

Discussion of Information Security and Privacy of Wearables for
eHealth Applications

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im
Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen
Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Le



Vorname: Thanh Van



Prüfer: Prof. Dr. M. H. Breitner

Hannover, den 11.08.2017

Table of Contents

Abstract.....	I
List of Figures.....	III
List of Tables	IV
List of Abbreviations	V
1 Introduction.....	1
2 Current State of Research.....	3
2.1 Methodology of Webster and Watson	3
2.2 Identification for relevant Literature	4
2.3 Evaluation of the Literature	5
3 Theoretical Background.....	6
3.1 Wearable Computing Technology	6
3.1.1 Definition of Wearables	7
3.1.2 Classification of Wearables	8
3.1.3 Current Wearable Market Industry	9
3.1.4 Application of Wearables.....	10
3.2 eHealth.....	12
3.2.1 Definition of eHealth	13
3.2.3 The role of eGA	14
3.3 The Quantified Self	14
3.4 Information Security and Privacy Concerns	16
3.4.1 Information Security	16
3.4.2 Privacy	18
3.4.3 Threats and Risks	19
4 Research Methodology	22
4.1 Approach: Technical Research	22
4.2 Approach: Qualitative Content Analysis	23
4.2.1 Selection Process of the Experts	23
4.2.2 Question Catalogue and Intention.....	24
4.3 Approach: Quantitative Survey	25
4.3.1 Question Catalogue and Intention.....	25
5 Results of the Applied Approaches	27
5.1 Results of the Technical Research	27
5.2 Results of the Qualitative Content Analysis.....	29
5.3 Results of the Quantitative Survey	31
6 Discussion	37
6.1 Implementations and Recommendation for Action	41
6.1.1 Implementations for Wearables Users	41
6.1.2 Implementations for Third Parties	41
7 Limitation and Further Research.....	43
8 Conclusion	44
List of References.....	46
Appendix.....	50
Ehrenwörtliche Erklärung.....	72

1 Introduction

As a result of the digitalization the new era of "Internet of Things" is becoming more relevant in the daily life of Humans. The importance of Automation and Networking is expanding from computers, machines and mobile devices to other everyday objects. IoT defines physical everyday objects being connected to the internet and having the ability to communicate with other devices. Thus, leading to objects to be more intelligent, supportive and facilitating humans with their lives. With the rising phenomenon of IoT, a new innovation emerges: Wearable Computing Technology. The Wearable Computing Technology are also known as: Wearables. Wearables are computing devices that are worn by users like an accessory. These are equipped with small sensors, which enable the measurement of different metrics.

Due to current demographic changes in Europe, the health sector, the government and the population need to deal with several consequences. An ageing population leads to a higher demand of accessibility of care and treatments not only in hospitals, however as well as at home. An important keyword in eHealth is the current megatrend "The Quantified Self". Since health is considered as one of the most important and highest good of mankind, hence wearables are starting to play a significant role in the health sector. People are more aware about their health and start to become eager in taking the role of self-managing and monitoring their health. It follows that wearables are especially gaining attention in one specific field: Healthcare.

Wearable devices are seen as hope which provide a breakthrough in improving healthcare by monitoring and preventing diseases. BfDI showed in their recent report that over a third of the German population older than 14 years already use health or fitness trackers, which are also the most known and used wearable devices (see BfDI, 2016, p.1). But aside the exhilaration and expected potentials this paper examines if there are any threats or risks, since these devices constantly gather personal and sensitive data, there may be a possibility of attracting third parties trying to seize the data for their own profit.

The intention of this paper is to discuss the information security and privacy of wearable devices applied in eHealth. Since there is a diversity of wearable devices on the market, this paper concentrates on the most widespread and most sold devices, which are the health and fitness trackers, as well as the smart watches. This work aims to answer the following questions:

Are there any risks and threats concerning user's data and privacy while using health and fitness trackers or smartwatches?

How do wearable users as well as non-users perceive the information security of wearable devices?

Do manufactures, app developers and service providers supply any methods to protect the users' privacy?

How do other actors from the health sector evaluate this trend?

In the second chapter, the current state of research based on the methodology from Webster and Watson regarding this research's topic will be elucidated.

In order to get a theoretical understanding, the third section gives a brief overview on the fundamentals in terms of the research's topic. Hereafter, three research methodologies, which were used for this paper to answer the research questions are outlined in the fourth chapter.

In the main chapter, a thorough discussion of the information security and privacy of wearables focused on the results of the three different applied approaches, information extracted out of papers and studies found in the literature review is given. This chapter is divided in three sections, as it examines this research's topic from three different perspectives: the actual state of security of health and fitness trackers, experts working in the health sector and wearable users and non-users. Lastly, limitations will be presented and a conclusion is drawn.

8 Conclusion

Due to the rapid development of IoT, wearable technology is growing renowned within the population. Wearable devices offer great potentials such as providing real time measured data such as pulse rate, heart rate. However, the usage of wearables unveils different information security and privacy risks, since these devices contain plenty of personal and sensitive information. This paper has investigated the information security and privacy of wearables, which are applied in eHealth. Since health and fitness trackers are the one most sold wearables supported by the quantified-self-movement, this paper has investigated the information security of these devices.

The research method of combining three different approaches, enabled us to draw conclusions considering different perspectives. Based on the literature review several involving risks and threats regarding the privacy of users while using wearable devices to track and monitor its health were identified and highlighted in a technical research. The research in this paper has highlighted, the involving severe risks and vulnerabilities, which need to be considered while using any health or fitness tracker. The identified threats and risks contain not only of on- device risks, but as well as transmission and cloud risks. Therefore, several factors such as the app developers, manufacturers, service providers are asked to ensure the information and data security and lastly the privacy of users. Not only application developers, service providers and manufacturers are playing an important role, however the users need also to be aware to mitigate risks.

The conducted survey has revealed that non-users and wearable users are less aware and concerned of their data. The findings of the survey highlighted that especially wearable users are neither aware of these, but nor do they want that third parties get access to their personal information. To protect the user and their data, it is crucial to identify the reasons for this condition. Possible reasons might be the lack of information and education through sellers, manufacturers, service's provider and privacy policies. The results of this paper indicate that the younger generation might be less worried and concerned about their data. A cause could be due to growing up with the digitalization, being a generation who shares everything with everyone on the social networks and ending up being less sensitive regarding data security and privacy. This assumption needs to be verified in further research.

Third parties such as doctors were interviewed on this research's topic. The response of the experts on wearables applied in the health sector were mixed. On the one hand, several potentials such as a better comprehension between doctor and patients, faster reaction to act for sudden vital changes were mentioned by the experts. On the other hand, skepticism and concerns

regarding the collected data especially information security and privacy of users were expressed. The picture is still incomplete, since several actors need to be considered such as security providers for the eGA or the health insurances.

The results of the conducted survey demonstrated that the eGA is mostly welcomed by the people. In addition, the experts interrogated for this paper, are also looking expectantly at the implementation of the eGA. However, the paper also pointed out several risks concerning the eGA, which is supported by the expert's concern. The eGA has to deal with internal and external risks in foreign countries, where it is already implemented. Since the collected data is high sought after on the black market for identity theft and medical fraud. For the implementation of the eGA in Germany, a legal framework needs to be established to protect the citizens' personal information and guarantee citizen's privacy.