6 provides conclusions of the work.

2 Literature Review

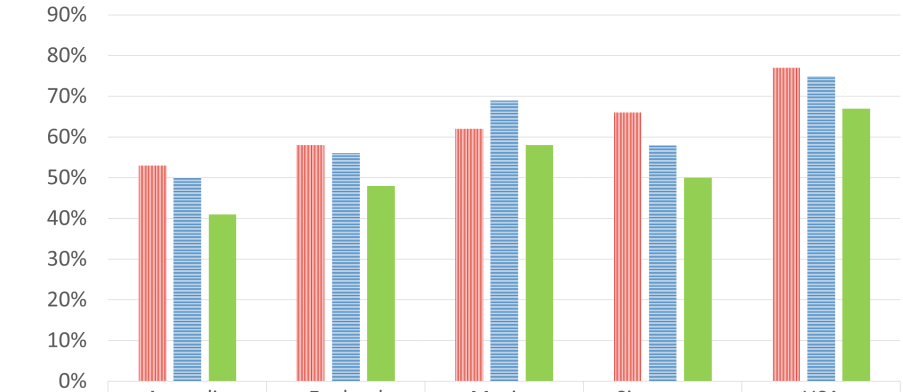
The terms "wearable technology", "wearable devices", and "wearables" all refer to electronic technologies or computers that are incorporated into items of clothing and accessories which can comfortably be worn on the body. These wearable devices can perform many of the same computing tasks as mobile phones and laptop computers [25].

Wearables are expected to provide the users certain information about health, fitness, disabilities, aging, education, enterprise, finance, transportation, gaming, and music in real time. Today, some examples of wearable devices include watches, glasses, contact lenses, smart fabrics (e-textiles), beanies (caps), headbands, jewelry (rings), bracelets, and hearing aid-like devices (earrings).

Before wearables were open to the consumer market, they were used in the field of military technology and had a considerable implication for healthcare and medicine. Nowadays, wearables are mainly projecting their aim in the fields of fitness, health, and dietary, considering the demand of users that are interested in acquiring these technological devices and what information they want to receive from wearable technology [17], as is shown on Fig. 1.

As any other technology, wearables extends the capabilities of a person through different features, providing enhanced communication, sensing, recognition, memory, and logistical skills, such as filtering phone calls or just monitoring the health. A clear example of this kind of devices is a special vest developed by "VivoMetrics", which allows to accelerate treatment in patients by monitoring their blood pressure and heart rate.

Wearable computing devices are no longer just modern and fashionable accessories that complement our mobile devices, they are taking their own place in our day to day lives, becoming an integral part of the business world. In the



	Australia	England	Mexico	Singapore	USA
Exercise	53%	58%	62%	66%	77%
Medical	50%	56%	69%	58%	75%
Dietary	41%	48%	58%	50%	67%

Fig. 1. What consumers want from wearables [17]

article "Why Wearable Tech Will Be as Big as the Smartphone" from the Wired Journal, many of their editors agree with the idea that "A new device revolution is at hand: Just as mobile phones and tablets displaced the once-dominant PC, so wearable devices are poised to push smartphones aside" [27], this statement ensures a successful growing for wearables' business in a non-so far future. However, in the other hand, there is a social and cultural impact of wearables for the privacy issues, especially for the health information that this devices generate.

"The distinguished capabilities of these devices are also the very reasons they require security and privacy protections of an unprecedented scale" [7, p. 75].

2.1 Privacy Issues

Compared to the smartphones and tablets, most of the wearable devices are designed with smaller size and readily attached on one's body, such as bands, watches, glasses, and so on. With the wider adoption by both consumer and enterprise sectors, more privacy issues are also brought by wearable devices to the people who are wearing and surrounded by those gadgets.

2.2 Health Data

As described in section two, the main features that the wearable manufacturers are promoting are: activity tracking, fitness, and dietary. However, in regards to data collection, wearable devices go further on top of the relatively traditional electronic portable devices [20]. Besides the common concerns on personal information, wearable devices are also recording health data as: users' steps, blood pressure, heart rate, sleep pattern, and other private medical data including dietary. All these information is more private and more sensitive than a mobile number and an email address [8].

2.3 Health Data in Consumer Sector

When the data is synchronized to the dashboard through a mobile or laptop, the users' data collected by the wearable devices is loaded into the centralized database maintained by the wearable manufacturer [13]. Thus, these private data can be potentially exploited by the manufacturers in order to generate more profit without the user's consent.

In most privacy policies of the wearable manufacturers, the possibility of releasing the sensitive health data without users' consent, are unequivocally disclosed with statements. For instance, users skip statements such as "We may share your information with third parties..." [12]. This implies that the wearable manufacturers are potentially able to abuse of users' health information and sell it to other commercial companies, affecting users' privacy. For example, the consumers can intermittently receive spam from some "health advisors", and the health insurance companies can adjust individual's premium based on acquired data, without user's awareness [21]. Also, the use of application programming interfaces (APIs) can enable more third-party programs to access the consumers' sensitive health data for different purposes, while consumers have no idea about their privacy policies and few awareness of what would happen.

In addition, according a report published in 2014 [16], 43 % of users were unwilling to share health data with friends and family because they did not feel comfortable sharing any information about their health condition. However, by 2016 the "The Wearable Life 2.0" report [17, p. 5] states that "Consumers are also less likely to agree that wearable technology will make us more vulnerable to security breaches" and that "will invade their privacy". While results show increased comfort levels between 2014 and 2016, there still a 25 % of consumers that would not trust any company with personal information associated to wearable technology [17]. Figure 2 clearly shows how consumers are still unhappy to trust their personal data to companies, by allowing them to capture their information through wearable technology.

Eventually, the default settings of social share and profile in the wearable devices are still posing more privacy leaking. Fitbit, one of largest wearable manufacturers, used to have default privacy setting as enabling the profiles created by the users, to be searchable by search engines like Google, Bing, and so on. This even includes the most intimate personal information, such as the sexual activity recorded in the profile [19]. Obviously, in this case the wearable manufacturers did not take proper actions to protect the users' privacy.

2.4 Health Data in Enterprise Sector

The wide adoption of wearable devices in enterprise sectors is also raising more privacy issues. By 2018, Gartner states that "two million employees will be required to wear health and fitness tracking devices as a condition of employment" [9].

Besides being a handy companion device to the laptop and smartphone, wearables, particularly smart watches and fitness bands, are mainly applied by

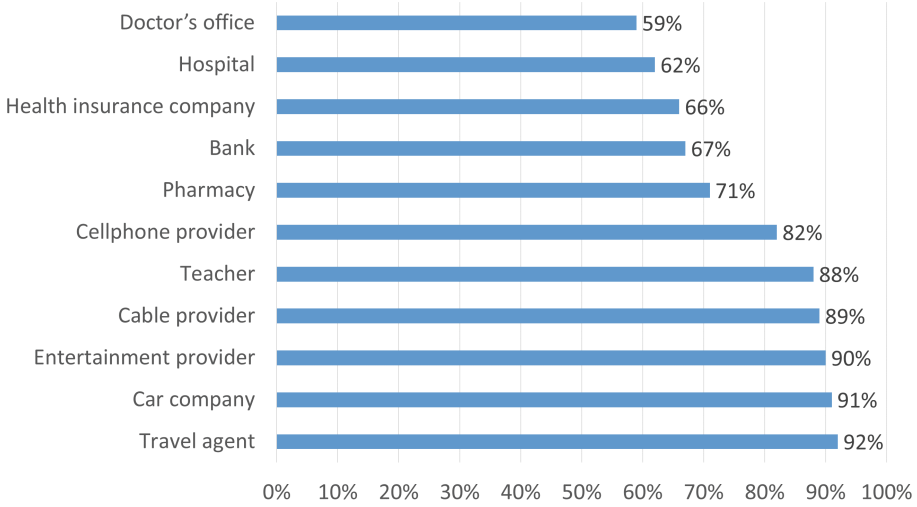


Fig. 2. Consumers' non-trusted companies to capture their information through wearables [17].

the employers to promote the staff wellness program. The wearable devices are distributed to and worn by employees to track their activities, heart rate, sleep pattern and so on, as their normal functions [26]. Then, these health data will be collected and analyzed by the employers and aimed to help employers identify the stress levels and fatigue levels of employees [17].

Considering these benefits, wearables offer a wealth of possibilities for both employer and employee. However, employees are not interested on wearing any of these devices, unless their employers give them any kind of incentive, or provide the devices for free. A survey conducted in five different countries by PriceWaterhouseCoopers obtained the top five biggest hesitations with regards to purchasing a wearable [17]. These results were organized in order to show the reasons from the most to the less important. To clarify what is stated, a radar chart (Fig. 3) is depicted to show how the price of a wearable is the main barrier from customers at the time to decide to purchase a wearable. Then, usability and utility follows the list, which indicates that customers will not pay a lot of money for something they do not even know if they would use.

Finally, the complexity of a wearable itself and the privacy issues that these devices arise, still being top concerns from employees by adopting this corporate trend (see Fig. 3). An extreme case occurred in a hi-tech office complex in Sweden, named Epicenter. This company requires employees to be implanted a tiny RFID chip in their hands [5]. This wearable technology furthers more than fitness bands, considering that employees are forced to implant them during work. The health data that wearables collect would readily blur the boundaries between work and routine life. Therefore, potentially invade employee's privacy, as the non-working life is also monitored by the employers and wearable

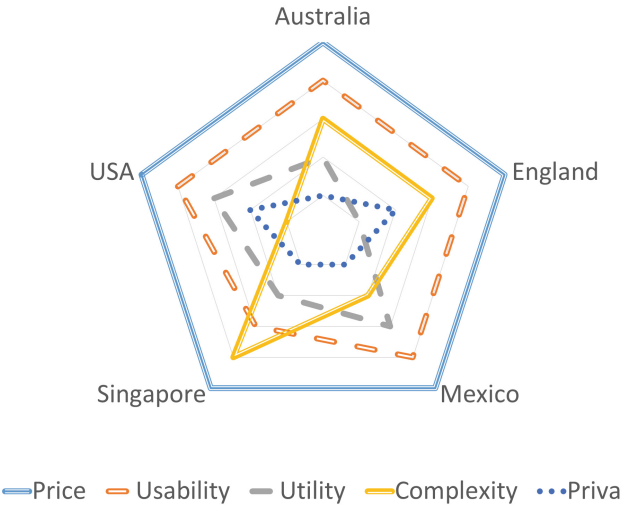


Fig. 3. Consumers' biggest hesitations with regards to purchasing a wearable [17].

manufacturers [23]. Furthermore, the legislation [8] only regulates on customer's personal and health information, while employees' privacy is completely uncovered, implying more serious risks.

3 Privacy Violation by Exploiting Wearable Devices

Besides the privacy concern from the consumers by wearing these technological devices, the privacy of other people within the consumer's proximity is also at risk. Some wearable devices not only track the user's own activities, they also record what the world is like within the user's proximity.

A good example to analyze are the Google Glasses, which raise companies' and people's extensive privacy concerns since its first debut. This is mainly due to the equipped mini camera that is constantly recording everything in front of the screen, which actually, somehow could affect indirectly others. Particularly, if facial recognition technology is implemented to the Google Glasses, people will be easily identified with effective data processing, and all behaviors will be recorded. Their privacy would be readily violated and people would have to be conscious of what it means [24]. Therefore, many restaurants, bars, casinos, and some other public places quickly banned Google Glasses [3], including Google's own shareholders meeting [10].

Even that Google has announced to forgo the plan of incorporating facial recognition technology in Google Glasses [22], it would still be difficult to restrain other similar privacy infiltrating technology in other wearable devices [18]. For example, the Samsung Galaxy Gear is likewise armed with a camera, yet less obtrusive, but can be maliciously abused to invade others' privacy.

4 Legislation and Regulation

As mentioned above, by collecting the data through gadgets, wearable manufacturers would be able to access the users' personal and health information, analyze the data, and share the outcomes, generating more profit. All this under their blurred privacy policies. The API function also enables third-party integration to access the data. A critical reason for those ambiguous privacy policies is that currently there are no mature regulations and legislations to protect customer's privacy and restrict the use of personal information by the emerging wearable technology.

A good example of a country that is working on legislation in this area is Australia. The "Australian Privacy Principles (APP) belonging to Privacy Act regulate the handling of personal information by Australian government agencies and some private sector organizations" [15]. It states that an APP entity that collects personal information for a particular purpose should not use those data for another purpose unless the customer consent, or in certain excepted situations [15]. This seems to provide powerful principles on restricting the data trading practices. But it has not clearly explicated the emerging trend of wearable devices, and, therefore, the uncertainty and possibility of not being applicable still exists [6]. In addition, only those private companies and Australian government agencies that have an annual turnover of at least 3 million AUD (Australian Dollars) are subjected to the Privacy Act [8]. Thus, other private organizations of small-scale may still use personal information for other purposes.

Moreover, due to the limited power of enforcement, Australian agencies can only take actions on onshore manufacturers and service providers physically located in Australia [6]. Since most worldwide famous wearable device manufacturers are headquartered in the United States (US), they may not necessarily comply with the APP. The wearable manufacturers may hold personal information, including the users' health data from all over the world, and they only have to comply the US regulations. Particularly for health information in the US, Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates how entities in health care area should be legally used and adequately protected. However, likewise in Australia, the emerging of wearable devices manufacturers are not clearly defined in the current entity categorization [1]. This means the wearable manufacturers are holding and processing the users' personal and health information in a dark-zone out of the regulations, which put users in a high risk of privacy violation.

5 Implications

From the discussion presented above, several implications are drawn in order to determine the most common as described in the following:

– Current regulations cannot effectively restrict the behavior of processing personal and health information by those wearable device manufacturers or third-party application providers.

- Regulations and legislations should be complemented to standardize the personal and health data collecting, storing and processing practices; those wearable companies need to be clearly identified, categorized and regulated into the privacy regulations of each country.
- Data collection should only be approved when it's necessary to devices functions, and when it comes to sensitive data such as health information should only be collected and used under the consent of individuals.
- Referring to the privacy regulations, information holders should also modify their privacy policies and clearly state how personal data will be collected, stored and the possible usage of these data in any conditions.
- Employers who are promoting workplace wearable devices should keep the transparency in all those data related practices. Sound regulations should be developed in each country to monitor the operations in terms of employees' privacy.
- Regulations and legislations are always playing a passive role facing emerging technologies and are far behind of them as it is very hard for regulations and legislations to predict and act proactively before the technologies are born; however, it is still necessary and feasible to reduce the gap between them, relevant government agencies should be more tightly connected to technologies and do more research and analysis.
- Collaboration between agencies and emerging technology companies plays an important role by prioritizing customers' needs and defining clear policies that can be easily adopted along the technology evolves.

6 Conclusions

Wearable industry is growing fast, while privacy issue is a topic that cannot be neglected. Furthermore, the privacy issue might become a big barrier to the adoption of wearable technology for users, as users' awareness on privacy are strengthened and the current condition of wearable devices represents a threat to the users' own privacy.

After the analysis performed in this paper, it is clearly defined that the privacy issue related with wearable technology implemented on all relevant computing devices requires thorough consideration by the wearable technology industry and the regulation parties. Even though the emerging wearable technology are bringing benefits to their lives, privacy protection should not be compromised. Users feel the need to be protected from their information not to being shared or leaked by any entity or third party. Therefore, the wearable manufacturers should take necessary actions to protect the users' privacy and the legislator needs to catch up the pace to regulate both personal and business uses of wearable devices to eliminate the risks of privacy violation within compliance.

References

1. Bromberg, K.H., Cranston, D.A.: Wearable technology: taking privacy issues to heart. New York Law J. (2015)
2. Business Wire: Worldwide Wearable Computing Market Gains Momentum with Shipments Reaching 19.2 Million in 2014 and Climbing to Nearly 112 Million in 2018 (2014), http://www.businesswire.com/news/home/20140410005050/en/Worldwide-Wearable-Computing-Market-Gains-Momentum-Shipments
3. Castillo, M.: Seattle restaurant bans google glass wearers (2013), https://www.cbsnews.com/news/seattle-restaurant-bans-google-glass-wearers
4. CCS Insight: Wearables Market to Be Worth $25 Billion by 2019 (2017), http://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight
5. Cellan-Jones, R.: Office puts chips under staff's skin (2015), http://www.bbc.com/news/technology-31042477
6. Daly, A.: The Law and Ethics of 'Self Quantified' Health Information: An Australian Perspective. Int. Data Priv. Law (2015)
7. Di Pietro, R., Mancini, L.V.: Security and privacy issues of handheld and wearable wireless devices. Commun. ACM **46**(9), 74–79 (2003)
8. Federal Register of Legislation, Australian Government: Privacy act 1988 (2015), https://www.legislation.gov.au/Details/C2015C00279
9. Gartner: Gartner Reveals Top Predictions for IT Organizations and Users for 2016 and Beyond (2015), http://www.gartner.com/newsroom/id/3143718
10. Lloyd, C.: Google Glass Banned at Company's Own Shareholders Meeting (2013), https://goo.gl/JhS2fe
11. Meola, A.: Wearable technology and iot wearable devices. Business Insider (2016), http://www.businessinsider.com/wearable-technology-iot-devices-2016-8
12. Misfit: Privacy policy (2016), http://misfit.com/legal/privacy_policy
13. Ng, C.: 5 Privacy Concerns about Wearable Technology (2015), https://blog.varonis.com/5-privacy-concerns-about-wearable-technology
14. O'Donovan, T., O'Donoghue, J., Sreenan, C., Sammon, D., O'Reilly, P., O'Connor, K.A.: A context aware wireless body area network (ban). In: 3rd International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), pp. 1–8 (2009)
15. Office of the Australian Information Commissioner: Privacy fact sheet 17: Australian Privacy Principles (2014), http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles
16. PwC Health Research Institute: Health wearables: Early days (2014), http://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/pwc-hri-wearable-devices.pdf
17. PwC Health Research Institute: Half of people would use a workplace smartwatch (2016), http://pwc.blogs.com/press_room/2015/04/half-of-people-would-use-a-workplace-smartwatch-pwc-research.html
18. Ranger, S.: Google glass is just the beginning: Invisible cameras and the privacy headaches of tomorrow (2013), http://www.zdnet.com/article/google-glass-is-just-the-beginning-invisible-cameras-and-the-privacy-headaches-of-tomorrow
19. Rao, L.: Sexual Activity Tracked By Fitbit Shows Up In Google Search Results (2011), https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results

20. Sacco, A.: Fitness Trackers are Changing Online Privacy - and It's Time to Pay Attention (2014), https://www.computerworld.com/article/2491195/personal-technology/fitness-trackers-are-changing-online-privacy-and-it-s-time-to-pay-attention.html
21. Shemkus, S.: Fitness trackers are popular among insurers and employers - but is your data safe? The Guardian (2015)
22. Simpson, J.M.: Welcomes Death Of Google Glass, Says Internet Giant Should Not Offer "Glass 2.0" Until Privacy Issues Are Solved (2015), https://goo.gl/hc73te
23. Spicer, A., Cederstrm, C.: What companies should ask before embracing wearables. Harvard Bus. Rev. (2015)
24. Swearingen, J.: How the Camera Doomed Google Glass (2015), https://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570
25. Tehrani, K., Andrew, M.: Wearable technology and wearable devices: Everything you need to know (2014), http://www.wearabledevices.com/what-is-a-wearable-device
26. Tractica: Wearable Devices for Enterprise and Industrial Markets (2016), https://www.tractica.com/research/wearable-devices-for-enterprise-and-industrial-markets
27. Wasik, B.: Why wearable tech will be as big as the smartphone. Wired (2013)
28. Yang, H., Yu, J., Zo, H., Choi, M.: User acceptance of wearable devices: an extended perspective of perceived value. Telematics Inform. **33**(2), 256–269 (2016)