

Contents

List of Figures	v
List of Tables.....	v
List of Abbreviations.....	vi
List of Symbols	vii
1 Introduction	1
1.1 Relevance and Motivation.....	1
1.2 Research Gap and Question	2
2 Theoretical Background	4
2.1 Literature Review	4
2.2 Information Privacy.....	9
2.2.1 Definition	9
2.2.2 Privacy Models & Concerns.....	9
2.2.3 Prediction of Behavioral Intention	13
2.2.4 Privacy Legislation.....	14
2.3 Smart Home.....	15
2.3.1 Definition	15
2.3.2 Smart Home Services	16
2.3.3 Smart Home Technologies	19
3 Research Model and Hypotheses	22
3.1 Relationship between the Privacy Model, TAM & TPB.....	22
3.2 Covariates.....	28
4 Research Design and Methodology.....	29
4.1 Qualitative Research (Expert Interviews)	29
4.1.1 Operationalization of interviews	29
4.1.2 Methodology	31
4.1.3 Results	32
4.1.4 Conclusions for the proposed Research Model.....	38
5 Quantitative research (SEM)	41
5.1 Survey design and Sample	41
5.2 Measurement and Instrumentation	43

6	Data Analysis and Results	47
6.1	Overall Model.....	47
6.1.1	Measurement Model Assessment.....	48
6.1.2	Structural Model Assessment.....	51
6.1.3	Hypotheses Testing	55
6.2	Multi-Group Analysis	59
7	Discussion and Recommendations	63
8	Limitations & Future Research	70
9	Conclusion	72
	References	I
	Appendix	XII
	Declaration of Authorship	XCI

1 Introduction

1.1 Relevance and Motivation

*“If you want to keep a secret, you must also hide it from yourself.”
- George Orwell*

The fusion of the physical and digital world in the Internet of Things has significant effects on the design of residential spaces. Appliances in the home are not longer operated separately and locally. Increasingly, domestic appliances are mutually connected via information and communication technology, resulting in the emergence of smart homes. Sensors, network connections and applications build a dynamic architecture aiming at increasing efficiency of everyday tasks and improving safety of homes and the people living in them (Geneiatakis, 2017). Many studies predict an exponentially rising importance for smart home environments with the potential to become an essential installation in housing environments (Ghaffarian Hoseini et al., 2013; Kim et al., 2017). The diffusion of mobile networks and the growing popularity of smart devices lead to rapid growth of the business segment. While the global market for smart home services was estimated at \$24.39 billion in 2016, it is forecasted to increase up to \$119.01 billion until 2022. By that time, the global market penetration is expected to be 19.5% (Statista, 2018). This is as well caused by global high-tech companies like Google and Amazon, who have commercialized smart home products and services and have thus become drivers of the trend. Despite the positive prospects for the spread of the technology in the future, smart home devices have not yet been widely adopted (Yang et al., 2017). An important reason may be the still very fragmented market, where many technologies are not yet mature and standardization is not yet in place to ensure interoperability between different manufacturers. Nevertheless, a major obstacle to adoption is the nature of the technology that gives rise to new concerns about information privacy (Bugeja et al., 2016). Smart home devices make use of various sensing technologies to provide services. These sensors collect vast amounts of data, which are processed and analyzed to provide a service to the users. This collection of personal data in combination with the increasing deployment of internet-connected devices in the home exposes residents to new privacy and security risks. According to a survey by YouGov (2017), 88% of Germans consider the security risks associated with the use of smart home devices to be critical. According to this, privacy concerns could represent a potential barrier to the adoption of smart home devices. Consequently, the influences of users' privacy concerns should be part of empirical research and are therefore the objective of this scientific work. For this purpose, the present work aims to identify relevant privacy concerns of potential users in connection with the use of smart home devices and

to investigate whether these have a significant influence on the acceptance of this particular technology.

In this regard, the following section highlights the research gap and formulates the central research questions of this work.

1.2 Research Gap and Question

While studies on user acceptance and on the behaviour of potential customers are of great importance for successful acceptance and diffusion in the market, little research has been done on this topic. Rather, the majority of scientific work in the context of smart home has a technological background (Reinisch et al., 2011). Technical threats to privacy and data security have often been presented in scientific papers. However, users' worries resulting from these dangers and their influence on technology acceptance remained largely unconsidered. Especially the construct of privacy concerns has not yet been part of scientific research on this topic. Consequently, influences of the diffusion and adoption of smart home technologies have not been adequately addressed. This study at hand seeks to get a deeper insight into the adoption of smart devices in households against the background of information privacy concerns. Consequently, this thesis aims to provide deeper insight into the issue by answering the following research question:

RQ: To what extent do users' concerns for information privacy influence the intention to use smart home devices?

In order to answer this research question, chapter 2 of this thesis at hand provides the theoretical background to the topic. This consists of a systematic literature review, which identifies the most important privacy concerns for the application to smart home devices and instruments for measuring information privacy concerns and user acceptance. In addition, this section contains definitions and descriptions of the most important issues identified within this analysis. Chapter 3 subsequently deals with the proposition of a research model. Moreover, hypotheses are formulated, which represent the relationships between the individual variables of the model. In chapter 4, the research design and methodology of the conducted qualitative and quantitative analysis are illustrated. Furthermore, the proposed research model is evaluated and modified according to the results of the seven expert interviews conducted. In Chapter 5, the results of the applied structural equation modeling are presented and the hypotheses are evaluated to determine whether they are supported. Chapter 6 then deals with the discussion of the results. On the one hand, the findings are evaluated with regard to their significance for the individual hypotheses. On the other hand, a comparison is made with the findings of the expert interviews in order to compare the theoretical findings with practical experience.

Moreover, this chapter contains recommendations for suppliers of smart home devices. Chapter 7 then presents limitations of the present work and makes recommendations for future research. The work concludes in chapter 8 with a summary of the results and the presentation of theoretical and managerial implications.

9 Conclusion

The purpose of this thesis was to assess the influence of privacy concerns on the acceptance of smart home devices by potential consumers. For this purpose, a literature review was conducted in the first step of this work. By means of a structured analysis of the current research, relevant privacy concerns and acceptance models for the context smart home were identified. Subsequently, a research model was set up on the basis of the findings of the literature analysis and conducted expert interviews. Secondary use of information, perceived surveillance, perceived intrusion and awareness of privacy practices were identified as essential elements for representing information privacy concerns. In addition, the elements of the TAM and TPB were integrated into the model as mediating variables for behavioral intention. In a next step, the validity of the model was examined using an online survey. By evaluating and discussing the results of the quantitative analysis and comparing them with the findings of the expert interviews, targeted conclusions could be drawn for the effects found.

This paper makes several contributions to the theory. Firstly, this study is the first to address the influence of privacy concerns on the acceptance of smart home devices. Therefore, the insights gained set an important basis for further research in this domain. Secondly, the evaluation of results shows that the developed research model is a meaningful instrument for the investigation of user concerns' influence regarding information privacy on behavioral intention. The empirical results have proven a good explanatory power for the proposed research model. Especially the individuals' perceptions with regard to attitude, subjective norm and perceived behavioral control have been identified to play a decisive role for the acceptance of the technology. Consequently, this model can be used by future research to investigate the user acceptance of certain smart home services or devices.

On the other hand, this study provides useful managerial implications for decision-making of smart home device manufacturers. The present work elaborated the influence of different variables on the decision to use smart home technology. Having empirically proven the relevance of these factors, they can now be targeted by the industry to increase adoption rates. The realization that privacy concerns have no direct influence on the decision to use smart devices in the home is of great importance to industry. This allows resources to be focused on addressing the key factors of decision making directly, namely attitude, subjective norm and perceived behavioral control. Besides, differences between groups with various demographic characteristics were identified. Based on these insights into different groups in society, smart device vendors can focus their development and sales efforts on the needs and concerns of these potential customers.