



**LUND UNIVERSITY**

School of Economics and Management

*Department of Informatics*

---

**Willingness to Disclose Sensitive  
Information for Underwriting Purposes  
Wearable Devices in Life and Health Insurance**

Master thesis 15 HEC, course INFM10 in Information Systems  
Presented in June 2016

Authors: Ali Chehab  
Annina Oelschläger

Supervisor: Styliani Zafeiropoulou

Examiners: Björn Johansson  
Miranda Kajtazi

# **Willingness to Disclose Sensitive Information for Underwriting Purposes**

## **Wearable Devices in Life and Health Insurance**

Authors: Ali Chehab and Annina Oelschläger

Publisher: Dept. of Informatics, Lund University School of Economics and Management.

Document: Master Thesis

Number of pages: 76

Keywords: Big Data, information disclosure, wearable devices, health and life insurance, information privacy, privacy calculus, privacy paradox, perceived risks, perceived benefits.

Abstract:

The rise of Big Data is creating tremendous opportunities across all industries. As the development promises disruptive changes of business processes and manifold benefits both on the company and customer side, health and life insurance companies engage and invest in Big Data approaches. By collecting, storing, and analysing huge amounts of customer centric data, they hope to enhance their risk assessment, prevent insurance fraud, to operate more efficiently and ultimately to gain a competitive advantage. Therefore, new insurance policies rely on the adoption of wearable devices which measure fitness achievements and health related values, providing the insurer with valuable information and at the same time giving the customer the opportunity to influence the insurance premium and earn other rewards.

Despite some benefits, this approach evokes major privacy concerns and the fear of potential negative consequences amongst current and potential customers. Our study shows that both aspects, perceived benefits and perceived risks, are affecting the willingness to disclose information as individuals engage in a risk-benefit analysis which is additionally influenced by the level of trust in the insurance company and individual customer characteristics.

Building on a profound theoretical background, including established theories like the privacy paradox and the privacy calculus, and on a qualitative study, comprising nine semi-structured interviews and a thoroughly conducted analysis, we develop and present a research model which clearly identifies and explains all factors influencing the willingness to disclose sensitive information collected by wearable devices to health or life insurance companies.

## Content

1	Introduction .....	1
1.1	Background .....	1
1.2	Problem Area .....	2
1.3	Motivation .....	3
1.4	Purpose and Research Question .....	4
1.5	Delimitation .....	4
1.6	Outline .....	5
2	Basic Concepts and Definitions .....	6
2.1	Big Data, Internet of Things, and Wearables .....	6
2.1.1	Big Data .....	6
2.1.2	Internet of Things .....	7
2.1.3	Wearable Devices .....	8
2.2	Information Privacy and Security .....	9
2.3	The Insurance Industry .....	9
2.3.1	Adverse Selection .....	10
2.3.2	Moral Hazard .....	11
2.4	Big Data in the Insurance Industry .....	11
2.4.1	Life and Health Insurance .....	11
3	Theoretical Background .....	13
3.1	Willingness to Disclose Personal Information .....	13
3.1.1	Information Disclosure in an E-Commerce Context .....	13
3.1.2	Information Disclosure in a Health Information Context .....	15
3.2	Information Privacy and Related Theory .....	17
3.2.1	Privacy Paradox .....	17
3.2.2	Privacy Calculus .....	18
3.2.3	Other Remarks on Information Privacy .....	19
3.3	Wearable Devices .....	19
3.3.1	Adoption and Acceptance of Wearable Devices .....	21
3.3.2	Privacy and Security Concerns .....	22
3.4	Disclosing Health Information to Insurance Companies .....	23
3.5	Research Model .....	25
3.5.1	Perceived Risks .....	26
3.5.2	Perceived Benefits .....	29

3.5.3	Moderators .....	32
4	Methodology.....	34
4.1	Research Strategy.....	34
4.1.1	Purpose of Research.....	34
4.1.2	Research Philosophy.....	35
4.1.3	Research Method and Approach.....	35
4.2	Data Collection and Analysis.....	37
4.2.1	Thematizing .....	38
4.2.2	Designing .....	38
4.2.3	Interviewing .....	41
4.2.4	Transcribing .....	43
4.2.5	Analyzing.....	44
4.2.6	Verifying and Reporting .....	46
4.3	Research Quality.....	46
4.3.1	Credibility .....	46
4.3.2	Transferability.....	47
4.3.3	Dependability .....	47
4.3.4	Confirmability.....	47
4.3.5	Ethics.....	48
5	Data Analysis and Empirical Findings .....	50
5.1	Public Opinion and General Attitude.....	50
5.2	Perceived Risks.....	51
5.2.1	Invasion of Privacy .....	52
5.2.2	Data Accuracy.....	52
5.2.3	Manipulation .....	53
5.2.4	Secondary Use .....	53
5.2.5	Discrimination.....	54
5.2.6	Security Concerns .....	55
5.3	Perceived Benefits .....	56
5.3.1	Financial Benefits .....	56
5.3.2	Receiving a Fitness Tracker.....	57
5.3.3	Health Motivation .....	57
5.3.4	Increased Fairness.....	58
5.3.5	Social Image.....	59
5.3.6	Improved Services .....	59
5.4	Moderators .....	60

---

5.4.1	Trustworthiness of Insurance Company .....	60
5.4.2	Customer Characteristics .....	61
5.5	Willingness to Disclose Information .....	61
5.6	Other Remarks .....	62
6	Discussion.....	63
6.1	Willingness to Disclose, Privacy Paradox and Privacy Calculus .....	63
6.2	Perceived Risks .....	65
6.2.1	Invasion of Privacy .....	65
6.2.2	Data Accuracy.....	66
6.2.3	Manipulation .....	66
6.2.4	Secondary Use .....	67
6.2.5	Discrimination.....	67
6.2.6	Security Concerns .....	67
6.3	Perceived Benefits .....	68
6.3.1	Financial Benefits .....	68
6.3.2	Receiving a Fitness Tracker.....	69
6.3.3	Health Motivation .....	69
6.3.4	Increased Fairness .....	70
6.3.5	Social Image.....	70
6.3.6	Improved Services .....	71
6.4	Moderators .....	71
6.4.1	Trustworthiness of Insurance Company .....	71
6.4.2	Customer Characteristics .....	72
6.5	Revised Research Model.....	73
7	Conclusion.....	74
7.1	Summary and Main Findings.....	74
7.2	Theoretical and Practical Implications.....	75
7.3	Limitations and Future Research .....	76
Appendix 1	.....	77
Appendix 2	.....	79
Appendix 3	.....	85
Appendix 4	.....	87
Appendix 5	.....	90
Appendix 6	.....	92
References	.....	135

---

## Figures

Figure 3.1: Preliminary research model.....	25
Figure 4.1: Research approach.....	36
Figure 4.2: Seven stages of an interview inquiry (according to (Kvale, 2007)).....	38
Figure 4.3: Example of colour coding .....	45
Figure 6.1: Revised research model.....	73

---

## Tables

Table 3.1: Considered research in the field of information disclosure (e-commerce).....	14
Table 3.2: Considered research in the field of information disclosure (health information)....	15
Table 3.3: Additionally considered research in the field of information privacy .....	17
Table 3.4: Considered research in the field of wearable devices.....	20
Table 3.5: Considered research in the field of disclosing health information to insurers .....	23
Table 4.1: Overview of the interview questions .....	40
Table 4.2: Key characteristics of respondents .....	42
Table 4.3: Overview of interviews.....	43
Table 4.4: Coding scheme.....	46
Table 5.1: Perceived risks mentioned by respondents without interviewer interference .....	51
Table 5.2: Perceived benefits mentioned by respondents without interviewer interference ....	56
Table 5.3: Willingness to disclose sensitive information to insurance companies.....	62

# 1 Introduction

This introductory chapter provides a short and precise opening to this thesis. It comprises an outline of the background and summarizes the problem area of the studied phenomenon. Furthermore, the choice of the research field is motivated and the purpose of the inquiry is stated alongside the research question. Additionally, a delimitation to other research areas is given, before presenting the structure of the remaining publication.

## 1.1 Background

In recent years, the technological advancement has significantly increased the ability to collect, store, and analyse vast amounts of data. The growing dissemination of sensors in all kinds of devices and appliances, a dramatic decrease in storage cost, incremented processing power, and innovations in machine learning fuel this development (Washington, 2016). Summarized under the term 'Big Data', the large amount of collected information and the advanced analytics which are deployed to make sense out of it, promise manifold benefits and create new opportunities across all industries (Chen, Chiang, & Storey, 2012). Smart cities, data-driven manufacturing, customized advertisement on social media, or individually tailored offers, are just a few examples of how companies, organizations and governments try to leverage Big Data for their business goals or other endeavours. All of these diverse applications aim for improvements in terms of efficiency, effectiveness, and quality, as well as for major cost reductions (Chen et al., 2012). Businesses and institutions who excel in Big Data analytics are capable of creating an important competitive advantage (Davenport, 2006).

Consequently, the rise of Big Data is also affecting the insurance industry. Just like in any other area of business, insurers are hoping to benefit from the arising opportunities and according to insiders, disruptive changes in how business is conducted in the insurance industry can be expected (Economist, 2015). As insurers always relied on customer data in order to perform risk assessments and to develop predictive models, it can be said that data is the backbone of the business. Consequently, the great interest in Big Data is perfectly logical. While in the past, decisions were dependent on the statements made by the policyholders themselves which could often not be verified, today other possibilities for data collection are available (Vaia, Carmel, DeLone, Trautsch, & Menichetti, 2012). The uncertainty of future events, lying at the core of the insurance business, is met with an increasing reliance on data. Prospects of enhanced marketing and insurance fraud detection further encourage the desire for more customer centred information.

Following this reasoning, insurance companies increasingly invest in data-driven approaches and, dependent on the specific type of insurance, try to find appropriate sources and means for data collection as well as analysis. While auto insurances for example install black boxes in vehicles to record accurate driving profiles of individual customers, home insurers connect their services to smart home appliances in order to improve their decision making.

In life and health insurance the means of choice for collecting more precise, more timely, and greater amounts of information are wearable devices (Olson, 2014). By tracking fitness achievements and other health related values, the insurers have access to valuable real-time data allowing for an accurate evaluation of their customers' health status and lifestyle choices (Christophersen, Mørck, Langhoff, & Bjørn, 2015). Building on this acquired knowledge, insurance premiums and services can be tailored to individual particularities and needs. Instead of paying a once determined, fixed amount of money per year, insurance premiums are constantly re-evaluated, accounting for the specific risk shifted to the insurance fund. Additionally, the approach aims at changing the behaviour of policyholders towards a healthier way of living by rewarding fitness efforts.

While the insurance companies hope to profit from an improved risk assessment, to be able to prevent moral hazard and insurance fraud, and consequently to operate more efficiently, the approach also potentially yields benefits and advantages for customers. Value is created in terms of customization with opportunities for financial savings and improved services. Thus, at first glance, the adoption of wearable devices for underwriting purposes seems to be a win-win situation for both parties, health and life insurance companies as well as customers.

## 1.2 Problem Area

Despite these manifold opportunities and expected benefits of Big Data approaches in the insurance industry, the development is accompanied by major concerns and criticism. From a customer perspective, potential downsides and the inherent trade-off become very obvious. In order to benefit from the new policies, customers have to reveal a great amount of sensitive information, granting insights into their private lives and, to a certain degree, give up or sacrifice control over their data. Questions arise concerning who has access to the data, if the transmission and storage of the data is secure, and how exactly the information will be used.

These widely spread privacy and security concerns, which have been acknowledged in public opinion polls (Westin, 2001), are a common cause for discussion in all Big Data related fields of inquiry. However, an extensive, critical media coverage indicates that the apprehension in the context of health related data given to private organisations is especially severe (Economist, 2015; Marr, 2015; Olson, 2014). The concern for private insurance companies having access to health information of a very sensitive nature, seems to be unsettling and the idea of constantly tracking customers with wearable devices evokes thoughts of surveillance scenarios in which private companies are influencing and controlling individual lifestyle choices (Zeh, 2014). Fears are expressed that while 'Big Brother' is watching, people become manipulable and their freedom is threatened (Boyd & Crawford, 2012).

However, despite major criticism and discussion in the media, the new data-driven insurance policies are already offered in various countries and customers are choosing this form of insurance over traditional policies (Olson, 2014). Thus, the willingness to disclose information and ultimately the decision whether to buy such an insurance plan seems to be influenced by more than just the privacy concerns. A comparable paradoxical observation can be made in the e-commerce context, where people also voice immense privacy concerns, but still increasingly conduct their shopping online, indicating that the benefits are overruling the initially perceived risks (Phelps, Nowak, & Ferrell, 2000). Quite obviously, "individuals make choices

in which they surrender a certain degree of privacy in exchange for outcomes that are perceived to be worth the risk of information disclosure” (Dinev & Hart, 2006, p. 61).

As the main source for worry and point of criticism in the context of insurance policies linked to wearable devices is the revelation of private information, one main question arises: What specifically makes customers reveal their information, or in other words, what factors influence the willingness to disclose sensitive information to health or life insurance companies?

The customers’ willingness to disclose sensitive information to insurers not only reflects the societal acceptance of the new insurance model, but also forms a prerequisite for the data-driven policies to become a success and to further disseminate.

### 1.3 Motivation

The rapid development and advancement of Big Data applications has led to massive changes not only in how business is conducted but also on a societal level, especially when it comes to privacy perceptions (van Rijmenam, 2016). Given the broad and severe implications for individuals or the society and the fact that decisions about the dealing with Big Data taken today might determine what our future will look like, the heightened need for extensive research is justified. The assessment of the consequences, especially in the areas of major concern, including moral and ethical issues such as information privacy, demands thorough examination. But while general information privacy issues have attracted a fair amount of research attention in the past (Smith, Dinev, & Xu, 2011) and have been studied extensively in the context of e-commerce (Dinev & Hart, 2006), other new and emerging applications of data-driven approaches have not yet been considered to a great extent.

The adoption of wearable devices to collect information for underwriting purposes of health and life insurance companies, has a strong presence in the media and is a highly controversial topic. As more and more insurance companies introduce respective programs and alter their business practices, the expected benefits but also the potential dangers and negative implications are extensively discussed. Due to the sensitive nature of the health related data and the severe consequences of possible misuse or inappropriate handling of the data (Bansal, Zahedi, & Gefen, 2010), the importance of ethical and moral issues becomes even clearer. Despite this topicality and relevance, the research community failed to keep up with this development and to cover the issue adequately. A significant research gap exists in the context of information disclosure, wearable devices, and health and life insurance companies. Thus, no systematic research is available which examines this specific phenomenon which lies at the heart of information systems research. The technology for data collection and transmission, the wearable device, has been considered, the business processes of insurance companies have been explored, and the customer concerns in the context of privacy have been investigated. Still, an integrated approach towards this topic is missing. It is not clear what the general opinion towards data-driven health or life insurance policies is, how customers feel about disclosing private information to insurance companies, or what specifically makes them reveal their data despite major criticism.

This lack of research, the broad implications for individuals and society, the deep concerns and the topicality of the phenomenon on hand, impressively highlight the importance of research which takes a customer perspective and refers to the willingness to disclose sensitive information collected by wearable devices to health or life insurance companies.

## 1.4 Purpose and Research Question

Consequently, the goal of this research is to explore under which circumstances people are willing to disclose their personal sensitive information to health or life insurance companies, or more precisely, determine which factors have an influence on the decision whether to reveal health information or not. Moreover, we want to assess the public opinion and general attitude towards the use of health data collected by wearable devices for underwriting purposes. As information disclosure can be seen as the main impediment for buying data-based insurance policies, we are also investigating the customer acceptance and expected adoption of the new insurance offers.

Therefore, the specific objective and knowledge contribution of this study is to develop a comprehensive research model which contains all factors influencing the willingness to disclose health information, with implications for the insurance companies, policymakers and future research.

For this purpose, the following research question was developed:

*What factors influence the willingness of customers to disclose sensitive, personal information collected by wearable devices to health or life insurance companies?*

## 1.5 Delimitation

The advent of Big Data and the adoption of data-driven approaches in the insurance industry have raised many questions and opened up new research directions. Due to the limited scope of this work, it is therefore necessary to delimit our study to a specific type of insurance and to a particular perspective. We chose to approach the topic of Big Data in the insurance industry with a customer focus. As outlined in Section 1.3, a significant research gap and concerns about risks for individuals and society, especially in the context of sensitive health information, justify this research focus. Consequently, the reasons and the potential benefits for insurance companies to engage and invest in this new development will not be considered in detail. Likewise, it will not be of interest, if the new insurance policies and ways of data collection actually have a positive effect on the risk assessment and ultimately on the efficiency and effectivity of the companies. Moreover, the often mentioned intention of changing the customer behaviour towards a healthier lifestyle or risk-averse attitude is not examined. Technical aspects like the collection, transmission, storage, and mining of data are as well out of the scope of this work. Additionally, the legal framework and thereby the feasibility of an adoption of Big Data approaches in the insurance context in different countries is excluded from the study. This decision was taken in order to reduce the complexity of our research and is based on the assumption that, even if the described scenario might be unrealistic in a specific country, for example in Sweden where the insurance is state provided, the individual willingness to disclose information in a hypothetical scenario can still be assessed.

All of these mentioned, manifold and interesting issues can be attributed to the company side of the phenomenon and are out of the scope of our study, thus left for future research.

Consequently, the study on hand and the proposed model specifically investigate and explain the factors influencing the customers' willingness to disclose health information collected by wearable devices to health or life insurance companies.

## 1.6 Outline

The remaining part of the work is structured as follows: in Chapter 2 basic concepts and definitions, relevant for the understanding of the context this work is rooted in, are given. Chapter 3 contains an extensive literature review constituting the theoretical background on the grounds of which our preliminary research model is developed. The methodological approach is outlined in Chapter 4, followed by a detailed analysis of the collected data and presentation of the findings in Chapter 5. These findings and their relation to and implications for our research model as well as previous research are discussed in Chapter 6, before the work is concluded with a summary, the main contributions, implications, limitations and an outlook to future research in Chapter 7.

## 2 Basic Concepts and Definitions

A lot of different areas of research and fields of interest come into play when examining the willingness to disclose information in the context of life or health insurance companies which adopt wearable devices for underwriting purposes. Technical prerequisites, privacy concerns, and the business practice of insurance companies have to be considered. In this chapter these basic concepts necessary for the understanding of the rest of the thesis are introduced, explained, and illustrated with some examples.

### 2.1 Big Data, Internet of Things, and Wearables

The concepts and paradigms of Big Data, the Internet of Things (IoT), and wearable devices constitute the technical prerequisites and the foundation which make the current development towards increased reliance on collected, personal data in the insurance industry possible.

#### 2.1.1 *Big Data*

In recent years the concept of ‘Big Data’ has gained more and more attention and popularity among practitioners, researchers and the media (Chen et al., 2012; De Mauro, Greco, & Grimaldi, 2015). A lot of scientific publications have been issued in the field and even more magazine articles and blog posts discuss the arising opportunities, implications, and limitations accompanying the advancement of the technology. Despite the lack of a commonly accepted definition (De Mauro et al., 2015; Gandomi & Haider, 2015; Labrinidis & Jagadish, 2012; Ward & Barker, 2013), there is consensus about the great potential this new technology entails and the massive impact it will have on individuals, corporations and society (Chen et al., 2012; Mayer-Schönberger & Cukier, 2013). The often cited “three Vs”: volume, velocity, and variety, sometimes complemented by a fourth V: veracity (Zikopoulos, Parasuraman, Deutsch, Giles, & Corrigan, 2012), describe the key attributes of this new kind of data which “promises to solve virtually any problem” (Marcus & Davis, 2014).

Consequently, collecting large and complex data sets in real time and performing advanced or predictive analytics over it, has become a source of competitive advantage in all industries (Davenport, 2006). Various different appliances and applications like social media sites, mobile phones, and digital devices in the context of the Internet of Things, produce data points constantly, in real time and contribute to the immense data volume. Companies which are able to make use of this data and excel in adopting Big Data analytics are one step ahead of their contestants (Davenport, 2006).

The ultimate goal of new technologies in the realm of Big Data is to facilitate and improve decision making, leading to faster and better decisions which in turn give rise to greater efficiency, reduced costs and risk on various levels (Chen et al., 2012).

Hence, companies in every industry (also non-profits and governments) implement Big Data projects and try to leverage the opportunities of those massive amounts of data (Chen et al., 2012). For example, corporations try to better understand customers and their behaviours in order to predict what might appeal to them and to customize offers. Additionally, they are able to filter attitudes and sentiments towards a specific brand or a product over social media, allowing them to adjust marketing efforts or product features. Other applications can be found in the sports world where the success story of the Oakland A's, as published in "Moneyball" by Lewis (2004), proved that data and algorithms are the better talent scouts. Delivery route optimization, fraud detection or more thrilling: predictive policing, are just a few more examples of how Big Data can create benefits and value in various different areas. Big Data is believed to make life easier and more convenient in various ways.

Despite this "strong celebratory thread in the literature on Big Data" (Crawford, Gray, & Miltner, 2014, p. 1666), it has to be said that the arising advantages and opportunities of the Big Data phenomenon, highlighted through "anecdotes and success stories" (De Mauro et al., 2015, p. 100), are accompanied by significant challenges. Boyd and Crawford (2012), for example, advise caution and state that "claims of objectivity and accuracy are misleading" (p. 666). "Big Data is still subjective" (Boyd & Crawford, 2012, p. 667), therefore "subject to limitation and bias" (Boyd & Crawford, 2012, p. 668). Problems of data errors, spurious correlations and how limited access could create new digital divides have to be critically examined. Additionally, moral and ethical concerns, especially major privacy issues (Boyd & Crawford, 2012; Tene & Polonetsky, 2012) have to be considered. According to Boyd and Crawford (2012), "very little is understood about the ethical implications underpinning the Big Data phenomenon" (p. 672) and it is time "to question the assumptions embedded in Big Data" (p. 665). Big Data is potentially "enabling invasions of privacy, decreased civil freedoms, and increased state and corporate control" (Boyd & Crawford, 2012, p. 664). Fears concerning "profiling, discrimination, exclusion, and loss of control" (Tene & Polonetsky, 2012, p. 65) are expressed in the context of the new technology and its applications.

Consequently, while undoubtedly there are tremendous opportunities arising with the occurrence and advancement of Big Data, it should still be examined critically as it also comes with major limitations and yet unsolved issues (Marr, 2015).

### *2.1.2 Internet of Things*

Big Data is strongly related to other concepts such as the so-called Internet of Things (IoT). The Internet of Things is a "novel paradigm" (Atzori, Iera, & Morabito, 2010, p. 2787) which describes how physical objects connect to each other and to the Internet, exchange data which they collected and communicate with each other (Atzori et al., 2010). "The embedding of electronics [software, sensors and connectivity] into everyday physical objects" (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012, p. 1497) will make them "seamlessly integrate within the global resulting cyberphysical infrastructure" (Miorandi et al., 2012, p. 1497). Consequently, information is generated and made available to a great extent and thus, IoT forms the "fundamental reasons for [the] Big Data phenomenon to exist" (De Mauro et al., 2015, p. 98). The US National Intelligence Council describes IoT as one of the "disruptive civil technologies" and forecasts that "by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more" (Council, 2008). Scenarios in which an approaching car is communicating with the owner's house, its lighting and heating systems, signalling the upcoming arrival in order to turn the respective systems on, is no longer far fetched.

Consequently, these connected things “promise important efficiency, social, and individual benefits” (Peppet, 2014, p. 89), and the development is believed to have a “high impact [...] on several aspects of everyday-life and behaviour of potential users” (Atzori et al., 2010, p. 2787). Possible applications can be found in several domains, such as personal and home, enterprise, utilities, and mobile (Gubbi, Buyya, Marusic, & Palaniswami, 2013). They include for example the control of home equipment, assisted driving or environment monitoring. Despite these great opportunities and the accompanying enthusiasm, the technological advancement does, just as the phenomenon of Big Data, come with challenges and concerns. A lack of standardization is often discussed (Atzori et al., 2010; Miorandi et al., 2012) and security and privacy risks are a major field of interest as well (Atzori et al., 2010; Mayer, 2009; Medaglia & Serbanati, 2010; Miorandi et al., 2012; Weber, 2010). According to Mayer (2009) “the protection of data and privacy of users is one of the key challenges in the Internet of Things” (p. 1).

### 2.1.3 *Wearable Devices*

An integral component or a subset of IoT is the wearable (Britton, n.d.). Wearable devices, as the name indicates, “can be directly worn on the body” (Gao, Li, & Luo, 2015, p. 1704) and “are attracting much attention as the next generation of portable electronics” (Yang, Yu, Zo, & Choi, 2016, p. 256). “The market is predicted to grow” (Gao et al., 2015, p. 1704) and according to Mason (2014), it will generate \$22.9 billion in revenue in 2020, indicating a growth of 50 percent between the years of 2014 and 2020. “Wearable computers are always on and accessible” and they are believed to “become more intimately connected to our daily lives” (Billinghurst & Starner, 1999, p. 57). Amongst those wearable devices which are equipped with practical functions and features, are smart clothing, smart glasses, smart watches, and smart bracelets or wristbands, also called fitness trackers. Popular examples include Google Glass, Apple Watch, and various fitness trackers like Fitbit, Jawbone UP or Garmin.

While most wearables are perceived by the general public as “fashionable accessories” (Gao et al., 2015, p. 1704) and have not reached the mainstream yet, fitness trackers are increasingly used in a more serious context, for example in healthcare (Gao et al., 2015). With their ability to monitor and track all kinds of fitness- and health-related metrics 24 hours a day, they are perfectly suited for providing important data not only to their owners, but also to other stakeholders. Therefore, the information is wirelessly send to a computer or smartphone for long-term data tracking or data analysis. Metrics include, amongst others, the number of steps taken or distance walked or run, calories consumed, the heart rate, body temperature, and quality of sleep (Chan, Estève, Fourniols, Escriba, & Campo, 2012).

Tracking the health and fitness status in real time is not only interesting for individuals involved in self-monitoring looking to improve their lives, often called the ‘quantified self’ movement (Bottles, 2012; Swan, 2013), but is also increasingly valued by corporations and governments, as more and more possible use cases of the data are discovered.

As wearable devices are a subset of IoT which in turn is a foundation for the Big Data phenomenon, it is no surprise that their increasing dissemination is inducing discussions in the field of information privacy and security as well (Britton; Di Pietro & Mancini, 2003).

## 2.2 Information Privacy and Security

As outlined above, the advent of Big Data, IoT, and wearable devices is accompanied by major privacy and security concerns. Public opinion polls, not only in the U.S. but all over the world, show that individual consumers are highly worried about their personal privacy (Dinev & Hart, 2006; Phelps et al., 2000; Smith et al., 2011) and consequently these issues can be described as a key challenge and restraint when it comes to the wider dissemination of new technologies and their applications. Privacy and security matters also play an important role in the context of information disclosure to private companies and are therefore of great importance for our study.

“Privacy has been studied for more than 100 years” (Dinev, Xu, Smith, & Hart, 2013, p. 295), in various fields of social science, but despite a widespread interest, there is “disagreement among scholars on what privacy is” (Dinev et al., 2013, p. 295). No single agreed on definition of privacy exists (Phelps et al., 2000; Smith et al., 2011). While in 1890, Warren and Brandeis (1890) for example refer to it as “the right to be left alone” (p. 195), Smith et al. (2011) give a more detailed overview of various other perspectives and definitions for the concept. The narrower notion of information or data privacy, which is of relevance in this study, was defined by Van Dijk (2012) as “the right to selective disclosure”. He states that “information privacy is about the grip the individual has and keeps over his or her personal data and over the information or decisions based on these data” (Van Dijk, 2012, p. 122). A similar, control-oriented definition of information privacy can be found in Westin (1967) or by Stone, Gueutal, Gardner, and McClure (1983) who phrased it as: “the ability of the individual to control personally information about one's self” (p. 460). With the increasing collection, storage, and usage of personally identifiable, or sensitive information by companies in all industries, many people feel that their privacy is invaded.

The concept of information privacy has to be distinguished and clearly delineated from data security which is defined as the protection against threats such as “destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse” (Belanger, Hiller, & Smith, 2002, p. 249). These threats “can be made either through network and data transaction attacks, or through unauthorized access by means of false or defective authentication” (Belanger et al., 2002, p. 249). Therefore, “security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of [...] disclosure, or to reassure users” (Ackerman, 2004, p. 433).

These issues obviously demand a legal and political framework, but they also raise questions about ethics and morality as “general privacy beliefs are integrated in the moral value system of the society” (Smith et al., 2011, p. 991).

## 2.3 The Insurance Industry

While it is out of the scope of this thesis to describe all mechanisms and the nature of the insurance industry in detail, it is still relevant to outline and understand the basic concepts, underlying dynamics, and biggest challenges in this business field. These aspects provide the background for the study on hand and motivate why insurance companies adopt Big Data approaches in the first place. The embracement of wearable devices for underwriting purposes

in the life and health insurance industry is a logical consequence of the technological advancement and the nature of the challenges in the insurance operations.

In general, insurance is a means to protect individuals or other entities from financial loss. In order to hedge the risk of a contingent, uncertain loss in the future, a person or entity buys an insurance policy from an insurer, accepting a known relatively small loss in form of the paid price, the insurance premium. The insurance policy thereby forms a contract between the insurance company and the policyholder, stating that in exchange for the premium paid, the insurer has to compensate the insured in case of a covered loss. The contract specifically determines which claims the insurance company is legally required to pay. In summary, the insured hedges the risk of an uncertain loss in the future against a relatively small, certain loss in the present.

Therefore, it can be said that the insurance business model “works on the principle of risk” (Marr, 2015). A person's “individual risk [...] is insured by an insurance company. The primary insurer takes on the risk for a premium (calculated on the individual's risk group) and is liable in the event of loss” (Müller & Zimmermann, 2003, p. 4). As ‘underwriting’ specifically describes the process insurance companies involve in, in order to assess and select the risks to insure, and decide about insurance pricing, it can be said that “underwriting is the core of insurance business” (Manral, 2015, p. 7). In this context the importance of accurate risk assessment becomes obvious and the main challenge is “to calculate loss propensity and exposure” (Manral, 2015, p. 8). Thereby, uncertainty forms “the essence of the problem” (Cardon & Hendel, 2001, p. 414) as the policy premium has to cover the risk to ensure a profit but at the same time has to be set before the total number and cost of claims is known. Thus, statistical modelling is necessary in order to predict what is likely to happen in the future (Marr, 2015). Consequently, the insurance industry has always been data intense and the promise of Big Data and the “increasing ability to record, store and analyse data” (Marr, 2015) has tremendous potential in enhancing the predictive models and better coping with the uncertainty underlying the insurance industry.

### *2.3.1 Adverse Selection*

The precise and appropriate risk assessment is especially important in the light of the phenomenon of adverse selection. Adverse selection is based on asymmetric information, meaning that, in a health insurance context, the person buying a policy has better knowledge about his or her status of health than the insurance company. In other words, adverse selection refers to “the exercise of an option by a person in his own favor and against the interest of the insurer in a case where his and the insurer’s interests are not the same” (Long, 1990, p. 34). “Individuals who have prior knowledge of their future health problems, will buy the most comprehensive coverage they can in order to cover their future health related costs. Insurance companies accepting these applicants without having knowledge of their potential health problems will offer them policies with premiums which do not reflect true risk” (Borna & Avila, 1999, p. 356). This also indicates that “people who are likely to buy insurance will be those who are increasingly certain that they will need insurance” (Borna & Avila, 1999, p. 356) which will lead to higher costs for insurance companies who then in turn raise the premiums. Ultimately, this process could lead to the better risks no longer buying insurance, “leaving a higher proportion of poor risks to share the costs of benefit payments” (Borna & Avila, 1999, p. 356).

### 2.3.2 Moral Hazard

Another issue in this context of principal-agent problems and asymmetric information is moral hazard. It describes the tendency that insured individuals might take on risk prone behaviour as they know someone else, the insurance, will cover the claim and bear the cost of those risks (Cardon & Hendel, 2001). Additionally, a major problem associated with moral hazard is insurance fraud. Policyholders who file fraudulent, bogus claims cost insurance companies, alone in the U.S. and excluding health insurance, more than \$40 billion per year (FBI, 2016).

These described challenges and problems caused by asymmetric information could be mitigated or prevented if the insurance companies had the same information available as the agents, the customers. Thus, they proclaim an ever increasing need for information to engage in ‘fair discrimination’, meaning “to measure as accurately as practicable the burden shifted to the insurance fund by the policyholder and to charge exactly for it, no more and no less” (Worham, 1985, p. 361). Therefore, the use of Big Data, or IoT and wearable devices, and the collection of more sensitive, private data is generally endorsed by industry insiders and the benefits are believed to be manifold.

As this study takes a customer perspective, it might seem that the described challenges inherent in the insurance industry are irrelevant for the conducted research. But as they motivate the adoption of wearable devices by the insurance companies, and as the implications are broad, ultimately affecting every individual buying an insurance policy, those phenomena are important to consider.

## 2.4 Big Data in the Insurance Industry

As shown above, the concept of Big Data and the associated new technologies offer great potential for insurance companies. Big Data has “the power to transform processes, organizations and entire industries” (Schroek & Shockely, 2015). Therefore, massive changes in how business is conducted in the insurance industry can be expected (Economist, 2015).

Already today is the increasing reliance on crunching numbers to enhance organizational performance affecting and revolutionizing business practices. Improved predictive models and, as a result, a more precise risk assessment, also postulated as ‘underwriting 2.0’ (Sureify, 2016), promise benefits but also new challenges, both on the company and customer side.

While across all types of insurances Big Data is offering potential improvements, the two most discussed applications are in life or health and auto insurance. Since the focus of this work is on the former, only this application is going to be discussed in detail.

Still, research in the context of auto insurance entails significant similarities to our field of study and some valuable insights into the problem area can be gained. Therefore, a short introduction into the matter can be found in Appendix 1.

### 2.4.1 Life and Health Insurance

In recent years industry insiders and the media have engaged in a lively discussion about the usage of wearable devices for underwriting purposes in health and life insurances (Jurgens, 2015; Martin, 2015; Olson, 2014). Opportunities and benefits are outlined as well as the con-

cerns accompanying the adoption of Big Data approaches in the industry. Especially in countries which are traditionally more concerned when it comes to consumer privacy, for example Germany, the implementation and adoption of respective policies is controversial and the debate is heated (Endt, 2014; Janker, 2014). Meanwhile, insurance companies in other parts of the world are already offering policies to their customers in which wearable technology, smart watches or fitness trackers, play a major role. According to a survey conducted by Accenture, a third of the polled insurers are already using wearables to engage customers and “63 percent of respondents believe that wearable technologies (“wearables”) will be adopted broadly by the insurance industry within the next two years” (Accenture, 2015).

The approach is fairly simple: the customer buys an insurance policy and is provided with a free fitness tracker (some insurance companies might also only offer the opportunity to use one’s own device) and a corresponding app that monitors the individual fitness achievements. Moreover, the customer agrees to share the collected data concerning specific health or fitness values with the insurance company and consequently the insurer can use the personal data in order to tailor the service. Fulfilling fitness challenges or requirements, such as increasing the number of steps taken or reducing weight, then leads to a reduction in the premium or other rewards, depending on the specific insurance plan. While traditionally underwriting is based on certain fixed customer variables and result in insurance premiums which fluctuate once a year, at very most, the new approach provides for flexibility, a great degree of personalization, and premiums which are adjusted almost in real-time according to relevant metrics. “It’s about having a lifetime of data on a policyholder instead of one static portrait” (Sureify).

For example, Hancock (2016), a U.S. based company, advertises a life insurance with the slogan “protect the ones you love, while saving money and earning valuable rewards and discounts by simply living a healthy life” (Hancock, 2016). Moreover, they state “the healthier your lifestyle, the more you’ll save and the greater your rewards” (Hancock, 2016). Similar policies are offered by HumanaVitality (2016) who think that “you should be rewarded for making healthier choices”, VitalityLIFE which tries to “encourage you to lead a healthier life and reward you for doing it”, and the Australian company AIA (2016) which believes “you can achieve a fitter, healthier lifestyle; and working towards improving your health will earn you points [...], unlocking the added incentive of ongoing discounts and rewards along the way”. Country specific laws and regulations might still inhibit the wider adoption, but the overall trend towards these data-based approaches in health and life insurance is evident.

While insurance companies hope to improve their risk assessment and consequently increase profits with this approach, they also expect to change their customers’ behaviour towards a healthier lifestyle so that less costs occur to begin with. From a customer perspective these new policies provide the opportunity and the incentive to lower the insurance premium and to collect further rewards. But at the same time sensitive information has to be revealed and transmitted to private corporations, causing major privacy concerns which are the main controversial subject in the current discussion (Christophersen et al., 2015).

As the specific, perceived benefits and risks of these new approaches constitute the major theme and area of research for this thesis, they will not be anticipated here. Instead, a detailed examination of related scientific literature will be outlined in Section 3.4.

In the end, the success of the data-driven approach is dependent on the customer’s willingness to disclose their information to the insurance companies.

## 3 Theoretical Background

In this chapter the related work and conceptual background relevant for this thesis is summarized. It forms the fundament for our research model which is developed based on the illustrated concepts and presented at the end of the chapter.

Given the fact, that our study is rooted in the area of Big Data in the insurance industry and that specifically the usage of data collected by fitness trackers in health and life insurance is considered, we believe that literature in all of the below mentioned fields provide theoretical foundation for this work. Nevertheless, this review does not represent an exhaustive search of publications, but rather the intent to provide a structured and comprehensive background.

### 3.1 Willingness to Disclose Personal Information

The purpose of this study is to determine factors which influence the individual willingness to disclose personal, sensitive information collected by wearable devices to health or life insurance companies (see Section 1.4). As already outlined in the motivation (Section 1.3), a significant research gap exists in this field and consequently no prior research models or frameworks, suitable for this particular problem area, are available. However, an extensive literature search revealed that a lot of studies have been conducted in related fields, for example information disclosure in an online shopping or e-commerce context and the sharing of information in the healthcare system. While the nature of the information to be disclosed or the recipient of the data may differ significantly from the scenario in our research study, it is still believed that the general dynamics and principles are similar and, with careful consideration, can be transferred to our field of interest. The most important publications in these areas which contain research models relevant for the purpose of our study are listed in Table 3.1 and 3.2.

#### 3.1.1 *Information Disclosure in an E-Commerce Context*

The willingness to disclose personal information, also called the intention to disclose, has been thoroughly researched in an e-commerce context. As the competitive strategies of companies, especially online vendors, increasingly depend on vast amounts of customer data (Culnan & Armstrong, 1999), there is a heightened interest in factors influencing customers decision to disclose or withhold their personal information online.

Several different models including various constructs with an effect on the dependent variable of intention or willingness to disclose information have been developed, tested and proposed to the research community (see Table 3.1).

**Table 3.1: Considered research in the field of information disclosure (e-commerce)**

Reference	Topic	Constructs	Constructs borrowed
(Dinev & Hart, 2006)	E-commerce transactions	<ul style="list-style-type: none"> <li>- Perceived Internet privacy risk</li> <li>- Internet privacy concerns</li> <li>- Internet trust</li> <li>- Personal Internet interest</li> <li>- <i>Willingness to provide personal information</i></li> </ul>	<ul style="list-style-type: none"> <li>- Perceived risks</li> <li>- Perceived benefits</li> <li>- Trustworthiness of insurance company</li> </ul>
(Treiblmaier & Chong, 2012)	Online Information Disclosure	<ul style="list-style-type: none"> <li>- Perceived risk of personal information</li> <li>- Trust in the online vendor</li> <li>- Trust in the internet</li> <li>- Internet experience (Moderator)</li> <li>- <i>Disclosure of personal information</i></li> </ul>	<ul style="list-style-type: none"> <li>- Perceived risks</li> <li>- Trustworthiness of insurance company</li> </ul>
(Uilenberg, 2015)	Disclosing personal information when shopping online	<ul style="list-style-type: none"> <li>- Perceived benefits</li> <li>- Perceived risks</li> <li>- Website trust</li> <li>- Cultural values (Moderator)</li> <li>- Internet skills (Moderator)</li> <li>- <i>Willingness to disclose personal information</i></li> </ul>	<ul style="list-style-type: none"> <li>- Perceived benefits</li> <li>- Perceived risks</li> <li>- Trustworthiness of insurance company</li> <li>- Customer characteristics</li> </ul>
(Wakefield, 2013)	Online information disclosure	<ul style="list-style-type: none"> <li>- Internet security</li> <li>- Website trust</li> <li>- Website privacy</li> <li>- Positive affect</li> <li>- Negative affect</li> <li>- <i>Intention to disclose</i></li> </ul>	<ul style="list-style-type: none"> <li>- Security concerns</li> <li>- Trustworthiness of insurance company</li> <li>- Invasion of privacy</li> </ul>
(Zimmer, Aarsal, Al-Marzouq, & Grover, 2010)	Online information disclosure	<ul style="list-style-type: none"> <li>- Trust</li> <li>- Risk</li> <li>- Relevance</li> <li>- Attitude</li> <li>- Usefulness</li> <li>- <i>Intent to disclose</i></li> <li>- <i>Actual disclosure</i></li> </ul>	<ul style="list-style-type: none"> <li>- Trustworthiness of insurance company</li> <li>- Perceived risks</li> </ul>

Thereby, the focus is set on distinct factors and different aspects of the phenomenon are examined. It is out of the scope of this research to summarize and outline every single study, nevertheless, several concepts recur and are confirmed by multiple researchers. For example, the construct 'risk', labelled as 'perceived risk of personal information' (Treiblmaier & Chong, 2012) or 'perceived Internet privacy risk' (Dinev & Hart, 2006) is a predominant theme (Dinev & Hart, 2006; Treiblmaier & Chong, 2012; Uilenberg, 2015; Zimmer et al., 2010). It is generally accepted as a fact that perceived risks have a negative effect on the willingness to provide personal information (Culnan & Armstrong, 1999). We therefore borrowed this construct for our research model and examined it in detail (see Section 3.5.1).

Another reoccurring idea is that of trust. Either defined as internet, website, or vendor trust it was as well shown to have a crucial effect on the willingness to disclose information (Dinev & Hart, 2006; Treiblmaier & Chong, 2012; Uilenberg, 2015; Wakefield, 2013; Xu, Tan, & Hui, 2003; Zimmer et al., 2010). Transferring the idea to our context, we frame it as the trustworthiness of insurance companies. Additionally, we found evidence that privacy is a major issue and that security concerns might exist (Wakefield, 2013). Moreover, Uilenberg (2015) highlights the fact that cultural values and international differences have an influence on the disclosure decision. This is also examined by Gupta, Iyer, and Weisskirch (2010) and

Treiblmaier and Chong (2012). Hann, Hui, Lee, and Png (2002), Phelps et al. (2000) and Malhotra, Kim, and Agarwal (2004) include specific personal characteristics in their considerations. We combine these ideas into the concept of ‘customer characteristics’, considering cultural effects by including the country of origin.

Due to the prevalence and proven influence on information disclosure in the literature concerning e-commerce, the constructs of perceived risks, invasion of privacy, security concerns, customer characteristics and trustworthiness of insurance companies were borrowed for the purpose of our study (see Section 3.5 for a detailed description). The constructs not considered were too specifically tied to the e-commerce context and thus not relevant for our study.

The reviewed literature also shows that the type of information requested makes a difference with regard to the willingness to disclose (Phelps et al., 2000). Thus, while it seems to be reasonable to borrow some concepts from the e-commerce background for our purposes, it still has to be considered that personal health information is more sensitive than other types of information (Bansal et al., 2010). Therefore, additional factors specifically referring to this kind of information might play a role.

### 3.1.2 Information Disclosure in a Health Information Context

Literature pertaining directly to health information disclosure, even if not in the context of the insurance industry, is rare but highly relevant in order to inform our research.

**Table 3.2: Considered research in the field of information disclosure (health information)**

Reference	Topic	Constructs	Constructs borrowed
(Anderson & Agarwal, 2011)	Consumer willingness to disclose personal health information	<ul style="list-style-type: none"> <li>- Electronic health information privacy concern</li> <li>- Trust in electronic medium</li> <li>- Type of information</li> <li>- Intended purpose</li> <li>- Requesting stakeholder</li> <li>- Health status emotion</li> <li>- Controls (e.g. age, gender, education)</li> <li>- <i>Willingness to provide access to personal health information</i></li> </ul>	<ul style="list-style-type: none"> <li>- Invasion of privacy</li> <li>- Trustworthiness of insurance company</li> <li>- Security concerns</li> <li>- Consumer characteristics (especially health status)</li> </ul>
(Bansal et al., 2010)	Disclosing health information online	<ul style="list-style-type: none"> <li>- Perceived health information sensitivity</li> <li>- Health status</li> <li>- Personality</li> <li>- Health information privacy concern</li> <li>- Previous online privacy invasion</li> <li>- Trust in the health website</li> <li>- Risk beliefs</li> <li>- Prior positive experience with the Website</li> <li>- <i>Intention to disclose health information</i></li> </ul>	<ul style="list-style-type: none"> <li>- Consumer characteristics (Health status and other features)</li> <li>- Invasion of privacy</li> <li>- Trustworthiness of insurance company</li> <li>- Perceived risks</li> </ul>

When examining the respective publications, the first thing that becomes apparent is that, despite a broad consistency with research in the e-commerce context, the topic of privacy is attracting more attention. Privacy concerns are explicitly mentioned in the models by Anderson and Agarwal (2011) as well as Bansal et al. (2010), suggesting that in the health information environment privacy considerations are even more important than in the e-commerce context. The sensitive nature of the data is affecting people's willingness to share this information openly. This observation confirms our prior decision to incorporate 'invasion of privacy' as a construct in our research model.

Additionally, both studies verify that trust is as important as in the e-commerce context. As already described above, we adopt this idea in our concept of 'trustworthiness of the insurance company'. Nevertheless, Anderson and Agarwal (2011) explicitly talk about "trust in electronic medium". As our electronic medium for data transmission is the fitness tracker, we also see an indication for existing 'security concerns' regarding the device and the surrounding infrastructure (see Section 3.5.1.6).

Furthermore, the authors include risk scenario variables as moderating factors in their examination (Anderson & Agarwal, 2011). Since our research model is specifically tailored to the disclosure of health information collected by wearable devices for underwriting purposes of health or life insurance companies, those factors are irrelevant for us. The type of information, the purpose of usage, and the requesting stakeholder are fixed and not changing in the context of our study. They consequently do not have to be incorporated in the model as moderators. Still, the authors make another valuable contribution with their consideration of the health status and associated emotions. For simplification reasons we concentrate on the health status only, neglecting the additional component of emotions. The importance of the individual health condition is also reflected and justified in the publication by Bansal et al. (2010). They argue that "individuals' intention to disclose [...] information depends on their trust, privacy concern, and information sensitivity, which are determined by personal dispositions" (Bansal et al., 2010, p. 138). Personal dispositions are thereby defined as personality traits, health status, prior privacy invasions, risk beliefs, and experience. All of these aspects, except for the specific personality traits which would have been out of the scope of this work due to complexity, influenced our work and are reflected in the model. Thereby, prior privacy invasions and experience are not individually mentioned as it is assumed that they are contained in the construct of trust. If someone experienced prior privacy invasions by his or her insurance company or instead had positive experience with them, this is most certainly going to influence the level of trust in the corporation. The inspiration to incorporate 'customer characteristics' as a moderator in our model was taken from the controls as mentioned by Anderson and Agarwal (2011) and the moderators as outlined by Bansal et al. (2010).

An additional source in the field of sharing personal health information examined the influence of financial rewards on health information disclosure (Pickard, 2014). It could be shown that "consumers exist who are willing to sell their de-identified personal health information" (Pickard, 2014, p. 1). While in our scenario the information is not necessarily de-identified, we still believe that financial incentives could have a severe effect on disclosing intention.

In summary, the literature concerned with the willingness to disclose information, both in an e-commerce and health information context, led us to include the constructs of perceived risk (Section 3.5.1), invasion of privacy (Section 3.5.1.1), security concerns (Section 3.5.1.6), financial benefits (Section 3.5.2.1), trustworthiness of insurance company (Section 3.5.3.1), and customer characteristics, particularly the health status, (Section 3.5.3.2) in our research model.

## 3.2 Information Privacy and Related Theory

All of the above examined scientific papers are closely interweaved with information privacy considerations. Apparently, disclosing information to a third party is unavoidably connected to major privacy concerns. The sensitive nature of health data is further aggravating the worries. In order to account for this strong affiliation, the literature search was expanded to include additional background information, such as specific privacy theory and other privacy related concepts (see Table 3.3).

**Table 3.3: Additionally considered research in the field of information privacy**

Reference	Topic	Theory
(Culnan & Armstrong, 1999)	Information disclosure in consumer transactions	Privacy calculus
(Dinev & Hart, 2006)	E-commerce transactions	Extended privacy calculus
(Laufer & Wolfe, 1977)	Privacy	Calculus of behaviour
(Norberg, Horne, & Horne, 2007)	Personal information disclosure intentions versus behaviors	Privacy paradox
(Smith et al., 2011)	Information privacy research	various

### 3.2.1 Privacy Paradox

In times where “personal consumer data is the fuel for information driven programs that may differentiate a firm from its competitors and create strategic advantages” (Wakefield, 2013, p. 157), the collection, distribution and storage of personal information has become a standard procedure. Companies in all industries try to “leverage the ability to collect and analyze ever-greater amounts of consumer information” (Norberg et al., 2007, p. 100). However, as already described in Section 2.2, information privacy is a “highly cherished value” (Dinev & Hart, 2006, p. 61) and concerns among customers are widespread and rising (Hann et al., 2002). Consequently, “a tension exists between the user’s desire to protect personal information and the needs of online businesses for consumer data” (Wakefield, 2013, p. 157). Consumers often find themselves in a dilemma, where they have to give up their control over “when, how, and to what extent information about them is communicated to others” and “when such information will be obtained and what uses will be made of it by others” (Westin, 1967, p. 7), in order to be able to use a specific service.

The phenomenon called “privacy paradox” (Norberg et al., 2007; Smith et al., 2011) specifically describes how despite the complaints about privacy violations, “it appears that consumers freely provide personal data” (Norberg et al., 2007, p. 100). In other words, it illustrates the “discrepancy between individuals’ intentions to protect their own privacy and how they behave in the marketplace” (Norberg et al., 2007, p. 101). Norberg et al. (2007) proof the existence of the phenomenon and try to explain why it occurs. They hypothesize that risk only affects the intention to disclose, while trust directly influences the actual behaviour and therefore is a major factor in the final disclosure decision. In their study, they find that risk “significantly influences individuals’ intentions to provide” information, and state that “the influence of trust on actual behavior [...] is still a question” (Norberg et al., 2007, p. 118). While the study focuses on the discrepancy between behavioural intention to disclose information and actual disclosure behaviour, our study is only concerned with the behavioural intention.

Still, the findings affirm the importance of risk as a construct in our model and justify the incorporation of trust as a moderating factor. Additionally, while trying to answer the question what makes customers disclose information despite the prevailing privacy concerns, the authors point to another concept. By stating that it is no surprise “that people are willing to trade personal information for perceived benefits” (Norberg et al., 2007, p. 101), they indicate that information is disclosed, if the expected value of the benefits is greater than the perceived privacy risk.

### 3.2.2 *Privacy Calculus*

This abiding theory which is mentioned by most authors concerned with the disclosure of private, sensitive information (see Section 3.1) is the so-called ‘privacy calculus model’. As stated above, the model builds on the observation that “individuals are willing to disclose personal information in exchange for some economic or social benefit” (Culnan & Armstrong, 1999, p. 106). More precisely, people engage in a ‘privacy calculus’ in order to decide whether to disclose information or not (Culnan & Armstrong, 1999). This decision process takes the form of a risk-benefit analysis or a trade-off where the expected benefits and costs (risks) are weighted against each other. Again, the factor of trust influences users’ beliefs about the cost-benefit calculus (Dinev & Hart, 2006). It is believed that “individuals will disclose personal information if they perceive that the overall benefits of disclosure are at least balanced by, if not greater than, the assessed risk of disclosure” (Dinev & Hart, 2006, p. 62). Thus, the concept of privacy is not viewed as “absolute but, rather, subject to interpretation in ‘economic terms’” (Smith et al., 2011, p. 1001). Consequently, this approach explains why people might disclose sensitive information despite major privacy concerns. In summary, the theory identifies perceived privacy risks and perceived benefits as independent variables which influence the willingness to disclose personal information.

The concept of a privacy calculus as described by Culnan and Armstrong (1999) and extended by Dinev and Hart (2006) is based on the calculus of behaviour (Laufer & Wolfe, 1977) which suggests the consideration of future consequences in decisions concerning the engagement in a specific behaviour. This corresponds to expectancy theory (Vroom, 1964) which “broadly supports the notion that a person considers the sum of the valences of all possible outcomes and seeks to maximize positive outcomes and minimize negative outcomes in her motivation to act or not act” (Anderson & Agarwal, 2011, p. 471). Moreover, the model is also rooted in the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) and the theory of planned behaviour (TPB) (Ajzen, 1991). While the derivation is out of the scope of this work, the prevalence of the model is undeniable. Due to this wide dissemination and adoption in the literature relevant to our field of study, the theory of the ‘privacy calculus’ is considered as very important and almost forming a standard in the research area. Therefore, the trade-off between risks and benefits forms the main underlying idea of our study and serves as a foundation for our research model. These two constructs of perceived risks (see Section 3.5.1) and perceived benefits (see Section 3.5.2) are borrowed as the central components of our conceptual framework, forming the main factors which influence the willingness to disclose sensitive information to health or life insurance companies. Furthermore, the privacy calculus as described by Dinev and Hart (2006) again highlights the important role of trust in the context of information disclosure and justifies its adoption as a moderator in our research model.

In the course of our previous research (see Section 3.1) it became apparent that alongside the privacy risk, other factors, not directly related to privacy concerns, are contributing to the cost

side of the calculus equation. Similarly, the benefits of disclosing information to health or life insurance companies might be too complex and versatile to condense them in one construct, even if the above reviewed literature does not specifically outline dedicated instances. It was therefore decided to generalize the factor ‘privacy risk’ to a multi-layered construct called ‘perceived risks’ which includes privacy concerns as the subconstruct ‘invasion of privacy’. This multidimensional nature of the construct was also described by Smith et al. (2011). Correspondingly, is the element of benefits filled with various different aspects which will be derived in the following Sections 3.3 and 3.4.

### *3.2.3 Other Remarks on Information Privacy*

While it is generally acknowledged that privacy concerns are “a hot topic” (Norberg et al., 2007, p. 100) and common amongst consumers, researchers found that “privacy perceptions vary widely across populations and even within specific segments” (Norberg et al., 2007, p. 101). According to Smith et al. (2011), “privacy concerns form because of an individual’s personal characteristics or situational cues” (p. 998). Specifically, this means that personality differences, for example in terms of the “big-five” personality traits, have been found to influence individual privacy concerns (Bansal et al., 2010; Lu, Tan, & Hui, 2004). Moreover, demographic differences were stated as a factor affecting “the degree of stated privacy concerns” (Smith et al., 2011, p. 999). According to Sheehan (1999), women are more concerned about their privacy than men, and “also, it was found that those consumers who were less likely to be concerned about privacy were more likely to be young, poor, less educated” (Smith et al., 2011, p. 999). Additionally, differences in cultural values also account for varying perceptions of privacy risks. Consumers in different countries show diverging levels of concern for their privacy (Bellman, Johnson, Kobrin, & Lohse, 2004; Dinev et al., 2006). Moreover, the concepts of privacy experience, describing if individuals have previously “been exposed to or been the victim of personal information abuses” (Smith, Milberg, & Burke, 1996, p. 186), and general privacy perceptions were found to influence privacy concerns (Smith et al., 2011).

These effects on the perception and assessment of risks, and also on benefits, are integrated into the conceptual model as moderators. As they do not directly affect the willingness to disclose sensitive information, but rather influence how the risks and benefits are evaluated, this moderating role is most appropriate. Summarized under the construct of ‘customer characteristics’ (see Section 3.5.3.2), we include demographic values and cultural differences, such as age, gender, and country of origin in our considerations. While it was decided to not incorporate specific personality traits in the study due to the limited scope of the work, general privacy perceptions are accounted for. The concept of privacy experience is believed to be strongly correlated with the trustworthiness of the insurance company and was therefore not reported separately.

## **3.3 Wearable Devices**

A prerequisite for sharing personal health information with insurance companies is that customers actually wear devices capable of measuring relevant values and transmitting the collected data to the insurer. Therefore, research conducted in the field of wearables or fitness trackers (see Section 2.1.3) is highly suitable for the purpose of this study.

Nevertheless, it has to be considered that in the described scenario wearable devices are mostly distributed for free by the insurance companies, without any further costs. Moreover, they do not only fulfil the purpose of measuring and tracking fitness or health achievements for one's own self-interest, but are worn consciously with the intention to send the information to the insurer. Consequently, some of the concepts in the literature cannot be transferred easily to the context of this study and have to be examined critically or even have to be neglected.

Generally, the non-technical literature concerned with wearable devices can be divided into two main categories: firstly, user acceptance and adoption of the devices and secondly, major challenges, especially data privacy and security concerns. A listing of the considered papers is given in Table 3.4.

**Table 3.4: Considered research in the field of wearable devices**

Reference	Topic	Theory	Constructs	Constructs borrowed
(Britton, n.d.)	Data Privacy and Security	-	-	- Invasion of privacy - Security concerns
(Gao et al., 2015)	Acceptance of wearable technology in healthcare	Unified theory of acceptance and use of technology (UTAUT2)  Protection motivation theory (PMT)  Privacy calculus theory	- Performance expectancy - Hedonic motivation - Effort expectancy - Functional Congruence - Self-Efficacy - Social influence - Perceived vulnerability - Perceived severity - Perceived privacy risk - Product type - <i>Intention to adopt wearable devices</i>	- Social image - Perceived risks - Invasion of Privacy - Perceived benefits - Health motivation - Customer characteristics (health status)
(Kim & Shin, 2015)	Acceptance of smart watches	Extended technology acceptance model (TAM)	- Affective quality - Relative advantage - Mobility - Availability - Perceived usefulness - Perceived ease of use - Subcultural appeal - Attitude - Cost - <i>Intention</i>	- Social image
(Langley, 2014)	Privacy Problems	-	-	- Invasion of privacy
(Yang et al., 2016)	Acceptance of wearable devices	Not specified, but grounded in privacy calculus and TAM	- Functionality - Compatibility - Visual attractiveness - Brand name - Perceived usefulness - perceived enjoyment - social image - performance risk - financial risk - Perceived value - <i>Intention to use</i>	- Social image - Perceived benefits - Perceived risks

### 3.3.1 Adoption and Acceptance of Wearable Devices

As wearing a fitness tracker is required in order to benefit from the advantages of the new insurance policies, the acceptance of those devices might also have an influence on the willingness to buy such a policy and consequently on the willingness to disclose information to the insurance company. Therefore, the three acceptance models of Gao et al. (2015), Kim and Shin (2015), and Yang et al. (2016) were considered for the purpose of our work.

The publication of Gao et al. (2015) is concerned with wearable technology acceptance in healthcare and is therefore thematically the closest examination to our topic in the examined wearable literature. However, the context is still quite different from our research and it again has to be noted that the dependent variable is not the willingness to disclose information but the intention to adopt healthcare wearable devices. Still, some constructs might be of relevance for our research endeavour.

The authors build their model on three different perspectives: technology, healthcare, and privacy. The technology perspective is rooted in the unified theory of acceptance and use of technology (UTAUT2). According to the authors, this technology acceptance model is “the most comprehensive one to explain consumer’s technology acceptance and use” (Gao et al., 2015, p. 1707). From the seven direct factors which affect consumer’s intention to adopt a technology mentioned in the original model (Venkatesh, Thong, & Xu, 2012), the authors adopt performance expectancy, hedonic motivation, effort expectancy, social influence, facilitating conditions, and functional congruence. As already described above, the intention behind wearing a fitness tracker for underwriting purposes might substantially differ from the normal motivation to adopt this technology. Therefore, the adoption is not necessarily expected to “bring effectiveness to users in performing certain activities” (Gao et al., 2015, p. 1708) or to “fulfil the functional and basic product-related needs” (Gao et al., 2015, p. 1709), especially as it comes for free. Moreover, we assume that the ease of use is not a barrier since the need for interaction with the device is very limited and no prior knowledge is required in order to be able to handle the device. Therefore, all of these constructs, except for hedonic motivation and social influence, are irrelevant for our research purposes. Nevertheless, we think that the social influence might form a factor with a direct influence on the willingness to disclose information. The user’s decision making might be influenced by others’ perceptions (Gao et al., 2015). Additionally, the idea of a hedonic motivation, defined as “pleasure or enjoyment derived from adopting and using a technology” (Gao et al., 2015, p. 1708), is adapted for our purposes. We believe that the motivation to lead a healthier lifestyle caused by the wearable and the insurance policy itself, might serve as a benefit to certain people.

The second angle on their model is constituted by a healthcare perspective based on the protection motivation theory (PMT). Following this theory Gao et al. (2015) add perceived vulnerability, “the possibility that one will experience health threat” (p. 1710), and perceived severity, “extent of threat from unhealthy behaviors” (p. 1710) to their model. Again, users in our scenario are not primarily adopting the technology to “reduce or avoid health threats” (Gao et al., 2015, p. 1710), and thus these constructs are not transferable, either. However, they are comparable to our conceptualization of the health status and health motivation.

The last influence on their model is constituted by a privacy perspective, more precisely, the privacy calculus approach. As extensively discussed in Section 3.2.2, this entails the consideration of perceived privacy risks and perceived benefits.

Another acceptance model, with respect to smart watches, was developed by Kim and Shin (2015). They base their framework on the technology acceptance model (TAM). According to

the authors, this “is one of the most extensively utilized theoretical models for studying the end-user acceptance of ICT” (Kim & Shin, 2015, p. 528). It determines perceived ease of use and perceived usefulness as the key psychological determinants of user acceptance of technology (Davis, 1989). In their work Kim and Shin (2015) develop and test an extended version of this model in which they include additional factors of smart watch adoption such as affective quality, relative advantage, mobility, availability, subcultural appeal, and cost. As explained before, the concept of ease of use, including the factors mobility and availability, are dispensable in the context of this study as it is assumed that the transfer of the data is initiated automatically, no further handling of the fitness tracker is necessary and no additional features available (in contrast to smart watches). Similarly, the explanation for the exclusion of perceived usefulness and cost was given in the context of the model developed by Gao et al. (2015). However, subcultural appeal is comparable to social influence, described by Gao et al. (2015), and is believed to play a role in the decision whether to disclose information or not.

Yang et al. (2016) develop a similar structural model. Following the privacy calculus approach, they define perceived risks and perceived benefits which are shown to influence the perceived value of the device and consequently the adoption intention. Just like in the conceptualization of Kim and Shin (2015) the benefits consist of perceived usefulness (influenced by functionality and compatibility), perceived enjoyment, and social image. Again, the first two constructs are neglected in our research, while the social image is adopted. In order to lower the complexity of our proposed model the influencing factors of ‘visual attractiveness’ and ‘brand name’ are summarized in the umbrella concept of social image. While the general idea of perceived risks is included in our model, the specific risk in financial terms or performance do not apply in our context.

All in all, the literature concerned with the acceptance of wearable devices shows that the trade-off between perceived risks and benefits is also a common concept in this area of research. While most of the constructs are not relevant, due to different circumstances in the scenario to be investigated, it could still be derived that the factors of ‘social image’, ‘health motivation’, and the individual state of health might have an influence on the willingness to disclose information to health or life insurance companies. Furthermore, the publications inspired us to also include the receiving of a wearable in general as a construct in our research model, as it might be of value to potential or current customers.

### *3.3.2 Privacy and Security Concerns*

In addition to the examinations of acceptance and adoption of consumer wearable devices, the issues of privacy and security have attracted some attention. While the technical literature is concerned with the underlying infrastructure and its weak spots, e.g. “wireless communications make physical eavesdropping almost undetectable” (Di Pietro & Mancini, 2003, p. 76), other publications take on a legal or societal perspective. For example Britton examines related concerns in the legal framework of the United States and Langley (2014) calls for an adaptation of old laws to modern times and poses several questions including “are people comfortable with companies knowing how truly lazy they are? How stressed they get around the holiday season? How their heart rate skyrockets whenever they are around certain people? How well they sleep?” (p. 1659). While our study tries to answer these questions in the specific context of health and life insurance companies, those publications strengthen first of all the argument for the inclusion of ‘invasion of privacy’ and ‘security concerns’ as perceived risks in the research model.

### 3.4 Disclosing Health Information to Insurance Companies

In contrast to the more general topics of wearable devices, data privacy, and the willingness to disclose information in other contexts, the specific application of Big Data technologies in the health or life insurance industry did not receive a comparable amount of scientific attention. While the field becomes increasingly popular amongst practitioners, industry insiders and the general media, relatively few scientific articles can be found which are concerned with the arising opportunities and challenges accompanying the advent of wearable devices and its adoption for underwriting purposes.

For this reasons, scientific papers not explicitly concerned with the disclosure of information collected by wearable devices, but with genetic data or information gathered through data mining in the context of health or life insurances, were also included in the review process. The relevant literature is listed in Table 3.5.

**Table 3.5: Considered research in the field of disclosing health information to insurers**

Reference	Topic	Derived Constructs
(Christophersen et al., 2015)	Wearable health tracking devices to reduce health insurance costs in organizations	<ul style="list-style-type: none"> <li>- Invasion of Privacy</li> <li>- Data Accuracy</li> <li>- Secondary Use</li> <li>- Discrimination</li> <li>- Manipulation</li> <li>- Health Motivation</li> <li>- Financial Benefits</li> <li>- Increased Fairness</li> </ul>
(Al-Saggaf, 2015)	Data mining by private health insurance companies	<ul style="list-style-type: none"> <li>- Improved Products and Services</li> <li>- Increased Fairness</li> <li>- Discrimination</li> <li>- Invasion of Privacy</li> <li>- Secondary Use</li> <li>- Data Accuracy</li> </ul>
(Borna & Avila, 1999)	Disclosing genetic information to insurance companies	<ul style="list-style-type: none"> <li>- Increased Fairness</li> <li>- Discrimination</li> <li>- Invasion of Privacy</li> <li>- Secondary Use</li> </ul>
(Armstrong et al., 2003)	Disclosing genetic information to life insurance companies	<ul style="list-style-type: none"> <li>- Discrimination</li> </ul>

The only publication available which specifically addresses the adoption of wearable health data tracking devices in the context of health insurance was issued by Christophersen et al. (2015). The authors focus on American self-insured companies which adopt health-tracking devices “to combat rising health insurance costs” (p. 1) by discouraging employees’ unhealthy behaviour through monitoring and by differentiating insurance premiums (Christophersen et al., 2015). Taking into account that “more than half of all Americans receive health insurance through their employers” (Christophersen et al., 2015, p. 2), the scientists investigate how the introduction of wearable devices “in an organizational setting shapes the relationship between the employee, the organization, and health conditions in certain unforeseen ways” (Christophersen et al., 2015, p. 1). Thus, the main difference to our approach is that the relationship between employees and employers is investigated, not the direct relationship between insurance companies and their customers. Furthermore, the authors do not develop a model,

but rather explore and discuss the issues. Three central challenges are stated: firstly, “wearable health-tracking devices in organizational settings risk disciplining employees, by tempting or penalizing them financially”, secondly, “health concerns are reduced to numbers” and finally the new approaches “bring health surveillance into everyday lives of people jeopardizing privacy” (Christophersen et al., 2015, p. 2).

The authors take a qualitative approach based on grounded theory in order “to gain a comprehensive overview and insight into the possible challenges of wearable health-tracking devices” (Christophersen et al., 2015, p. 2). They highlight that it is “important to pause and debate wearable health-tracking technology before it is fully embedded into organizational settings and societies” (Christophersen et al., 2015, p. 2).

Al-Saggaf (2015) is not specifically referring to Big Data and wearable devices, but explores the use of data mining by private Australian health insurance companies. He especially focuses on customers' privacy and develops an argument based on an empirical approach. By using classical philosophical theories for an ethical analysis, he comes to the conclusion that “the use of data mining by private health insurance companies in Australia [is] unethical” (Al-Saggaf, 2015, p. 281). While in our context customers are aware that the data collected by fitness trackers is used for underwriting purposes by the insurance company, Al-Saggaf (2015) is assuming an absence of consent or that customers do not have knowledge about the data mining at all. This forms a major difference between our works, preventing a direct comparison. Still, the discussion about major privacy concerns, including potential discrimination and cherry-picking of customers, is highly relevant, just as the introduced concept of “secondary use” and his summary of standard theories of privacy.

Moreover, two publications, concerned with the disclosure of genetic information to health or life insurance companies, are available. Borna and Avila (1999) claim to “assess public opinion concerning access to genetic information for underwriting purposes” (p. 355), and discuss “alternatives available to cover the health insurance costs of individuals who carry genetic materials which predisposes them to certain illnesses” (p. 355). Especially, the first part of this research goal is comparable to ours, even though genetic information might be more critical than health and fitness data collected through wearable devices. Still, it is believed that the implications are similar and can therefore, at least partially, be transferred to our context. The authors present arguments for and against the disclosure of genetic data to insurance companies and demonstrate the results of a resident opinion survey (Borna & Avila, 1999). The biggest concern accompanying the disclosure of genetic information is discrimination and privacy. Ironically, “respondents were against the use of genetic testing for underwriting purposes and rejecting applicants because of their genetic makeup” while at the same time they were “also against higher premiums and an increase in taxes to cover the health care cost of individuals with suspect genes” (Borna & Avila, 1999, p. 361).

Closely related to the above described publication, is the research conducted by Armstrong et al. (2003). Again the focus is on genetic information but this time the purposes are, amongst others, to “determine the effect of breast cancer risk information on subsequent life insurance purchases, [and] to characterize the influence of concerns about life insurance discrimination on testing for BRCA1/2 mutations” (Armstrong et al., 2003, p. 360). The conducted study led to the following main findings: “almost one half of the women [...] studied expressed concern about future life insurance discrimination if they underwent genetic testing”, additionally “although concern about insurance discrimination is high, we found no evidence of actual life insurance discrimination among women who participated in risk assessment and genetic test-

ing”, and finally “the decision to increase life insurance coverage is associated with information about the predicted risk of breast cancer” (Armstrong et al., 2003, p. 362). For the purpose of our study, it would be especially interesting to find out if the finding that the “concern about insurance discrimination is an important barrier to the use of genetic testing despite the absence of evidence that such discrimination actually occurs” (Armstrong et al., 2003, p. 363) is transferable to the adoption of wearable devices for underwriting purposes.

None of the above presented articles develop a specific model explaining the willingness of customers to disclose health information to their insurance companies. Nevertheless, the discussion of possible advantages and challenges and the examination of the field of study, provide valuable ideas and relevant insights, as summarized above. In order to be able to extract and transform these into defined constructs, a structured analysis approach was taken. Statements with relevance for the purpose of our work were sorted in a table according to their affiliation with perceived risks and benefits. Subsequently, concepts with an expected influence on the willingness to disclose health information were identified and derived. The table containing the quoted statements and inferred constructs can be found in the Appendix 2.

In summary the examined publications provided evidence for the constructs of invasion of privacy, data accuracy, secondary use, discrimination, manipulation, health motivation, financial benefits, increased fairness, and improved products and services. All of these factors are described in detail in the following.

### 3.5 Research Model

Building on the theoretical background presented above the following preliminary research model was developed (Figure 3.1).

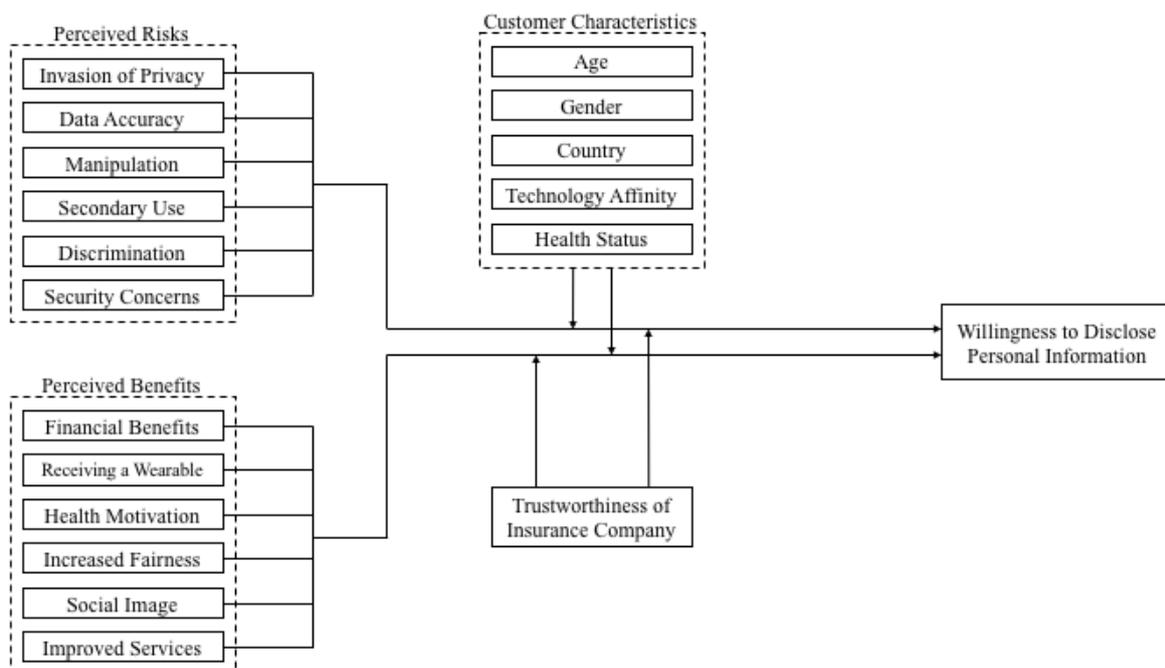


Figure 3.1: Preliminary research model

As the privacy calculus theory (see Section 3.2.2) serves as a foundation for this model, the basic structure distinguishes between constructs forming ‘perceived risks’ and constructs constituting ‘perceived benefits’. The impact of those factors on the willingness to disclose information in the health or life insurance context is moderated by the ‘trustworthiness of the insurance company’ and the individual ‘customer characteristics’.

### 3.5.1 *Perceived Risks*

Dinev et al. (2013) define perceived risk as “the user’s perceived expectation of suffering a negative outcome as a consequence of online disclosure of personal information” (p. 301). A similar view is stated by Smith et al. (2011) who believe that “an individual’s calculation of risk involves an assessment of the likelihood of negative consequences” (p. 1001). Additionally, the authors explain that the negative impact of perceived risks on the intention to disclose personal information was supported by previous studies (Smith et al., 2011). Hence, we follow these conceptualisations of perceived risk as the expected negative outcomes or consequences of disclosing personal information for our study.

According to Beldad, de Jong, and Steehouder (2011) “the risks related to the disclosure of personal data are copious and depend on the amount and type of the personal information disclosed” (p. 222). As health data is generally perceived as very sensitive information (Gao et al., 2015; Malhotra et al., 2004), its disclosure is potentially more risky than revealing other, less sensitive, information (Malhotra et al., 2004). Due to this delicate nature of the data and the expected severe negative impact on the willingness to disclose information, it was decided to treat ‘perceived risks’ as a multidimensional instead of a single-dimensional construct. Anderson and Agarwal (2011) support this decision by stating that “the highly personal and sensitive nature of the information suggest that investigations [...] must pay attention to a broad range of risk elements” (p. 472). While Smith et al. (2011) summarize different types of risks included in the decision process, for example misuse of information or sharing information with third parties, there is a lack of research which clearly identifies, categorizes, and defines risks associated with information disclosure in the specific area of health, or even more precisely with data collected by wearable devices. Therefore, the following subconstructs were developed or derived from the literature in order to increase the accuracy of the research model and tailor it specifically to the requirements and characteristics in the context of the disclosure of health information to insurance companies.

#### 3.5.1.1 *Invasion of Privacy*

Almost all authors concerned with disclosure of health information mention “privacy threats” (Al-Saggaf, 2015), “privacy concerns” (Al-Saggaf, 2015; Meingast, Roosta, & Sastry, 2006), or an “invasion of privacy” (Angst, 2009; Phelps et al., 2000) as a major risk perceived by customers when revealing sensitive data. Only few of them actually define what is meant with these expressions.

Following the definition given in Section 2.2, information privacy refers to “the ability of the individual to control personally information about one’s self” (Stone et al., 1983, p. 460). This implicates that customers expect a loss of control over their information as a consequence of disclosing this data to health insurance companies (Smith et al., 2011). Additional to this control perspective which is strongly related to ‘secondary use’ (see Section 3.5.1.4), another dimension is considered important: “instinctive recoil” (Solove, 2006). As described by Dinev et al. (2013), “many discussions about privacy are targeted toward people’s fears and anxiety to the extent that the expression ‘this violates my privacy’ or ‘my privacy should be protected’ has become more a product of instinctive recoil void of meaning rather than a well-articulated

statement carrying reason and a specific relevance” (p. 296). These fears and anxieties go hand in hand with a general concern about being surveilled, constantly monitored and disciplined by an organization (Christophersen et al., 2015), not least triggered by media coverage. Since the perceived loss of control over one’s information is a more complex phenomenon, it deserves additional attention and is, in all its facets, covered in the separate construct of ‘secondary use’ (see Section 3.5.1.4). Still, it contributes to the undefined, vague, disquieting feeling accompanying the disclosure of health information which forms the perceived risk of an ‘invasion of privacy’.

### **3.5.1.2 Data Accuracy**

The construct of ‘data accuracy’ was derived from the publications by Christophersen et al. (2015) and Al-Saggaf (2015). Christophersen et al. (2015) state that the lack of common standards for wearable devices and the fact that they have not been subject of any validation process “could mean that a person’s health data set might vary depending on which tracking device is used to measure and collect it” (pp. 7-8). “Each device or sensor could potentially collect different data even when measuring the exact same situation” (Christophersen et al., 2015, p. 5). Consequently, the health status assessment based on this data could be inaccurate and not reflecting reality.

This concern is aggravated by the type of information which is collected and subsequently used for the risk assessment. According to Christophersen et al. (2015), “health concerns are reduced to numbers” (p. 1) and cannot account for other external factors. “The readings [...] fail to factor in social, psychological, environmental and physical circumstances, which can all influence [...] the state of a person’s health” (Christophersen et al., 2015, p. 5). The data measured by wearables, such as “number of steps taken, glucose levels, blood pressure, amount of sleep” (Christophersen et al., 2015, p. 5), might not be enough to reliably determine the state of a person’s health. As a consequence, a perfectly healthy customer might be categorized as unhealthy based on inaccurate data and face severe aftereffects due to this wrong assessment (Al-Saggaf, 2015).

Therefore, customers’ concerns about the data accuracy will have a negative influence on the willingness to disclose health information to insurance companies. If they expect an inaccurate measurement and a wrong assessment of their health status due to limited capabilities of the wearable devices, customers are believed to withhold their sensitive information with a higher probability.

### **3.5.1.3 Manipulation**

Another statement made by Christophersen et al. (2015) is that “there is a possibility for manipulation, and the algorithms used can potentially be modified by an organization wishing to change the analytical outcome” (p. 5). The same risk of manipulation is conceivable for the transmitted health data itself. Insurance companies could at any time “re-categorize what is considered healthy and unhealthy” (Christophersen et al., 2015, p. 7), meaning that from one day to the next a person with constant fitness efforts will be assessed differently. Just like the risk of ‘data accuracy’, manipulation could lead to discrimination in further consequence.

The perceived risk of data manipulation or in other words, individual beliefs about the probability of the transmitted data to be manipulated by the insurance company, are therefore expected to have a negative influence on the willingness to disclose sensitive information to the corporations.

#### **3.5.1.4 Secondary Use**

The ‘secondary use’ of revealed information is “when personal information collected for one purpose is subsequently used for a different purpose” (Culnan, 1993, p. 341). As this practice can be associated with a loss of control over one’s data, it is also viewed as an “invasion of privacy” (Culnan, 1993). Nevertheless, ‘invasion of privacy’, as framed by us (see Section 3.5.1.1), primarily refers to instinctive recoil and an undefined, blurry fear constituting general privacy concerns expressed by customers when it comes to the disclosure of data. In contrast, the impact of secondary use seems to be beyond that and the concept is explicitly stated and clearly defined by various researchers (Al-Saggaf, 2015; Borna & Avila, 1999; Christophersen et al., 2015; Smith et al., 1996).

Smith et al. (1996) distinguish between internal and external secondary use. In our context, the internal secondary use of information would involve a scenario in which the insurance company misuses the data by utilizing it not only for underwriting purposes but “in new and unanticipated ways, often without the knowledge of customers” (Al-Saggaf, 2015, pp. 282-283). While today it might not be obvious how this data could be beneficial to the company beyond the initially intended usage, “it is common for organizations to find new uses for data” (Smith et al., 1996, p. 171) in the future.

The external secondary use describes the practice of passing on the data to third parties (Smith et al., 1996). These routines, also called “subsequent disclosures” (Stone & Stone, 1990), might include the sale of data to interested actors not party to the original disclosure, for example other organizations or even potential employers (Al-Saggaf, 2015). Consequently, it paves the way for abuses, for example employment discrimination (Borna & Avila, 1999), and might even have an influence on credit worthiness (Al-Saggaf, 2015). As “electronic personal information has the potential to be easily duplicated and shared” (Al-Saggaf, 2015, p. 283) and as the data on hand is sensitive and potentially useful to many stakeholders, it is especially vulnerable to becoming victim of this kind of misuse.

Secondary use of information, especially unauthorized and without the possibility to dissent, therefore potentially causes “harm to individuals” (Al-Saggaf, 2015, p. 287) with unforeseeable consequences. It was shown that concerns about unauthorized secondary use of data contribute to the perceived risks (Smith et al., 1996) and consequently have a negative influence on the willingness to disclose information.

#### **3.5.1.5 Discrimination**

The fear of being discriminated against as a consequence of disclosing information to health or life insurance companies has been described by Christophersen et al. (2015), Armstrong et al. (2003); Borna and Avila (1999) and Al-Saggaf (2015). They don’t provide an explicit definition of the concept, but describe that the transmitted data enables insurance companies to treat people different from others based on their health information. This procedure corresponds to the definition of discrimination given by CambridgeDictionaries (2016): “treating a person or particular group of people differently, especially in a worse way from the way in which you treat other people, because of their skin colour, sex, sexuality, etc.”. In the context of health or life insurance, discrimination would be based on a person’s health status and his or her assessed risk of becoming diseased or of dying in the near future. The discrimination could take the form of higher insurance premiums (Al-Saggaf, 2015; Borna & Avila, 1999; Christophersen et al., 2015), in other words “a significant adverse premium rating” (Borna & Avila, 1999, p. 355), or cherry-picking of customers by insurance companies (Al-Saggaf, 2015). In detail this means that the ability to get health insurance might be affected to an extent that individual’s “may even be denied insurance coverage” (Al-Saggaf, 2015, p. 283). An adverse premium rating and the exclusion from health or life insurance coverage eligibility

are the most described forms of discrimination in the corresponding literature. Additionally, as a consequence of external use of information, discrimination could also be initiated by third parties and entail different consequences for the individual.

As shown by Armstrong et al. (2003) the “fear of insurance discrimination” (p. 359) is a prevailing concern in the context of genetic information disclosure and it is therefore believed to also have a negative influence on the willingness to reveal sensitive health data collected by wearable devices to insurance companies.

### **3.5.1.6 Security Concerns**

Information security has to be delimited from privacy issues (see Section 2.2) and is defined as “the processes and methodologies which are designed and implemented to protect [...] confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption” (SANS, 2016).

While security concerns are not mentioned in the literature specifically concerning health information disclosure, they are relevant in the wearable device context (Britton, n.d.; Lymberis, 2003). Wearables “are subject to cybersecurity attacks” (Britton, n.d., p. 2) in which unauthorized parties gain access to the data and are able to modify, destroy, or misuse it. As the data considered in our study is collected and transmitted via fitness trackers and other wearable devices, they have to be considered as a risk of information disclosure. Additionally, Wakefield (2013) incorporates “Internet security” in his model, confirming the relevance of security matters in the context of revealing information.

Consequently, the perceived extent to which insurance companies in cooperation with wearable manufacturers manage to guarantee the security of the health data, will affect the willingness to disclose this data to insurance companies.

## **3.5.2 Perceived Benefits**

In the privacy calculus model (see Section 3.2.2) it is argued that the benefits brought by information disclosure may compensate for users’ loss (Dinev & Hart, 2006). People carefully assess and trade-off their perceived risks, as described above, against the perceived benefits and subsequently decide about the disclosure of sensitive information.

According to Sun, Wang, and Shen (2014) perceived benefits thereby include all benefits resulting from disclosing personal information and those vary across different research contexts. Consequently, perceived benefits in health or life insurance differ from perceived benefits in, for example, e-commerce. In general, benefits can be assigned to two categories: tangible or intangible (Beldad et al., 2011). According to Smith et al. (2011), “scholars have identified three major components of benefits of information disclosure including financial rewards, personalization, and social adjustment benefits” (p. 1001). Since there is no literature available identifying accurately all the benefits associated with information disclosure in the field of life and health insurance, we collected and transferred advantages from various sources and different contexts. In total two tangible benefits (financial benefits and receiving a fitness tracker) and four intangible benefits (health motivation, increased fairness, social image, and improved products and services) were identified.

### **3.5.2.1 Financial Benefits**

The “most straightforward benefit” (Hui, Teo, & Lee, 2007, p. 20) and explicitly mentioned advantage of disclosing health information is that the insurance premium for customers might be reduced (Al-Saggaf, 2015; Christophersen et al., 2015). By fulfilling specific fitness requirements individuals can demonstrate their good health condition and save a significant

amount of money. Additionally, some insurers might even offer the possibility to collect extra rewards or, if applicable, avoid fines (Christophersen et al., 2015; VitalityLIFE, 2016). Hui et al. (2007) affirmed that monetary incentives have a positive influence on the disclosure of personal information in the field of e-commerce and it has been widely acknowledged “that people are willing to trade personal information for perceived benefits” (Norberg et al., 2007, p. 101). While Pickard (2014) found out that “consumers exist who are willing to sell their de-identified personal health information” (p. 1), the effect of monetary rewards in the context of non de-identified health information disclosure to insurance companies was not yet tested. Anderson and Agarwal (2011) propose this topic as an area for future exploration and it is expected that the anticipated financial benefits have a positive effect on the willingness to disclose information to insurance companies.

### **3.5.2.2 Receiving a Fitness Tracker**

In addition to the potential monetary rewards offered by insurance companies, the gratuitous distribution of fitness trackers or other wearable devices might serve as an incentive for potential or current customers. If an individual was considering to buy a fitness tracker anyway, he or she might as well buy an insurance policy which comes with a free wearable device. Thereby, the bestowed fitness device serves as an incentive for everyone who assigns a value to it, influencing the willingness to share health information with the insurer in a positive way. While there are no scientific resources available verifying this explicit assertion, the free wearable can be rated as a tangible reward whose positive influence on information disclosure was confirmed (Hui et al., 2007).

### **3.5.2.3 Health Motivation**

An improved awareness about personal health and increased motivation towards a healthier lifestyle is mostly described as a benefit for the insurance company as it potentially leads to cost reductions in the long run (Christophersen et al., 2015). Nevertheless, the encouragement to become healthier might also serve as a benefit for customers themselves.

It is general knowledge that a more active and healthier way of living is preferable over unhealthy lifestyle choices. Still, many people fail to motivate themselves in order to take appropriate actions over longer periods of time (Kranz et al., 2013; Sundar, Bellur, & Jia, 2012). Despite an intrinsic motivation to avoid disease and ill-health, a lack of self-determination is prevailing (Sundar et al., 2012). In the literature concerning fitness and health wearables or associated apps this motivation plays an important role (Handel, 2011; Kranz et al., 2013). Customers specifically state that they acquire a device “to motivate [them] to be a bit more active” (Fritz, Huang, Murphy, & Zimmermann, 2014, p. 491). In the described insurance setting, people not only receive the wearable which allows them to measure their efforts, but the motivational value is even increased with the external insurer component. This external motivation provides for immediate consequences in case the fitness efforts are abandoned. Thus, customers might be willing to trade their personal health information in exchange for an extrinsic motivation to finally meet their fitness goals and to lead a healthier lifestyle.

### **3.5.2.4 Increased Fairness**

The concept of “fair discrimination” is often used as an argument by insurance companies to justify their practice of charging different amounts of money for the same insurance coverage to different people. In other words, “individuals with different risk factors [...] bear different costs for their insurance” (Borna & Avila, 1999, p. 356). The argument holds that insurers should try “to measure as accurately as practicable the burden shifted to the insurance fund by the policyholder and to charge exactly for it, no more and no less. To do so is ‘fair discrimination’... Not to do so is unfair discrimination” (Worham, 1985, p. 361). Therefore, “fair dis-

crimination” also explains the insurer’s increasing wish to get access to more and more personal data in order to properly assess the risk they underwrite (Borna & Avila, 1999).

Thereby, the advantage for the insurance company is pretty obvious, but also for the individual customer an increase in fairness might be highly valuable. Borrowing from the auto insurance environment, it was often perceived as unfair that young, male drivers had to pay significantly more for their insurance coverage than others. The new data-driven approach allows for personalized insurance fees which are believed to be a more appropriate and fairer charge (Troncoso, Danezis, Kosta, Balasch, & Preneel, 2011). Gaulding (1994) confirms this view, stating that “most people would agree, for instance, that automobile insurers should be able to “discriminate” against those who have been convicted for drunk driving or otherwise have poor driving records by charging them higher premiums” (p. 1647). In the health insurance context, a similar reasoning is conceivable: a perfectly healthy customer might wonder why he or she is supposed to pay as much as a person not engaging in any preventive fitness activities and reasonable health choices. Those customers will appreciate an increase in perceived fairness and will therefore be willing to disclose their health information to make it comparable to others (whereas unhealthy individuals might judge this procedure as discrimination, see Section 3.5.1.5).

In this context, it should be mentioned that adverse selection, insurance fraud and moral hazard (see Section 2.3) could also be potentially prevented with the help of disclosed data. Thus, the extent to which customers believe that disclosure of information will contribute to the prevention of these concepts and increase fairness amongst all policyholders in the health and life insurance context, will determine their willingness to reveal that information.

As we are only looking at consequences of customers’ health information disclosure which might be perceived as benefits, the question whether this “fair discrimination” procedure really is fair or morally and ethically correct will not be discussed here.

### **3.5.2.5 Social Image**

According to Yang et al. (2016), “individuals frequently respond to normative social influences to make a favorable impression within a reference group” (p. 259). Individuals “try to be cool, do cool things, and have cool commodities in order to satisfy their desire to be different and express themselves in unique ways” (Kim & Shin, 2015, p. 530). “‘Coolness’ has become an important psychological criterion” (Sundar, Tamul, & Wu, 2014, p. 169). Consequently, social adjustment benefits, defined as “the establishment of social identity by integrating into desired social groups” (Smith et al., 2011, p. 1002), were demonstrated to have an effect on intended disclosure behaviour.

As fitness trackers are often categorized as “fashionable accessories” (Gao et al., 2015, p. 1704) and as “smart watches are viewed not only as time-telling utilitarian tools but also as aesthetic items that express users’ individual characters and values” (Kim & Shin, 2015, p. 530), these devices qualify to demonstrate one’s values and to impress peers. A specific brand name or the visual attractiveness of the device might amplify the effect (Yang et al., 2016).

Kim and Shin (2015) summarize this concept under the term ‘subcultural appeal’ and define it as the “belief that using a certain digital device currently rare in mainstream culture distinguishes its users from the vast majority” (p. 530). But not only the wearable device itself might constitute a benefit for customer’s who care about approval and appreciation from their peers, also the purchase of an innovative, new insurance policy could serve to express the self-conception of an early adopter. Therefore, we extend the concept by Kim and Shin (2015) to also include the acquisition of innovative services. A similar idea is stated by Gao et al. (2015) who call the construct ‘social influence’ and define it as “the extent to which user’s

decision making is influenced by others' perceptions" (p. 1709). Lin and Bhattacharjee (2010) refer to it as 'social image', the "extent to which users may derive respect and admiration from peers in their social network as a result of their IT usage" (p. 165).

Thus, the more a customer expects appreciation and approval from their peers as a consequence of buying such an insurance policy, the more he or she will be willing to reveal personal information.

### **3.5.2.6 Improved, Personalized Products and Services**

Especially in the context of e-commerce, the benefit of personalization, products which are specifically tailored to customer needs, has been highlighted (Beldad et al., 2011). Smith et al. (2011) explain that the value of personalization has been found to override privacy concerns. Accordingly, Chellappa and Sin (2005) refer to personalization as "the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information" (p. 181). But also in the health or life insurance environment the disclosure of information promises to improve and "facilitate the provision of tailored products and services" (Al-Saggaf, 2015, p. 287). Particularly, this means that the insurance coverage could be adjusted in order to perfectly meet the customer's needs or that rewards and special offers are issued according to the actual, individual health status.

The expected comfort and convenience of improved, personalized products and services will therefore positively affect the willingness to disclose the information needed by the insurance company in order to provide these personalized products and services.

### **3.5.3 Moderators**

The linear relationship between the two independent variables, perceived risks and benefits, and the dependent variable, willingness to disclose information to health or life insurance companies, is believed to be moderated by two additional constructs. Based on previous research and logical reasoning customer characteristics, including a variety of attributes, and the trustworthiness of the insurance company are introduced to the model as the main moderators.

#### **3.5.3.1 Trustworthiness of Insurance Company**

Trust or trustworthiness is an important and common concept in the literature concerning information disclosure in an e-commerce environment. Several studies found that the level of trust a consumer has in a website or in a vendor is decisive for the willingness to disclose (Dinev & Hart, 2006; Gefen, Karahanna, & Straub, 2003; Schoenbachler & Gordon, 2002; Wakefield, 2013). The few studies related to the disclosure of health information confirm this important role of trust (Anderson & Agarwal, 2011; Bansal et al., 2010).

Transferring the definition of website trust by Wakefield (2013) to our context, we refer to the trustworthiness of an insurance company as the user's belief that the health or life insurer will keep its promises and commitments, and cares for the interests of the policyholder.

As the perceived benefits can be interpreted as promises from the insurer and as risks indicate that an insurance company does not care about the interest of the policyholder, it was decided to introduce the concept of trustworthiness as a moderating factor. Thereby, it not directly affects the willingness to disclose information but influences the relationship between perceived risks and benefits and the willingness of information disclosure. This moderating role is supported by Culnan and Armstrong (1999) who state that "trust reflects a willingness to assume the risks of disclosure" (p. 106).

### **3.5.3.2 Customer Characteristics**

It is believed that the customers' assessment of the potential consequences of information disclosure, the specific cost-benefit evaluation, and its effect on the willingness to reveal sensitive data, is strongly dependent on individual customer characteristics (Bansal et al., 2010; Pedersen, 1982; Smith et al., 2011). In other words, what is perceived as a risk or a benefit and the following decision to disclose health information to insurance companies is strongly influenced by cultural, social, personal and psychological characteristics. Bansal et al. (2010) summarize those influences under the term "personal dispositions", including personality traits, information sensitivity, health status, prior privacy invasions, risk beliefs, and experience.

For our study the characteristic of 'age' might play a significant role in the decision making process. Regan, FitzGerald, and Balint (2013) find "generational differences and patterns in some attitudes towards privacy" (p. 96) and in general, millennials who grew up with modern technologies are expected to be more prone to the adoption of new devices and services.

An own construct is dedicated to the idea of enthusiasm about innovative services and new technologies as even among same age groups the 'technology affinity' might differ immensely and consequently might influence the readiness to reveal information in this context. In addition, it has to be accounted for the customer's 'gender' as studies show that women are more averse to risk than men (Eckel & Grossman, 2008; Sheehan, 1999). Thus, their assessment of expected risks might significantly differ from men's evaluation. Moreover, the 'country' a customer grew up in and consequently the inherent cultural values were proven to influence the willingness to disclose personal information in previous research (Bellman et al., 2004; Gupta et al., 2010).

In the context of sensitive health information disclosure, the individual 'health status' is of particular importance. It was shown that a poor health status increases the "disutility of disclosing personal health information" (Bansal et al., 2010, p. 146). This confirms the general logic that most probably, a perfectly healthy person is less concerned about the consequences of revealing sensitive data than a person in a bad status of health who might expect to suffer from discrimination as a result of the revealed information.

Therefore, all these customer characteristics are believed to moderate the relationship between perceived risks, perceived benefits and the willingness to disclose health information to insurance companies.

The above described components of our preliminary research model are summarized in Appendix 3.

## 4 Methodology

Scientific research entails two key principles: it not only contributes to a body of knowledge, it also has to conform to the scientific method (Recker, 2013). In this chapter we therefore provide an outline of and motivation for our methodological approach. The research strategy and design, as well as the data collection and analysis process are explained in detail and designated design choices are justified. Additionally, we discuss our approach towards ensuring a high scientific quality and accounting for ethical considerations in this study.

### 4.1 Research Strategy

When choosing an appropriate research strategy for the study on hand, we aimed for a selection which best fits the purpose and research goal of our inquiry and at the same time accounts for the existing limitations of available resources, such as time, costs, and expertise.

#### 4.1.1 Purpose of Research

In general, “the purpose of science is to create scientific knowledge” (Bhattacharjee, 2012, p. 2) or in other words, “the goal of scientific research is to discover laws and postulate theories that can explain natural or social phenomena” (Bhattacharjee, 2012, p. 3). While this general goal exists for all research conducted, specific scientific research projects can be grouped into three categories: exploratory, descriptive, and explanatory (Bhattacharjee, 2012).

The goal or purpose of our research is to explore and explain the phenomenon of Big Data adoption in the insurance industry from a customer perspective, to gain an understanding of the problem field, or more precisely, to assess the public opinion towards the usage of wearable devices for underwriting purposes and to identify and describe “*What factors influence the willingness of customers to disclose sensitive, personal information collected by wearable devices to health or life insurance companies?*” (see Section 1.4). Ultimately, we aim for a research contribution in terms of a model reflecting and explaining the phenomenon.

Consequently, the nature of our research can be described as both explorative and descriptive. The topic on hand is not well researched and there is no deep knowledge about the underlying dynamics in this specific context (see Chapter 3). It is not clear how policyholders feel about disclosing private information to health or life insurance companies or what their attitude towards the usage of wearable devices for underwriting purposes is. Exploratory research in general is defined as the initial research into a hypothetical or theoretical idea and it is thus perfectly suitable in the context of our study, as it “is often conducted in new areas of inquiry, where the goals of the research are: (1) to scope out the magnitude or extent of a particular phenomenon, problem, or behaviour, (2) to generate some initial ideas (or “hunches”) about that phenomenon, or (3) to test the feasibility of undertaking a more extensive study regarding that phenomenon” (Bhattacharjee, 2012, p. 6).

This approach is complemented with a descriptive component, describing what is happening in more detail and expanding the understanding (Sandelowski, 2000). A descriptive study design assists in “making careful observations and detailed documentation of a phenomenon of interest” (Bhattacharjee, 2012, p. 6) and it “examines the what, where, and when of a phenomenon” (Bhattacharjee, 2012, p. 6). Therefore, the identification and explanation of the factors influencing the willingness to disclose health information to insurance companies can be attributed to the descriptive purpose of our study.

#### *4.1.2 Research Philosophy*

According to Saunders, Lewis, and Thornhill (2011), it is important to clarify the philosophical assumptions taken regarding the “relationship between [the nature of] knowledge and the process by which it is developed” (p. 108). In our thesis we are applying an interpretive approach or, in other words, are basing our research on an interpretivist epistemology in order to find an answer to our research question.

Interpretivism is “a research paradigm [...] that is based on the assumption that social reality is not singular or objective, but is rather shaped by human experiences and social contexts (ontology), and is therefore best studied within its socio-historic context by reconciling the subjective interpretations of its various participants (epistemology)” (Bhattacharjee, 2012, p. 103). This is contrasting the positivist idea in which reality is assumed to be objective, simple, and fixed and that it exists “independent of human consciousness and perception and rests on order consisting of strict, natural laws” (Recker, 2013, p. 67). The interpretive approach is instead grounded in a social-constructionist view of reality “that stresses an ontology prescribing that phenomena are bound within and shaped by their social and historical context and cannot be isolated from that context” (Recker, 2013, p. 89). “The world is produced and reinforced by humans through action and interaction” (Orlikowski & Baroudi, 1991, p. 14). Therefore, “interpretive researchers view social reality as being embedded within and impossible to abstract from their social settings, they “interpret” the reality though a “sense-making” process rather than a hypothesis testing process” (Bhattacharjee, 2012, p. 103). Interpretive research is consequently “well-suited for exploring hidden reasons behind complex, interrelated, or multifaceted social processes”, “helpful for theory construction in areas with no or insufficient a priori theory”, and “appropriate for studying context-specific, unique, or idiosyncratic events or processes” (Bhattacharjee, 2012, p. 105).

As we strongly believe that the individual decision whether to disclose sensitive information or not is highly dependent on the context or social settings, it is best studied in an interpretive way. Other possible paradigms, such as positivist or functionalist, were overruled as the interpretivist epistemology best fits our research study and our personal preferences.

#### *4.1.3 Research Method and Approach*

Qualitative research is well suited for exploratory and descriptive, as well as interpretive research. It allows for the uncovering of meanings and the in-depth investigation of a specific phenomenon in a real-life context (Recker, 2013). Following this reasoning, we select a qualitative approach for our study.

Qualitative research is next to quantitative approaches the most popular research methodology in information systems research (Recker, 2013) and includes developing a complex as well as comprehensive understanding of the problem area (Creswell, 2012). Recker (2013) highlights again that it is especially suitable for research “where a phenomenon is not yet fully understood, not well researched, or still emerging” (p. 88). It enables and assists researchers to study social and cultural phenomena in context, ultimately offering “explanations for why the phenomena occurred the way they do” (Recker, 2013, p. 88). As our research question is concerned with what makes people disclose health information to health or life insurance companies, this qualitative approach is the best fit for our research.

A quantitative approach, “characterised by an emphasis on quantitative data” (Recker, 2013, p. 66), thus numbers, was discarded for various reasons. Firstly, it is mostly associated with a positivist philosophy and deductive reasoning (Bhattacharjee, 2012). A deductive approach implies “starting with a theory and testing theoretical postulates using empirical data” (Bhattacharjee, 2012, p. 35), thereby building on a set of premises and assumptions. We believe that the existing research is too limited and weak to derive a profound theory which could be tested with quantitative methods. Additionally, the adoption of a quantitative approach would eliminate the possibility of establishing new influencing factors, producing incomplete results or lacking alternative explanations. We aim at a more substantiated and grounded model development based on a qualitative strategy. Our designated knowledge contribution is the research model, developed on the basis of a structured and comprehensive literature review, and refined with the help of opinions and views of the customers themselves, gathered in various face-to-face interviews. Only in a next step, left for future research, the testing of the developed research model with quantitative methods would be appropriate and valuable. This approach is pictured in Figure 4.1.

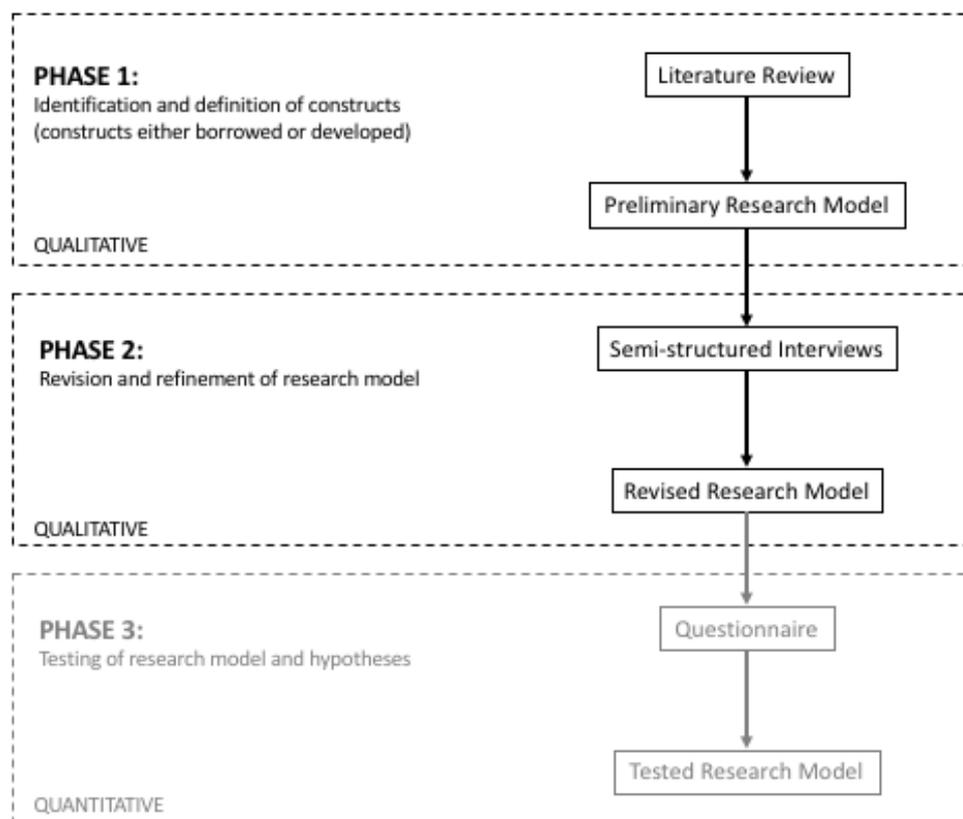


Figure 4.1: Research approach

By following a qualitative research approach, we study the phenomenon in its natural setting (Alvesson & Sköldbberg, 2009) in order to “understand the meaning of a phenomenon from the perspective of the participants” (Merriam, 2002, p. 12). We try to discover and explore the customers’ views, perceptions and opinions to finally conclude which factors are influencing their willingness to disclose sensitive information to their health or life insurance companies.

This research approach already implies an inductive reasoning which is complemented by a deductive element. We follow the idea of a “bottom-up analysis of data and the build-up of patterns, themes, and concepts into increasingly abstract units from the data” (Recker, 2013, p. 88). This approach seems reasonable, not only because qualitative research is in general mostly associated with inductive analysis, but also because we do not have in-depth knowledge about the phenomenon to be investigated. According to Recker (2013), “induction can be thought of as trying to infer theoretical concepts and patterns from observed data or otherwise known facts” (p. 31). It is more oriented towards theory-building, while deduction helps to test theory (Bhattacharjee, 2012).

Thus, developing our research model based on the collected data and thereby moving from the specific to the general can be described as an inductive approach. Nevertheless, as stated by Bhattacharjee (2012) “inductive and deductive reasoning go hand in hand in theory and model building” (p. 15). Therefore, the process of narrowing down the “tentative explanations to the most plausible explanation” (Bhattacharjee, 2012, p. 15), with the help of the gathered insights from the interviews (see Phase 2 in Figure 4.1), can be described as a deductive element complementing our research design.

## 4.2 Data Collection and Analysis

In order to collect the most meaningful and valuable data for our research, we decided to conduct qualitative, semi-structured, face-to-face interviews. Amongst other techniques of gathering qualitative data, such as observation and documentation, interviewing is certainly the most prominent form (Bhattacharjee, 2012; Recker, 2013). Interviews generate subjective understanding and “multiple individual perspectives regarding the phenomenon [are developed and exploited] to arrive at a comprehensive, multi-faceted description or conceptualisation. This conceptualisation can then generate interpretive understanding” (Recker, 2013, p. 90). Thus, the conduction of interviews supports the descriptive nature of our research as they “are used to provide a rich description of a phenomenon as perceived by individuals” (Recker, 2013, p. 90). Interviews can also have “hypothesis-testing purposes” (Kvale, 2007, p. 38), therefore they help testing the appropriateness of our developed research model. Furthermore, they assist in proposing new theory constructs, fulfilling an explorative purpose (Recker, 2013) and complementing our research in a meaningful way.

In addition, we utilized the technique of documentation. Documentation includes internal and external documents which can be structured, semi-structured, as well as unstructured (Recker, 2013). Besides our extensive literature review, we consulted insurance companies’ websites in order to receive public information about what insurance plans they offer, what specific characteristics they entail and how they handle private data. Additionally, blog posts and newspaper articles were gathered and checked for public opinions and further insights into the phenomenon of interest. This information helped to develop our background knowledge of the phenomenon and was used to inform our interviews.

In contrast, the technique of observation is not appropriate in the context of our study. As we are investigating the willingness, thus the intention, to disclose information the actual behaviour is not examined. This decision was taken as the agreement to disclose information is made in the form of a purchase contract which is signed in the insurance company itself, almost impossible to observe for a researcher. Furthermore, as the preceding decision process is a stream of thoughts including various considerations and an assessment of the situation, this as well cannot be monitored. Even the dealing with wearable devices does not require any direct interaction which could be inspected. Therefore, interviewing, with a reinforcing documentation, is the best suitable technique for gathering data in our field of study.

Having chosen the research approach, design, and our data collection technique, we decided to follow the seven stages of an interview inquiry as described by Kvale (2007) and depicted in Figure 4.2.



**Figure 4.2: Seven stages of an interview inquiry (according to (Kvale, 2007))**

#### 4.2.1 *Thematizing*

According to Kvale (2007) this stage of the process is concerned with the ‘why’ and ‘what’ of an investigation and includes the purpose of the inquiry as well as the conception of the theme. The question of ‘why’ we are investigating our specific problem area is answered in Section 1.3 and our conceptualization, including the preliminary research model, is extensively developed in Chapter 3.

#### 4.2.2 *Designing*

Always focused on “obtaining the intended knowledge and taking into account the moral implications” (Kvale, 2007, p. 34), we carefully designed our interview study. We therefore chose to conduct semi-structured interviews “which are open to the interviewees’ decisions about what is important and relevant to talk about, and how they choose to express themselves” (Schultze & Avital, 2011, p. 2). As we were specifically looking for factors influencing the individual willingness to disclose information collected by wearable devices to health or life insurance companies, this approach grants the possibility to freely explore the interviewees’ own perception of the matter without interference and to discover what risks and benefits they perceive. Generally, the openness of the approach allows new ideas to be brought up.

At the same time, the interview guide prepared beforehand (see Appendix 4), also granted the ability to inquire specific risks and benefits not mentioned by the respondent, but present in our research model. By following the framework of specific topics which we wanted to explore, we managed to focus the interviews on the important matters without constraining the answers. Instead of rigorously asking question after question, the thematic blocks were used to guide the interviews, still allowing the flexibility to divert, to change the order of the questions when appropriate, to follow up leads, clear up inconsistencies, and to further investigate raised issues in detail (Bryman, 2004). According to Recker (2013), other advantages of semi-

structured interviews are that “they are less intrusive to those being interviewed” (p. 91), they “encourage two-way communication” (p. 91), and “they can be used to confirm what is already known whilst at the same time providing the opportunity for learning” (p. 91). Additionally, “when individuals are interviewed personally and in a conversational rather than structured manner they may more easily discuss sensitive issues” (Recker, 2013, p. 91). Thus, semi-structured interviews constitute the best means in order to provide us with valuable answers, insights and ideas to our research question. This type of interview “is used the most in qualitative research in information systems” (Myers & Newman, 2007, p. 4).

Based on our research purpose (see Section 1.4), the theoretical background (Chapter 3), and the developed preliminary research model (see Figure 3.1) we designed the interview guide. While the complete guide can be found in Appendix 4, it can be divided into seven parts.

**Part 1: Introduction.** The interviewing process is opened with an introduction of ourselves and by learning the names of the interviewees. While trying to establish a friendly, open atmosphere, we collect the signature on the informed consent form (Appendix 5) and again inform about voluntary participation, confidentiality and confirm if it is ok to record the conversation. Subsequently, we explain what the interview is about and give a detailed introduction and description about the usage of wearable devices for underwriting purposes in the context of health and life insurance.

**Part 2: Consumer Characteristics.** Starting the actual questioning part of the interview, we begin with some easy, closed questions concerning the consumer characteristics. While the information is needed for subsequent analysis, the intention behind beginning with these questions is to break the ice and get the interview going.

**Part 3: Attitude.** The main part of the interview starts with the assessment of the general opinion of the interviewee towards the described phenomenon.

**Part 4: Perceived Risks and Benefits.** This most important section of the interview provides the opportunity to learn about the risks and benefits as perceived by the interviewee. By asking very open questions, we aim at gathering valuable insights without influencing the respondents. Only in a second step, more precise questions concerning concepts not mentioned by the interviewee will be asked. The amount of those questions depends on the extent and scope of the interviewee’s answer to the open question at the beginning.

**Part 5: Willingness to Disclose Information.** To assess the actual willingness of the interviewee to reveal sensitive information to health or life insurance companies after evaluating all the risks and benefits, we specifically ask them about their future intention.

**Part 6: Moderators.** In order to gain some valuable insights about moderating affects of certain constructs we included additional questions concerning their health status and trust towards the insurance company.

**Part 7: Closing.** We end the interview with a general question if the participant wants to add anything or if he or she thinks that there are any areas we did not cover and they would like to discuss. Finally, we thank the interviewees for their time and for participating.

As the focus of the research is to determine factors influencing the willingness to disclose information, the majority of questions were very open ‘what’ and ‘how’ questions rather than ‘why’ questions. We strived to keep the questions simple and easily understandable, to enable a smooth interaction and to gather as many valuable insights as possible (see Table 4.1).

**Table 4.1: Overview of the interview questions**

Nr.	Question	Referring to
Q1	How old are you?	Consumer characteristics (Age)
Q2	Where are you from? Where have you lived most of your life?	Consumer characteristics (Country)
Q3	Do you have a health or life insurance?	Consumer characteristics (Insurance)
Q4	Do you own a wearable device?	Consumer characteristics (Technology affinity)
Q4.1	<i>If yes:</i> Do you wear it regularly? <i>If no:</i> Have you ever considered buying a wearable or would you consider wearing one if it was given to you for free?	Consumer characteristics (Technology affinity)
Q5	Would you describe yourself as technology affine, meaning that you always have the newest gadgets and devices?	Consumer characteristics (Technology affinity)
Q6	Would you describe yourself as generally concerned about your privacy?	Consumer characteristics (Privacy)
Q7.1	What is the first thing that comes to your mind when you hear of this new concept of insurance?	Attitude
Q7.2	Do you think it is a good idea to use wearables in the context of health or life insurance?	Attitude
Q8	Can you think of any negative consequences resulting from disclosing your information to insurance companies? <i>Or</i> Do you think there are any risks affiliated to disclosing health information to insurance companies? <i>Followed by:</i> What do you think are the risks of disclosing your health information to insurance companies?	<b>Perceived Risks</b>
	IF NOT MENTIONED BEFORE:	
Q8.1	Do you think an invasion of privacy could be a concern?	Invasion of Privacy (IP)
Q8.2	Do you think the accuracy of the data collected by the wearable could be a problem?	Data Accuracy (DA)
Q8.3	Do you think there might be a risk that the insurance company manipulates your data?	Manipulation (MP)
Q8.4	Do you think it is probable that the insurance company gives away your data to a third party?	Secondary Use (SU)
Q8.5	Do you think these new approach towards insurance could lead to discrimination?	Discrimination (DM)
Q8.6	Do you think there are any security concerns affiliated with collecting data with a wearable and sending it to the insurance company?	Security Concerns (SC)
Q9	For what reason would you disclose your health data to insurance companies? <i>Or</i> Do you think there are any benefits affiliated with the disclosure of health information to insurance companies? <i>Followed by:</i> What do you think are the benefits of disclosing your health information to insurance companies?	<b>Perceived Benefits</b>

	IF NOT MENTIONED BEFORE:	
Q9.1	Do you think that financial benefits could positively influence your willingness to disclose your information?	Financial Benefits (FB)
Q9.2	Would receiving a fitness tracker constitute an incentive for you, influencing you in a positive way?	Receiving Fitness Tracker (FT)
Q9.3	Do you think the new approach would motivate you to be more active and healthy? Would you want to be motivated?	Health Motivation (HM)
Q9.4	Do you think the new policies would increase fairness amongst all policyholders?	Increased Fairness (IF)
Q9.5	Do you think your friends or peers would approve or even admire you for buying an insurance policy as described?	Social Image (SI)
Q9.6	Would you expect benefits in terms of improved services by the insurance company as a result of disclosing your information?	Improved Services (IS)
Q10	Considering all these aspects, would you be willing to disclose your health information to an insurance company?	Willingness to Disclose
Q11	How would you describe your health status? Do you have any severe illness?	Consumer characteristics (Health Status)
Q12	Do you think your opinion towards the issue of wearables in the insurance context would change if you were in a different state of health?	Moderating Effect of Health Status
Q13	Do you trust your insurance company? <i>Or:</i> Do you trust insurance companies in general?	Trustworthiness
Q14	Is there anything you would like to add in terms of the adoption of wearables for health and life insurance that you feel we should consider?	Wrap up

The interviews and the analysis were regarded as an iterative process, giving us the opportunity to “learn throughout the investigation” (Kvale, 2007, p. 42) and to slightly modify, adjust and improve individual questions or the introduction about wearable devices in health and life insurance during the course of the research.

#### 4.2.3 Interviewing

A total number of nine face-to-face interviews was conducted over a period of one week. When deciding how many interviews to conduct and whom to interview, several aspects were taken into consideration. In general, there is no definite answer to the question how many subjects need to be interviewed (Kvale, 2007). Instead, Kvale (2007) points out the trade-off between too many or too few interviews: “If the number of subjects is too small, it is difficult to generalize and not possible to test hypotheses of differences among groups or to make statistical generalizations. If the number of subjects is too large, there will hardly be time to make penetrating analyses of the interviews” (p. 43). Bhattacharjee (2012) confirms this view by stating that “too little data can lead to false or premature assumptions, while too much data may not be effectively processed by the researcher” (p. 105). Thus, we followed Kvale (2007) and his advice to “interview as many subjects as necessary to find out what you need to know” (p. 43). After conducting nine interviews we realised that no new concepts were brought up and that no additional insights could be gained. A point of saturation was reached. Consequently, we decided to stop the interviewing process at this point and to concentrate on analysing the gathered data. Using this procedure, we could optimize the ratio of gained insights and effort needed for the processing of the collected data, given the limited time frame

of the study. The nine conducted interviews constitute a compromise between obtaining a representative sample and not overstraining the available resources.

The selection of interviewees followed a theoretical sampling strategy. Therefore, respondents were selected “based on theoretical considerations such as whether they fit the phenomenon being studied [...], whether they possess certain characteristics that make them uniquely suited for the study [...], and so forth” (Bhattacharjee, 2012, p. 104). “Convenience samples and small samples are considered acceptable in interpretive research as long as they fit the nature and purpose of the study” (Bhattacharjee, 2012, p. 104). Additionally, according to Seale (1999), selecting appropriate and representative subjects is crucial to achieve transferability (see Section 4.3.2). Considering the fact that our study takes on a worldwide customer perspective, no expert opinions were needed and the respondents did not have to fulfil specific criteria. Instead, the only requirement was that the respondents were able to sign an insurance contract and thus to have an age of 18 years or older. Our theoretical considerations included a coverage as wide as possible of current or future customers of health or life insurance companies. In order to derive valuable insights, we strived for a sample balanced in terms of gender, covering various age groups and including people from different countries of the world. We wanted to assess the opinions of both potential and actual customers, wearable device owners and less technology affine humans, as well as people in a good state of health and those in a less fortunate position. The goal was to provide an as comprehensive picture of influencing factors of the willingness to disclose information to health or life insurance companies as possible.

The final sample includes four male and five female interviewees, covering an age span of 39 years and originating from six different countries. Two respondents did already own a wearable device and five participants called themselves technology affine. Two interviewees can be described as above average sporty while one was in a severe state of health. The complete sample with its main characteristics is illustrated in Table 4.2.

**Table 4.2: Key characteristics of respondents**

Interviewee	Age	Gender	Country	Insurance	Wearable	Technology affine	Health status
Respondent 1 (RP1)	47	Male	Sweden	yes	yes	yes	Good, very sporty
Respondent 2 (RP2)	62	Female	Sweden	no	no	no	Okay, not that sporty
Respondent 3 (RP3)	24	Female	Scotland/ Sweden	no	no	no	Okay, not that sporty
Respondent 4 (RP4)	23	Female	Sweden	yes	yes	no	Good, very sporty
Respondent 5 (RP5)	33	Male	Sweden	yes	no	yes	Good, moderately sporty
Respondent 6 (RP6)	23	Female	Albania	yes	no	no	Good, moderately sporty
Respondent 7 (RP7)	35	Female	India	yes	no	yes	Severe illness
Respondent 8 (RP8)	27	Male	South Africa	yes	no	yes	Good, not that sporty
Respondent 9 (RP9)	32	Male	Lebanon	yes	no	yes	Not good, not that sporty

After selecting the appropriate respondents, the actual interviews were conducted in the period of 25<sup>th</sup> of April till 29<sup>th</sup> April 2016 (see Table 4.3). The role of the interviewer was taken alternating by the two researchers. Thereby, we could counteract individual interviewer bias by employing researcher triangulation. All interviews were conducted in English. The locations were chosen according to the interviewee's preferences and consequently, some were conducted in the respondents' houses, some in their workplace and some in a neutral environment, the university. This contributed to our effort to make the interview situation as comfortable as possible, to avoid a feeling of artificiality and to make the researcher feel less a stranger to the interviewee. Furthermore, we tackled the challenge of reflexivity, meaning that "the interviewee responds with what the interviewer would like to hear" (Recker, 2013, p. 90) and other potential biases (also described in Section 4.3), by carefully choosing the wording of our questions. In order to "probe the respondent to elicit a more thoughtful, thorough response" (Bhattacharjee, 2012, p. 80), we engaged in silent probe, "just pausing and waiting" (Bhattacharjee, 2012, p. 80), as well as encouraging the respondent with occasional "okay"s or specifically asking for elaboration, such as "can you elaborate on that?" (Bhattacharjee, 2012, p. 80). At all times we tried to avoid that preconceptions and our previous understanding of the phenomenon tainted the nature of our inquiry and questions.

**Table 4.3: Overview of interviews**

Interview	Date and Time	Duration	Location	Method	Interviewer
1	26.04.16; 10:00	46:08 min	Interviewee's workplace	Face-to-face	Annina
2	26.04.16; 18:30	22:14 min	Interviewee's living room	Face-to-face	Ali
3	26.04.16; 19:30	20:06 min	Interviewee's living room	Face-to-face	Annina
4	27.04.16; 09:00	21:49 min	University	Face-to-face	Ali
5	27.04.16; 10:30	23:17 min	University	Face-to-face	Annina
6	27.04.16; 11:30	22:00 min	University	Face-to-face	Annina
7	28.04.16; 14:00	27:48 min	University	Face-to-face	Ali
8	28.04.16; 19:00	18:40 min	Interviewee's living room	Face-to-face	Annina
9	29.04.16; 12:00	21:55 min	Interviewee's living room	Face-to-face	Ali

#### 4.2.4 Transcribing

Taking into account the natural limitations of human memories, it is no surprise that the transcription of conducted interviews has become a standard procedure. "Transcribing the interviews from an oral to a written mode structures the interview conversations in a form amenable to closer analysis, and is in itself an initial analysis" (Kvale, 2007, p. 94).

A requirement for transcribing is that the interview was recorded in the first place. Therefore, all conversations were, with permission of the interviewees, digitally voice recorded, allowing the interviewer to concentrate on the topic and the dynamics of the interview (Kvale, 2007). Afterwards, the recordings were transferred and stored on our computers so that they were available for the transcribing purpose, but also for later re-listening.

As the interview transcriptions tend to be regarded as the "solid rock-bottom empirical data of an interview project" (Kvale, 2007, p. 92), the quality of transcription is of great importance. Transcribing a face-to-face conversation to a written form is an abstraction and involves a "series of judgements and decisions" (Kvale, 2007, p. 92). Therefore, even if no standard rules exist (Kvale, 2007), the amount and form of transcribing should be chosen wisely, de-

pending on factors such as the nature of the material, the purpose of the investigation, and availability of time, money, and a typist (Kvale, 2007). We chose a written over a verbatim oral style, not specifically indicating pauses, laughter, intonation or other contextual aspects and not noting ‘mh’-s and the like. Due to the fact that no linguistic analysis was conducted, this form of transcribing seemed sufficient and appropriate in the context of our research as it reduces the complexity, and facilitates analysis. All interviews were conducted in English, thus no further translation efforts had to be made.

As the transcribing was performed by us, we were able to benefit not only in terms of learning about our own interview style and improving for subsequent interviews, but also in terms of a reawakening of aspects and parts of the interview situation, growing familiar with the data and providing a starting point for the interview analysis (Kvale, 2007; Lapadat & Lindsay, 1999; Park & Zeanah, 2005).

All transcriptions were provided in a table format (see Appendix 6), perfectly preparing and supporting our analysis approach which is described in the following.

#### 4.2.5 Analyzing

In order to understand and make sense out of the data collected during the interviews, a comprehensive analysis is conducted. Following Kvale (1996) we acknowledge that it is “too late to start thinking of analysis after the interviews have been conducted and transcribed” (p. 101) and realize that in qualitative research “data analysis and collection can be highly interwoven or even dependent on another” (Recker, 2013, p. 92). Therefore, we already thought about the method of analysis in advance of interviewing. This gave us the opportunity to already engage in analysis during the interview situation itself. In an interpretation ‘as you go’, the interviewer can “attempt to confirm or reject his or her interpretations during the interview” (Kvale, 2007). For example, the interviewer tried to condense and interpret the meaning of the interviewees answer, sending the meaning back to the interviewee who then had the opportunity to confirm or disconfirm the interviewer’s interpretations. Ideally, the process “continues until there is only one possible interpretation left” (Kvale, 2007). Thereby, the subsequent analysis becomes much easier and “rests on more secure ground” (Kvale, 2007).

Right after conducting the interviews we wrote short and informal memos, a subjective commentary or reflection about important observations and about what was happening at the time or place of the interview (Recker, 2013). “Memos can be a useful tool to guide the further research process, and can guide the identification of concepts and themes” (Recker, 2013, p. 93).

While data analysis is defined as “the search for patterns in data and for ideas that help explain why those patterns are there in the first place” (Bernard, 2011, p. 452), there are no rules or standard methods to “arrive at essential meanings and deeper implications of what is said in an interview” (Kvale, 2007, p. 103). Still, some tools or techniques of analysis, such as coding, do exist and have been proven to facilitate the analysis process.

Since our data analysis was guided by the research question ‘*What factors influence the willingness of customers to disclose sensitive, personal information collected by wearable devices to health or life insurance companies?*’ the two primary goals of the analysis were (1) to confirm or disconfirm the influence of factors contained in our preliminary model based on the literature review, and (2) to discover and identify other, new concepts with an influence on the

willingness to disclose information which we did not consider beforehand. Therefore, the focus of the analysis was on meaning and not on the language or linguistic form.

We printed all the transcriptions and read each interview as a whole in order to gain a general overview of our data. Especially, the assessment of the overall attitude and opinion of the respondent towards the topic on hand could be assessed in this way. Only in a next step, we employed a coding scheme (see Table 4.4), going through the transcriptions line by line, highlighting statements which specifically referred to constructs defined in our preliminary research model with different colours (see Figure 4.3). Coding or “assigning tags or labels as units of meaning to pieces or chunks of data collected” (Recker, 2013, p. 92), not only helps to sort through the mass of data, but also enables the exact assessment and count of how many respondents mentioned a particular risk or benefit. These findings were captured in a structured way using a table (see Table 5.1 and 5.2). We thereby carefully distinguished between concepts brought up without interference of the interviewer and factors which were acknowledged as a risk or benefit, but only in response to the interviewer’s inquiry.

In a third and final walkthrough, we attentively looked for additional statements (coding units), forming factors with an influence on the willingness to disclose health information to insurance companies which we did not include in our considerations beforehand. This method corresponds to open coding as described by Corbin and Strauss (1990) “aimed at identifying concepts or key ideas that are hidden within textual data, which are potentially related to the phenomenon of interest” (Bhattacharjee, 2012, pp. 113-114).

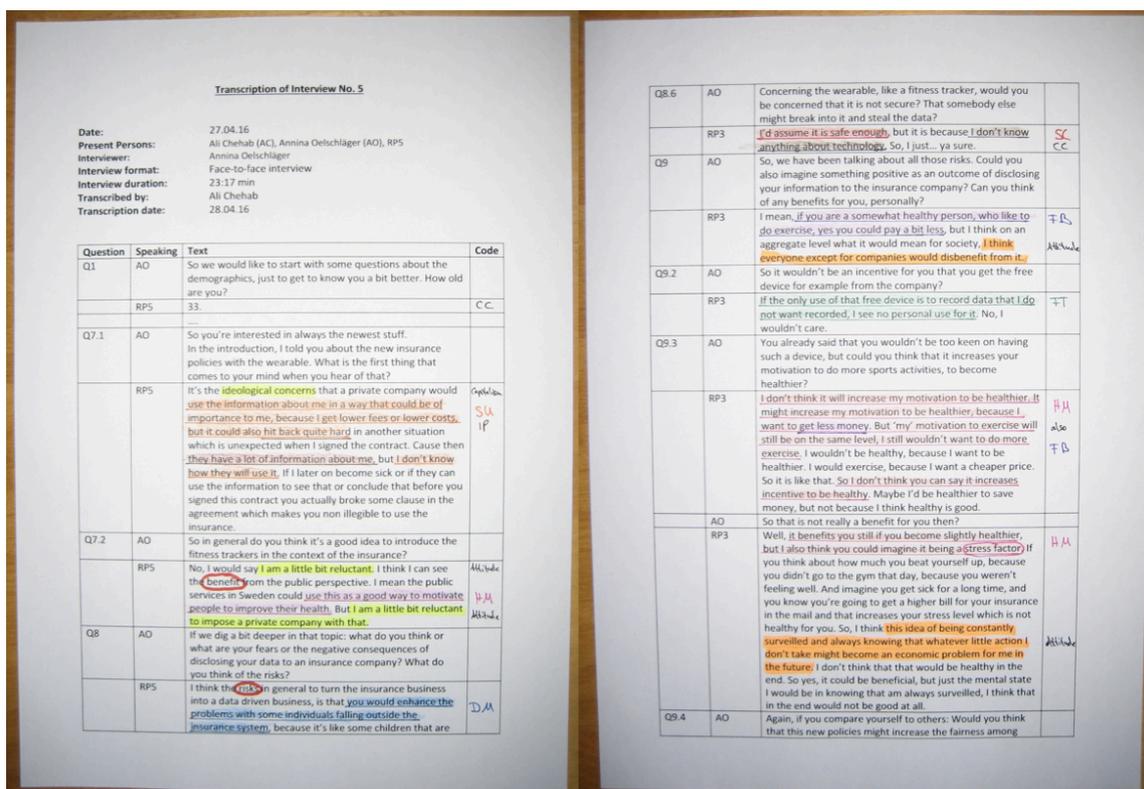


Figure 4.3: Example of colour coding

By individually analysing the transcriptions we again engaged in researcher or investigator triangulation gaining multiple perspectives on a single reality, preventing the risk of being exposed to each others opinions and biases (Seale, 1999). Afterwards, we collaborated and consolidated our insights and findings. By discussing our ideas, comparing our results with each other and merging them to a single picture, we arrived at a profound analysis of our collected data.

**Table 4.4: Coding scheme**

Perceived Risks	Code	Perceived Benefits	Code	Moderators	Code
Invasion of Privacy	IP	Financial Benefits	FB	Trust of Insurance Company	TI
Data Accuracy	DA	Receiving a Fitness Tracker	FT	Customer characteristics	CC
Manipulation	MP	Health Motivation	HM		
Secondary Use	SU	Increased Fairness	IF		
Discrimination	DM	Social Image	SI		
Security Concerns	SC	Improved Services	IS		

#### 4.2.6 Verifying and Reporting

Finally, the validity, reliability and generalizability of the interview findings have to be ascertained. Subsequently, the methods applied and the findings gathered have to be communicated “in a form that lives up to scientific criteria, takes the ethical aspects of the investigation into consideration and that results in a readable product” (Kvale, 2007, p. 33). The approach of an appropriate verification and towards high standard reporting is described in the following Section 4.3.

### 4.3 Research Quality

The quality of research is a highly relevant, crucial and much discussed matter (Bhattacharjee, 2012; Lincoln, 1995; Recker, 2013; Tracy, 2010).

While in quantitative research the main criteria for quality, internal validity, external validity (generalizability), reliability, and objectivity, are commonly acknowledged and applied, they are not directly transferable to qualitative or interpretative research (Bhattacharjee, 2012). Instead a discussion about the appropriateness of these criteria emerged and other analogues ones were developed, particularly for the application in qualitative research. These criteria include: credibility, transferability, dependability, and confirmability (Bhattacharjee, 2012; Frambach, van der Vleuten, & Durning, 2013). We are going to elaborate on each one briefly and additionally outline the role of ethics in scientific inquiry and how we confirm to ethical standards in our research.

#### 4.3.1 Credibility

Credibility as the counterpart of internal validity is defined as “the extent to which the study’s findings are trustworthy and believable to others” (Frambach et al., 2013). The need for

“trustworthiness, verisimilitude, and plausibility” in qualitative research is “noted by many qualitative scholars” (Tracy, 2010, p. 842). In order to achieve credibility for our research study we engaged in data triangulation. By conducting a thorough literature review, by including other documents such as newspaper articles and blog posts in our considerations, and finally by collecting data from customers themselves, we draw on multiple data sources. Additionally, as already stated above, we make use of investigator triangulation as at all times two authors and researchers were involved in the conducting of the research, the interviews and the data analysis. By independently working on the matter, followed by a discussion and consolidation, we increase the credibility of the study. Finally, our approach does also include a triangulation of theories as multiple different concepts were incorporated in our preliminary research model.

#### *4.3.2 Transferability*

In quantitative research external validity or generalizability refers to “the extent to which the results can be generalized from the research sample to the population” (Frambach et al., 2013). In qualitative research transferability, or “the extent to which the findings can be transferred or applied in different settings” (Frambach et al., 2013), is harder to achieve and usually requires the execution of other studies in different contexts (Bhattacharjee, 2012). Nevertheless, we make use of thick descriptions in order to make the findings as meaningful to others as possible. We describe them and their context in detail, providing as many specific aspects as feasible. Additionally, we give a thorough explanation for our sampling strategy (Section 4.2.3) and discuss the findings resonance with literature from different contexts.

#### *4.3.3 Dependability*

Dependability is defined as “the extent to which the findings are consistent in relation to the contexts in which they were generated” (Frambach et al., 2013) and comparable to the criterion that quantitative research should lead to the same results every time the operation of a study is repeated in equal settings (Bhattacharjee, 2012; Recker, 2013).

In order to increase the dependability of our study, we collected data, and conducted interviews, until no new themes emerged and consequently a point of saturation was reached. We were always open and flexible towards emerging ideas concerning the research topic. The process of data collection and analysis can furthermore be described as iterative as we continuously analysed and re-examined the data based on insights gained during previous stages of the analysis.

#### *4.3.4 Confirmability*

Another important criterion for the quality of qualitative research is “the extent to which the findings are based on the study’s participants and settings instead of researchers’ biases” (Frambach et al., 2013). In the first research phase this was achieved by actively searching in the literature for “evidence that disconfirms the findings” (Frambach et al., 2013). As such evidence could not be found, we furthermore engaged in a discussion about our findings with peers and actively reflected on our role and influence as researchers.

Moreover, we especially accounted for common biases during the interviews and their analysis, such as experimenter's bias, sampling bias, social desirability bias, or response bias. By engaging in researcher triangulation and by self-reflection, we tried not to be guided by our prior assumptions or expectations and instead proactively looked for information disconfirming our preliminary hypothesis or illustrating discrepancies. Moreover, we aimed at covering a sample as diverse as possible, including many different characteristics, and tried to establish a positive atmosphere, motivating the respondents to be honest and not adjust their responses to what they think is the appropriate answer in this context.

Additionally, a detailed documentation of the decisions and steps taken, as described in this chapter, is believed to increase the confirmability (Frambach et al., 2013).

Next to those quality criteria of qualitative research, the conformance with ethics is an important aspect while conducting scientific research.

#### 4.3.5 Ethics

Ethics are defined as “conformance to the standards of conduct of a given profession or group” (Bhattacharjee, 2012, p. 137). They determine “the principles of right and wrong conduct” (Recker, 2013, p. 141). Therefore, ethical behaviour is defined as “those actions that abide by rules of responsibility, accountability, liability, and due process” (Recker, 2013, p. 141).

Just like any other community, “science as a profession requires ethical standards as to what is acceptable and unacceptable behaviour in the conduct and publication of research” (Recker, 2013, p. 141) and scientists are generally expected to comply with acceptable behaviours in the professional conduct of science. “For instance, scientists should not manipulate their data collection, analysis, and interpretation procedures in a way that contradicts the principles of science or the scientific method or advances their personal agenda” (Bhattacharjee, 2012, p. 137). Still, it has to be said that ethical norms may vary from one society or culture to another and that what is “unethical may not necessarily be illegal” (Bhattacharjee, 2012, p. 137).

According to Bryman (2004) “a criterion of the ethical integrity of an investigation is its quality” (p. 52). Consequently, research quality and ethics are highly interrelated. While the research quality is ensured in the above mentioned ways, we additionally considered ethical issues which arise both in conducting the research and in writing (Recker, 2013). While the latter comprises “challenges of plagiarism, recognition of co-author contributions, honest reporting, and the appropriate use of language” (Recker, 2013, p. 144), the most important ethical principles during the actual conduct of scientific research are: voluntary participation and harmlessness, anonymity and confidentiality, disclosure, and analysis (Bhattacharjee, 2012).

Considering the challenges of writing in an ethical way, we made sure not to represent the ideas, thoughts or expressions of other authors as our own work by correctly quoting and referencing all our sources. As only the two authors, as mentioned on the cover sheet, were involved in the generation of the work, no other authors had to be recognized. Additionally, we complied to honest reporting, disclosing all our findings, even unexpected or negative ones (Bhattacharjee, 2012), both in the literature review and the interviewing process. With an appropriate use of language, we not only aimed for an easy to read and understandable text, but also to not make it “biased against individuals or communities in terms of gender, race, orientation, culture, or any other characteristics” (Recker, 2013, p. 146).

The remaining key ethical principles of conducting scientific research were considered in the specific context of face-to-face interviews, as undertaken by us. All participants were informed that their participation in our study is voluntary and that they have the “freedom to withdraw from the study at any time without any unfavorable consequences, and they are not harmed as a result of their participation or non-participation in the project” (Bhattacharjee, 2012, p. 137). We did not ask any personal questions, except for their age and health status, that may put the participants in an uncomfortable or compromising position. The question regarding the state of health was explicitly introduced with the remark that it should only be answered, if the respondent feels comfortable with it. As no rewards or incentives were offered for the participants, the non-participation was not affiliated to a disadvantage. An informed consent form, stating those aspects, was developed (see Appendix 5) and handed over to the participants before starting the interviews. In order to “comply with the norms of scientific conduct” (Bhattacharjee, 2012, p. 138) we retained these signed forms after the completion of the data collection process. Additionally, we explicitly asked for permission to record the interviews.

As the principle of anonymity, implying that “the researcher or readers of the final research report [...] cannot identify a given response with a specific respondent” (Bhattacharjee, 2012, p. 138), is hard to preserve in the setting of face-to-face interviews (Recker, 2013), we instead ensured confidentiality of the data. By removing all identifying information, for example names, from our transcripts and from the report, we guarantee that “the identity of a participant cannot be identified from any form of research disclosure” (Recker, 2013, pp. 143-144) and thereby “protect subjects’ interests and future well-being” (Bhattacharjee, 2012, p. 138). Additionally, we followed the principle of disclosure by providing the participants with information about our study before the data collection, namely the interviews. Based on the information included in the informed consent form, such as “who is conducting the study, for what purpose, what outcomes are expected, and who will benefit from the results” (Bhattacharjee, 2012, p. 139), people could decide whether or not to participate. Lastly, the process of how data was analysed is reported in detail (see Section 4.2) and all results were fully disclosed regardless of their effect and implication for this study.

During all stages of our research process and while writing our report, we took into account the above mentioned ethical issues at all times. By meeting the listed quality criteria and abiding to ethical standards of science, we ensure to conduct high-quality research and to write a high-quality report.

## 5 Data Analysis and Empirical Findings

In the following sections, we will present our analysis based on the insights gathered during the interviews and outline the resulting findings in a structured way. Since a great amount of information was collected, we will only highlight the most important and relevant statements and topics raised. In accordance with the structure of our developed research model, we will separately discuss the perceived risks and benefits, the effect of moderating factors, the ultimate willingness to disclose information and additionally the public opinion towards the adoption of wearable devices in the health or life insurance context.

### 5.1 Public Opinion and General Attitude

One of the declared goals of this work was to assess the public opinion and general attitude towards the usage of health data collected by wearable devices for underwriting purposes. After explaining the new approach of health and life insurance companies in detail, we therefore asked the interviewees bluntly about the first thing that comes to their mind hearing about those new policies and if they think that using fitness trackers in the insurance context is a good idea. While some respondents did not have any prior knowledge about the phenomenon on hand and consequently did not give it any consideration beforehand, other interviewees already heard about the new insurance policies and naturally formed some opinions. For example, RP7 stated: “insurance and wearable devices were two separate entities in my mind” (RP7), whereas RP1 had more extensive knowledge and even referred to similar approaches in the car insurance industry.

Only very few respondents expressed an unrestrained positive attitude towards the matter. By simply stating: “yes, I think it is a good idea” (RP7 as well as RP8) and referring to the expectation of some general benefits, still no gushing excitement towards the new use of technology was displayed. Instead, most participants showed a certain degree of reluctance and were rather reserved. The concept was observed with a lot of doubts and RP4 stated: “I think it is good, but on the other hand [...] it will maybe be a disadvantage” and “we will have to see if it works”. She expressed fears that “at the end of the day it would only benefit the insurance company not the individual” (RP4). Other interviewees voiced objections concerning the good intentions of the insurance companies as well. RP5 stated: “I think making insurance business more data-driven is dangerous, because at the end of the day it would only benefit the insurance company not the individual” and likewise RP2 apprehended, that it is just about “making profit for their company” (RP2). Following this argument, RP3 questioned “why anyone would suggest introducing this in the field”. She assumed that “it is a great idea for the business”, but she does not “think it is a great idea for the individual” (RP3) and summarized: “on an aggregate level [...] I think everyone except for companies would disbenefit from it” (RP3). Furthermore, RP5 was on the same page and elucidated that while he “can see the benefit from the public perspective”, he is still “reluctant to impose a private company with [the collection of data]” (RP5). He has “ideological concerns that a private company

could use the information” (RP5) about him in an unexpected way in the future. While seeing the benefits, he assumed “that it could also hit back quite hard” (RP5).

As RP6’s first associations with the phenomenon were security risks, her stance towards the matter can also be described as sceptical. She expressed concerns about the amount of information collected and confirms the prior interpretation with the statement “Big Data [...] is something unknown and probably, it might have a power that we don’t know yet” (RP6).

One respondent even found substantially harsher words and described the endeavour of the insurance companies as “silly” (RP1). He further explained: “I don’t like the policies pretty much. [...]. I think, it is a silly use of technology” (RP1) and “in general it sounds stupid on many levels” (RP1). He predicts that it won’t be “a big thing for insurance companies”, and also assumed that on a personal level: “I don’t think it would be very beneficial” (RP1).

While the other respondents did not voice as strong opinions, it can still be summarized that the mind-set towards the adoption of fitness trackers for underwriting purposes amongst our nine respondents was rather negative and repellent.

To find and examine the specific reasons behind this attitude, we will investigate in detail which particular risks and benefits were perceived and what influence they have on the ultimate willingness to disclose sensitive information to health or life insurance companies.

## 5.2 Perceived Risks

As outlined in the description of our data analysis approach (see Section 4.2.5), we firstly assessed which risks were mentioned by respondents without the further inquiry of the interviewer (see Table 5.1). Only in a second step we specifically asked the interviewees about risks which were identified in our preliminary model and strongly confirmed in related literature. The results and findings of each individual construct are presented in the following.

No additional risk, that we did not consider beforehand, could be identified from the data collected during the interviews. We therefore conclude that the developed model is complete, if not overloaded.

**Table 5.1: Perceived risks mentioned by respondents without interviewer interference**

Perceived Risks	RP1	RP2	RP3	RP4	RP5	RP6	RP7	RP8	RP9	Count
Invasion of Privacy (IP)	x		x	x	x					4/9
Data Accuracy (DA)	x									1/9
Manipulation (MP)		x								1/9
Secondary Use (SU)		x			x	x	x	x		5/9
Discrimination (DM)	x		x	x	x		x	x	x	7/9
Security Concerns (SC)				x		x				2/9

### 5.2.1 Invasion of Privacy

*“I don’t have enough control...” (RP3)*

*or*

*“Oh my god, what if they are recording me right now?” (RP3)*

Four out of nine respondents expressed concerns that their privacy is being invaded by insurance companies. Statements like “I think, it is a bit intrusive” (RP1) and “you have the feeling that you are being surveilled” (RP6) highlight these common fears.

Interviewee RP3 elaborated on that in more detail: “I would probably be sometimes [...] lying awake at night and suddenly the thought would strike me ‘Oh my god, what if they are recording me right now?’ [...]. I would be very concerned [...] about what they could find out about my private life.” (RP3). She continued explaining her aversion of “this idea of being constantly surveilled and always knowing that whatever little action I don’t take might become a [...] problem for me in the future” (RP3) and concluded “I am more of a liberalist and I believe freedom is important” (RP3).

Similarly, respondent RP6 confirmed these worries: “You don’t like the fact that you are somehow being tracked, and yes you have the feeling that you are surveilled, because someone else has your data” (RP6). The ‘creepiness’ of the approach was also thematised by RP4: “Since I have a GPS, they can see exactly where I am going”.

Besides this anxiety and discomfort of a surveillance scenario and the fact that the insurance companies might find out delicate details about their private lives, the interviewees were also anticipating a loss of control: “I would feel like I don’t have enough control to know what kind of data is actually being sent to them” (RP3).

When specifically asked, all of the respondents agreed that there is a risk concerning their privacy involved in disclosing sensitive information to the health or life insurance company.

### 5.2.2 Data Accuracy

*“No system is perfect.” (RP3)*

The perceived risk of ‘data accuracy’ was only mentioned and recognized by one respondent. The interviewee who described himself as technology affine, who already owns and uses several wearable devices and was rated as above average sporty, claimed that those fitness trackers “are incorrect” (RP1) and that he does not trust them. He additionally stated “steps are just steps” (RP1) and that he is “too concerned about details” (RP1) when it comes to the application in a health or life insurance context.

In contrast, other respondents were not concerned about an inaccurate measurement of their health values or a resulting wrong assessment of their health or fitness status. RP3, for example, outlined that “no system is perfect and no model is perfect”. But she explained: “I don’t think that would be an issue” (RP3). Similarly, RP4 stated that she is aware that “every watch has like a 10% difference” regarding the measurements, but as this is a known fact, stated in the manual, she assumes that also the insurance companies will be aware of that and consider it in their evaluation. She concluded: “I don’t think it will be a problem” (RP4).

### 5.2.3 Manipulation

*“I cannot say they cannot do that. They can.” (RP9)*

Interestingly, the possibility for ‘manipulation’ was foremost seen on the customer side. RP1 stated that “you can’t know who is wearing [the fitness tracker]. You can put it on your dog, and get lots of steps from him or give it to your kids while they are playing”. Likewise, another respondent wondered: “maybe I can have 4 watches on my hand and then I can track some other people’s training instead, I don’t know, if they will figure it out” (RP4).

While this room for tampering was almost perceived as a benefit, manipulation as defined in our research model, was perceived as a major concern by only one single respondent. The interviewee expressed fear that the insurance company “can a bit manipulate things, so that they could put you in a level that you shouldn’t be in. So, they make you pay more than you really should” (RP2). She continued by explaining that “they make the data so that they would make more profit, instead of me getting any good out of it” (RP2).

When specifically asked, this view was confirmed by other respondents. For example, RP3 stated: “Yap. Changing the rules. I mean Facebook does it all the time, [...] and it is just automatically done. So, I suppose that is a very good point, it is another thing for future discussions”. RP8, as well, sees a big risk “because they have access [to your data] and they might put stuff in, that you have not done” and RP9 confirmed: “I cannot say they cannot do that. They can”. Still, he is a bit more optimistic as he believes the probability that an insurance company actually engages in manipulation is relatively small, due to the high risks the company would be taking: “Which company is going to do that? I mean the reputation of the company [...], killing it by stupid acts like that?” (RP9). This optimistic view is shared by RP4: “I don’t think it is a problem. I trust the [insurance] company [...], as long as they not show me another side of [themselves]”.

### 5.2.4 Secondary Use

*“They have a lot of information about me,  
but I don’t know how they will use it.” (RP5)*

With five out of nine respondents mentioning ‘secondary use’ as a major concern, this construct forms one of the most anticipated risks of disclosing information to health or life insurance companies. There is a lot of uncertainty involved, as for example RP5 stated: “they have a lot of information about me, but I don’t know how they will use it”. He furthermore outlined: “Somehow you sell your information, and then it’s not yours anymore, so there is always room for [misuse]” (RP5).

Amongst our interviewees both internal and external cases of secondary use were apprehended. Concerning the internal misuse, RP2 remarked: “The first feeling is a bit unsecured, in terms of how the data is going to be used. Are they going to be used correctly and [can you be sure that they not] take your data and use it for other things?”. RP5 agreed: “I give them a lot of data, and I don’t know how it is aggregated in relation to other data the insurance company has, which could reveal new patterns that might not be very beneficial for me”.

With regard to external secondary use, RP3 thinks it is very realistic that “our data is being sold on without our knowledge” and that it is given “to other companies that want to use the

data for other purposes of research or market research” as “this is what is happening currently, [...] this is part of the information society”. RP8 condescends: “They have access to all your health data and you don’t know how they are going to share it and with who. [...] Yes, they always sell your information to make more money”. RP6 and RP7 share this concern for the data being sold to third parties for advertisement purposes.

On the other hand, few respondents stated that they do not see a potential danger due to secondary use of data as they trust the insurance company (RP4). They referred to the terms and conditions, “you obviously have to read the terms and conditions quite clearly” (RP5), and stated that they would not sign a contract which allows for secondary use of data, but would trust the insurers if they promise to not sell the data to third parties or misuse it (RP9).

### 5.2.5 Discrimination

*“Of course it is a discrimination, of course.” (RP7)*

‘Discrimination’ is the most relevant and important perceived risk among our interview respondents. Seven participants mentioned the unequal treatment of individuals as a consequence of disclosing sensitive information to insurance companies as a major concern. Thereby, two perspectives were revealed: on a personal level discrimination was mostly framed in terms of financial disadvantages, and from a societal point of view also broader implications, like social injustices, were considered.

For example, RP4 illustrated unfair discrimination by stating: “I think there will be some discrimination. Because if you have like cancer, you cannot exercise as much as when you don’t have it, and you will automatically pay more”. Similar views were stated by RP6 and RP7 who agree that “of course it is a discrimination, of course” (RP7). They “would not be very happy” (RP7) about it, because “when someone is really healthy, they will have to pay less and the other ones will have to pay more” (RP6). Interviewee RP8 shares this opinion and is afraid that the insurance company “can use [the collected information] against you”. He explained: “because then they know about all your health problems. So maybe that is not good, because then they can see something and then they push up your premiums” (RP8). Even more precise and specific are the concerns expressed by RP9 and RP3. Referring to his own health issues, RP9 is sure that the new insurance approach will disadvantage him: “Such a thing will kill my opportunity to get a fair health care [...]. I will have to pay double the amount of a healthy person in my age or even more” (RP9). RP3 described her personal situation similarly: “I exercise to a reasonable extent, once or twice a week [...], but [...] I don’t think that because anyone has a different interest, like if a friend of mine loves to go to the gym all the time, I don’t see why it would be fair that they pay less insurance than I do”. She summarized: “I just don’t think that how I choose to live my life should effect what I pay for my insurance” (RP3).

Additionally, discrimination as a result of secondary use of information was considered. Fearing that the insurance company might give away the collected data to third parties, RP2 was looking at the risk of employer discrimination: “If someone wouldn’t get a job because he would be diabetic or whatever [...], that would be terrible” (RP2).

RP3 discussed broader implications of the data-driven approach for the society as a whole: “We also know that health particularly is connected a lot to your economic background and your socio economic surroundings. So we already know that rich people have to pay even less because they can afford to live healthier lives, whereas working class people who can’t afford

to live as healthy, would have to pay more.” (RP3). She concluded that “it would further rig the system against the people already disbenefited by it [...] further making it difficult for vulnerable groups to [...] make the class journey, the transcending of class, because it’s just a further obstacle to both their economy but also their personal life” (RP3).

The drastic, rigorous consequence of an exclusion from insurance eligibility was only mentioned by one respondent. RP5 is concerned that turning an insurance company into a data-driven business “would enhance the problems with some individuals falling outside the insurance system” (RP5). He explained: “some children that are born with disabilities, and people who have well documented kind of diseases, they can’t sign any insurance because they are regarded as higher risk” (RP5). Furthermore, he fears that his behaviour might lead to a discrimination against his daughter: “I mean I don’t know if they use my data, and that might affect my daughter’s option to get an insurance, because they might say ‘You have a certain lifestyle and her health issues is directly related to how you live’” (RP5).

None of our nine respondents denied the existence of a risk of discrimination and especially the personal consequences were described as an influencing factor on their willingness to share health related data to their insurance companies.

### 5.2.6 Security Concerns

*“I know there are a lot of security issues, but...” (RP5)*

When it comes to ‘security concerns’, two participants of our study explicitly voiced their doubts and worries. RP6 stated: “the first thing that comes to your mind is that [...] there could be a cyber-attack” and RP4 hypothesized “maybe some other people can break into the system and see where I am and get into my house when I am outside running”. While these women are seriously concerned about potential security threats, other respondents are a bit more pragmatic: “The thing is that I know that there are a lot of security issues, but I think, since I am a gadget freak, I would probably disregard it, because I would like to use it.” (RP5).

Furthermore, some of the interviewees trust to the insurer to secure their data: “probably the company sets the right security infrastructure” (RP6) and again others just “assume it is safe enough, but it is because I don’t know anything about technology” (RP3).

In summary, most respondents would probably agree with RP7’s statement: “I am not 100% sure that my data is secured with my insurance company.”

### 5.3 Perceived Benefits

In contrast to the risks outlined above, the range of perceived benefits mentioned by the interviewees was very limited (see Table 5.2). Only three out of our six proposed constructs were proactively addressed by the respondents, while the other concepts were either not at all perceived as a benefit or not rated as an advantage on a personal level. The various specific constructs, believed to form a benefit influencing the disclosure decision, are presented in the following.

**Table 5.2: Perceived benefits mentioned by respondents without interviewer interference**

Perceived Benefits	RP1	RP2	RP3	RP4	RP5	RP6	RP7	RP8	RP9	Count
Financial Benefits (FB)		x	x	x	x	x	x	x	x	8/9
Receiving a Fitness tracker (FT)										0/9
Health Motivation (HM)	x				x				x	3/9
Increased Fairness (IF)										0/9
Social Image (SI)										0/9
Improved Services (IS)		x		x				x	x	4/9

#### 5.3.1 Financial Benefits

*“Money talks, money sells, money buys.” (RP2)*

The concept of ‘financial benefits’ is by far the most popular and most anticipated positive outcome of disclosing sensitive information to health or life insurance companies. Eight respondents instantly named savings when asked for expected benefits and all interviewees, in unison, agreed that monetary rewards in terms of reduced premiums are a strong argument influencing the disclosure decision. As RP2 prosaically put it: “Well, it is money. Money talks, money sells, money buys”. The respondent furthermore stated, that “of course, if I can get a lower cost, that is always interesting” (RP2).

However, it was indicated in the interviewees’ remarks that the perception of the benefit is closely tied to the own health status and fitness level. RP6, for example, said that “assuming that I will be healthy, it is a good thing that I will have to pay less”. Similar conditional statements were made by RP8 who answered “I think the benefits are, if you are a very healthy individual [...] then it can lower your premium”, and RP3 agreed “if you are a somewhat healthy person, who likes to do exercise, you could pay less”.

Moreover, one respondent highlighted that the amount of savings has to be significant in order to have an influence on his disclosure decision. He outlined: “I am selling my data of every day, of my daily life” (RP9) and therefore he expects appropriate rewards in terms of financial benefits.

### 5.3.2 Receiving a Fitness Tracker

*“It wouldn’t make any difference.” (RP6)*

In stark contrast to the financial rewards, the ‘receiving of a fitness tracker’ was not appreciated as a benefit amongst respondents. Only one person mentioned the wearable device on own initiative and it was by no means in the context of advantages, but very clearly perceived as a drawback: “I don’t want to wear crap, they are handing out crap [...]” (RP1). The interviewee who already uses a fitness tracker even sees the fact that he would be obliged to wear a specific wearable device as a “physical intrusion” (RP1) and stated “I don’t want to have something on me that I don’t trust myself” (RP1). While for the fitness prone respondent the potential low quality and the constraint to receive a specific device of a certain brand was obviously seen as a major disadvantage, the other interviewees did not even mention the wearable in the first place. When specifically asked, they stated that this bounty would not make a difference to them and would consequently not have an effect on their disclosure decision. “Either I want [the insurance policy] or I don’t want it. It is not that I’ll do it because I do get a pen or whatever” (RP2). RP6 stated that “it wouldn’t make any difference” and RP8 confirmed that for him personally it would not constitute a benefit. He supposed that the wearable device might be of greater value for “healthy people” (RP8), but this assumption could not be approved by our findings. The participants which were rated as healthy or sporty, did either already possess a wearable and, as shown above, even perceive the receiving of a specific fitness tracker as a disadvantage and “would hate that, because [they] don’t want to wear crap” (RP1), or they stated that it would not influence their decision in the insurance context, even if they would in general consider buying or using a wearable device (RP5). An interviewee who was already stating her reluctance to disclose information summarized: “If the only use of that free device is to record data that I do not want recorded, I see no personal use for it. No, I wouldn’t care” (RP3).

### 5.3.3 Health Motivation

*“It [...] motivates me to achieve my goal” (RP6),  
but*

*“I also think you could imagine it being a stress factor” (RP3)*

The benefit of an increased motivation to be more active and healthier as a consequence of collecting data with a wearable device and sending this sensitive information to the health or life insurance company, was recognized by three respondents during our interviews. Both, the general concept of motivating more people to work out, thus the “social benefit” (RP1), and the inducement on a personal level, were endorsed by the interviewees. RP5, for example, stated “I like the concept of encouraging people to track their health, [...] it could be something that really improves the general health of the population, and that is an obvious benefit”. This view is confirmed by RP1 who thinks that “it is good if you motivate people to take responsibility for your fitness and more people should do it” and RP9 added “this is a very useful way to push people to be healthy”. With regard to personal gains RP5 explained “I don’t do that much exercise, but I always have it in the back of my head that I should. So, if I would wear a gadget and I would be engaged in some kind of program [...], I think it would be beneficial for my health”. RP6 agreed: “from personal experience, keeping track of my activities helps me to get better [...]. It also motivates me to achieve my goal”.

On the contrary, the remaining interviewees either question the effectiveness in terms of motivation or see it rather as a stress factor which increases the personal pressure, than a benefit. While RP4 doubts the long-term effect, saying “I think, it will be motivating in the beginning and then [...] one month later they will be tired of it”, RP2 sees differences in the motivating value depending on the gender: “We have had this at my work. We all got one of these [pedometers] [...], and the young guys they started directly to compare with each other. But we girls, no.”

Additionally, RP3 questioned the value of this kind of extrinsic motivation: “I don’t think it will increase my motivation to be healthier. It might increase my motivation to be healthier, because I want to pay less money. But ‘my’ motivation to exercise will still be on the same level, I still wouldn’t want to do more exercise. I wouldn’t be healthy, because I want to be healthier. I would exercise, because I want a cheaper price.” She apprehends that this might form a factor that “increases your stress level” if you didn’t go to the gym that day, because you weren’t feeling well” or if “you get sick for a long time” as “you know you’re going to get a higher bill for your insurance”.

Several interviewees expressed that they would not want to be pressured to increase their fitness efforts: “I want to do it my way anyhow.” (RP2).

### 5.3.4 Increased Fairness

*“Pure and simple numbers: fair much fairer. When you add the complexity of life: it is not much fairer.” (RP3)*

The assumed benefit of ‘increased fairness’ was not recognized during the course of the interviews. None of the participants mentioned the construct on own initiative and even when specifically asked about the idea, they mostly did indeed acknowledge the interpretation and even described the approach as increasing the fairness, but they did not express that this would form a benefit for them personally, influencing their decision whether to disclose sensitive information to the insurance companies or not.

For example, RP4 stated “if I am more healthy, I will have less visits to the hospital and I will not be there as much as a non-healthy person, [...] and if they pay more, because they will use the hospital more, I think that is fair”. A similar view was stated by RP8: “if there is a high risk group that is not doing any exercise, then the healthy people pay for them. But if everyone gets tracked and you pay according to your health, then it is fairer”. RP3 agreed by saying: “I could probably say that fairness would increase. If you smoke for example, I personally believe that if you smoke maybe you should pay a bit more knowing that it’s bad for your health”. However, no statement was made indicating that this increase in fairness constitutes a benefit to the individual which might affect their willingness to disclose information.

A more critical examination of the issue, demonstrating that the matter might be more complex than initially thought, was given by RP3: “we also know that there are other variables that effect your health. And there are variables that you can’t affect yourself. So let’s say you’re a smoker, but you’re a smoker because you grew up in a house where lots of people smoked, [...], then you can’t really pull that down to individual choice. So, it becomes a question whether or not you believe in free choice and that every individual is ultimately responsible for their own actions. I don’t think I am a 100%. So, it really depends on which perspective I view this from. But yes, pure and simple numbers: fair much fairer. When you add the complexity of life: it is not much fairer”.

### 5.3.5 Social Image

*“I actually don’t think that it would give me any kind of social advantage.” (RP3)*

The findings of our interviews with regard to the perception of the construct ‘social image’ can be described similarly to the phenomenon outlined above. The concept is acknowledged and believed to exist, but no one personally expects or cares about approval or admiration from their peers as a consequence of buying such an insurance policy.

This perspective was highlighted by RP3. She thinks that the influence “depends on which group of people you hang out with” as “there are people who want the newest technology [in order to impress their friends] and who think that’s cool”. But she stated: “I am not that person, most of my friends aren’t, so I actually don’t think that it would give me any kind of social advantage.” Instead, she even fears a negative effect as “they would think I was a sell out” (RP3). Similarly, RP8 explained that the devices look cool and that people “would think that you are really tech savvy, always using the newest technology”, but at the same time he stated that it would not make a difference to him. RP4 likewise said: “Personally, I wouldn’t care”. Other respondents who also claimed to be interested in the newest technology, did not express an influence of this social component on their decision, either: “There is always the case of peer pressure [...], [but] I wouldn’t be the first mover in this case” (RP5).

Additionally, RP9 hypothesized that the age plays an important role with regard to the social influence: “Yes, it can be a trend, but not in my age. I mean at my age, I don’t give a f\*\*\*.” (RP9) and RP7 added that “it all depends on the person, what motivates you and [...] what is important to you [...], if your health and staying well is important [to you], then I am pretty sure that you will be very proud of your Fitbit”. She indicated that in this case there might be a benefit in the approval of others, but did not voice that this is the case for herself.

### 5.3.6 Improved Services

*“It will improve customization.” (RP8)*

Four out of nine respondents expect benefits in terms of improved offers and services as a positive consequence of disclosing their collected data to life or health insurance companies. While this perspective was also confirmed by interviewees who did not initially come up with that concept on their own, it still became clear that they do not have a specific idea how these services could look like.

For example, RP5 stated that insurance companies “would know exactly the status of my health and of how I lived my life [...], they could actually tailor your insurance and probably enhance your life”. Similarly, RP8 believes that ‘improved services’ form a benefit for him, “because then [the insurance] can customize what they sell you. So, it will improve customization. They see that you are [...] running marathons, then they can send you specials for marathons. Maybe. I don’t know.” This uncertainty concerning how the improved customization could specifically benefit the individual, was also reflected in RP4’s statement: “if they collect data, and see that this person needs more training, maybe they can help the person [with] a personal trainer, for example.”

Only RP9 had a more precise conceptions of what he is expecting from the insurance companies. He stated: “I am a very illiterate person in diets: what to eat and what not to eat and what to do and how to sport, or walk... I am very illiterate. [...]. So I need consultancy or maybe

something like an application, that might help me, it tells me today you do 1, 2, 3 [...]”. Thus, he is looking for an insurance “program to help [him] be healthy”.

On another note, it was mentioned that the disclosure of health data to the insurance company could also benefit the individual in a broader sense, referring to healthcare in general. As “all your data is on the wearable, [...] it will make access easier” (RP8). Interviewee RP2 stated, that it could make the interaction with medical facilities simpler as they can use the data already collected for underwriting purposes.

## 5.4 Moderators

Throughout the interviews the moderating nature of trust and customer characteristics was examined. Besides dedicated questions aimed at assessing the specific peculiarities and effects, utterances in the course of the conversations helped to gain a comprehensive picture of the moderators.

### 5.4.1 *Trustworthiness of Insurance Company*

In order to assess the trustworthiness of insurance companies, we specifically asked our respondents about their level of trust in those corporations (Q13). The answers varied widely amongst the interviewees. While three respondents claimed to “not have any trust issue with them” (RP4), to in general (RP8), or at least “not 100%, but 98%” (RP7) trust them, others were undecided, not sure (RP6) and could “not say yes or no” (RP9).

The respective explanations were often based on or grounded in past experience. Thus, RP4 for example stated: “I have too small knowledge not to trust them. [...] I think they fix everything. [...] I have never used my insurance, so I don’t know actually what will happen” (RP4). Nevertheless, these past experiences do not always overrule concerns or general beliefs. RP3, for example, stated: “I mean it feels unfair to say this, because I only had to use an insurance company once and they were very nice and very kind, but I generally don’t trust big business at all. I mean, I still use them, but trust... that I don’t. I am always suspicious whenever I am in contact with a private company or big business”. This concern about capitalistic intentions is shared by RP5: “It is a business, and the business’ end goal is to earn money. And they earn money based on people’s fear of getting an injury. [...] So, I think their agenda is from an ideological perspective a little bit difficult. [...] So, I have little trust.” (RP5). Also, RP2 does “not really” trust insurance companies and described them as “something that you need to have” (RP2).

In addition to this explicit assessment of trust, further insights about the moderating role of the belief that the insurance company will keep its promises and commitments, could be gained throughout the interviews. Several indications relating to this concept were detected. For example, it became obvious that the perception of the three risks ‘manipulation’, ‘secondary use’ and ‘security concerns’, are strongly dependent on the extent of trust in the insurance company. Furthermore, RP7 stated: “Well, if I see that what I am being promised, I am getting, then I will be ready to disclose. [...] But I must get what I am being promised”.

### 5.4.2 Customer Characteristics

The customer characteristics including age, gender, country of origin, technology affinity, and health status were assessed with straightforward, closed questions. The summary of the interviewees' data was already illustrated in Table 4.2.

Additionally, during the analysis of the interviews, several cues could be found which allow the derivation of further conclusions. For example, with regard to the 'health motivation', RP2 outlined a difference in the effect on men and women, and RP9 indicated that the extent of social influence might be dependent on the age.

Furthermore, when specifically asked, if their opinion or attitude towards the issue of wearable devices in the insurance context would change, if they were in a different state of health (Q12), all respondents, by common consent, held the opinion that the health status is an important determining factor. Only if the respective interviewee already stated a reluctance or unwillingness to disclose his or her data, it was reported that this opinion would not change with the health status (RP3, RP9). All the other respondents confirmed a change of opinion and behaviour. For example, RP1 stated: "There are companies that have my fitness data [...], I don't mind, [...] but I would mind that especially if I wasn't very fit" (RP1). RP2 agrees that she "would be more careful" in case of a worse state of health and outlined: "I don't think then I would be that positive to tell everybody about any illness that I had" (RP2). Similar views were stated by RP6 and RP4 who assumes: "maybe I wouldn't be so enthusiastic" (RP4) if she was less sporty. Interviewee RP7 asked: "What purpose will it serve me, if I am wearing it and I am not fit enough?" and explained that she would "rather not let the insurance company know about" illnesses which only last for a shorter period of time. RP8 summarized: "If you are a very healthy individual [...], then it can be beneficial [...]. But, I think if you are not that healthy, then I don't know why you would go for it". This observation and effect was already described in the context of 'financial benefits' (see Section 5.3.1).

Another concept that was repeatedly brought up by the interviewees, but not considered in our preliminary model, is that of income or economic situation. For example, RP5 thinks that "people with less money would be more forced [to disclose their information], if a low premium is what comes with the package" (RP5). He also stated that his personal decision whether to disclose this sensitive information, despite "a strong reluctance against the insurance companies" (RP5), will depend on his "economic situation" (RP5). Likewise, RP3 confirmed the decisive nature of the economic situation: "given that my economy is quite poor at the moment, I would consider it [...]" (RP3).

## 5.5 Willingness to Disclose Information

As the ultimate purpose of this research study is to examine the willingness to disclose sensitive information to health or life insurance companies, this dependent variable was also directly investigated with the study participants (Q10). The results are listed in Table 5.3.

**Table 5.3: Willingness to disclose sensitive information to insurance companies**

	RP1	RP2	RP3	RP4	RP5	RP6	RP7	RP8	RP9
Willing to disclose	maybe	yes	maybe (more no)	yes	maybe (more no)	no	maybe	no	yes

After discussing all the potential advantages and disadvantages involved, three out of nine respondents clearly confirmed that they would be willing to reveal the information collected by a wearable device to a health or life insurance company. While, for example, RP9 stated that he would do it, “if the company has a program for people to get a better health” (RP9), RP2 described the motives for her readiness to reveal sensitive information with “curiosity”. Similarly, RP4 said: “I will try it. I like to try new things. [...] I would definitely try and see if it will be a benefit, and see if the risks are high” (RP4).

Less confident in their decision were respondents RP1, 3,5 and 7. RP3 outlined: “given that my economy is quite poor at the moment, I would consider it, but I think ultimately I would say no”. She explained that due to the fact that she is not earning a lot, “money is a strong factor”, but in the end she thinks “I’d probably just say ‘no’ because of principle reasons, [...] I am not going to play the insurance companies game” (RP3). Likewise, RP5 showed some uncertainty concerning his decision: “I have such a strong reluctance against the insurance companies so probably even if they would offer me very low premiums [...], I would probably not go for it. Maybe... it depends. I think, it will depend on your economic situation” (RP5). Even the sporty participant RP1 stated: “I am not sure, it would benefit me” (RP1).

In contrast, RP8 was very confident that he would not disclose his information: “No, because I am not a healthy person, so it won’t be beneficial for me.”

## 5.6 Other Remarks

Another interesting topic raised during the interviews, is the general appropriateness or reasonableness of the idea to base the insurance premium on the health status or the fitness achievements. According to RP3 “it is stupid that [people who work out a lot] have to pay less for the insurance, because there are more accidents that happen in the gym than just staying at home” (RP3). RP1 raised similar concerns and explained that very sporty people who, for example, travel to the Alps to cycle are “at higher risk of something dramatic happening like crashing” (RP1) than anyone just sitting on the couch watching TV (RP1). He concluded: “the extreme sports person, I don’t think he is a good profile for the insurance company” (RP1).

Furthermore, a strong relation to and association with other healthcare services could be noticed during the interviews. Especially, when it comes to the perceived benefits, it was expressed that an integration with other systems would be endorsed. RP2 expressed how she would like the information to be available to doctors and RP8 stated that he would appreciate to have all information in one place with opportunity for easy access.

In summary, a tremendous amount of insights could be gained from the conducted interviews. The meanings of those findings and their implication for our preliminary research model will be discussed in the following chapter.

## 6 Discussion

A lot of the findings presented above, confirm previous research and the developed, preliminary research model. Nevertheless, some deviations and shifted focal points could be perceived. We are going to interpret the empirical findings in the context of the conducted literature review, discuss the accordances or divergences and finally present our final research model, revised on the grounds of the empirical results and the discussion.

### 6.1 Willingness to Disclose, Privacy Paradox and Privacy Calculus

The availability of detailed personal customer information is of increasing importance for companies and institutions in all industries (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Business models are build around the ability to collect, store and analyse vast amounts of data and companies try to leverage data-driven approaches in order to gain competitive advantages by tailoring marketing efforts and customizing products or services. In this context, the willingness of the customer to reveal personal information becomes a decisive factor for the success or failure of products, projects, or entire corporations (Culnan & Armstrong, 1999). As described in Section 2.4.1, this development towards data-driven business practices also holds true in the specific area of health and life insurance companies.

However, previous research and public opinion polls have found that consumers all over the world are highly concerned about their privacy and therefore share a rather reluctant attitude towards the increasing data collection efforts (Phelps et al., 2000; Smith et al., 2011). Especially in the context of sensitive information, such as health related data, worries about the accumulation and usage of data are common and widespread (Anderson & Agarwal, 2011). While most of these previous findings are grounded in an e-commerce or general healthcare background (see Section 3.1), our study confirms this pronouncement in the very specific case of the disclosure of data collected by wearable devices for health or life insurance companies. As presented in Section 5.1, the opinion and sentiments amongst our respondents towards the new data-driven insurance policies are dominated by suspicion, mistrust, and worries about potentially arising disadvantages. Various concerns about information misuse, privacy violations, security risks, and doubts regarding the good intentions of the insurance companies are expressed. A common fear is that only the insurer is going to profit from the new approaches, while for the individual customer disadvantages might arise. As only few respondents initially saw the opportunity for benefits, our research findings strongly affirm the negative and repellent stance on data collection, storage, and analysis practices by companies which was previously stated in the literature (Smith et al., 2011). No previous research was conducted in this specific context of insurance companies and wearable devices, and thus the confirmation of the reluctant attitude when it comes to the insurances' approach to collect data via fitness trackers and use this information for underwriting purposes, can be described as an important research contribution.

In related literature, it is stated that those privacy concerns and the prevailing negative attitude towards the issue can be described as a key challenge and restraint when it comes to the wider dissemination of new technologies and their applications (Mayer, 2009; Vaia et al., 2012). Transferring this notion to our research context, it has to be expected that the various concerns raised by our respondents are potentially hampering the further adoption of data-driven approaches in the life and health insurance industry as the customers would refuse to disclose their data and consequently not buy corresponding insurance policies. But against all expectations, this generally negative attitude on the issue is not reflected in the willingness to disclose sensitive information to insurance companies. Paradoxically, the actual intention to disclose, as described by our interviewees (see Section 5.5), seems to follow different rules. The voiced concerns and doubts do not directly translate into all participants agreeing that they would not reveal their sensitive information. Instead, actually three out of our nine respondents stated that they would be willing to reveal the information collected by fitness trackers to their health or life insurance company. Other interviewees said that they would consider it, while only two respondents reported to be sure and certain that they do not want to share their data. It was even explicitly stated by one respondent that he tends to disregard some of his own beliefs about the importance of privacy, if he likes to use a service or product (RP5). Thus, it cannot be concluded with certainty that the dissemination of the new insurance policies is going to be affected by the prevailing negative attitude as voiced by the general public. The same phenomenon was observed in the e-commerce context. Despite a very high level of consumer privacy concerns, the online shopping market continued to grow, apparently unaffected by the voiced issues (Phelps et al., 2000).

This observation is closely linked to the concept of the ‘privacy paradox’ as described in Section 3.2.1. But while the privacy paradox highlights the discrepancy between the intention to disclose personal information and the actual behavior (Norberg et al., 2007), our findings already indicate a significant difference between the expressed general opinion and the willingness to disclose, so the disclosure intention. Based on our findings and other literature confirming the privacy paradox, it can be expected that the actual disclosure behaviour further deviates from the disclosure intention and even more from the public voiced opinion. While the perceived risks of revealing personal information seem to determine and dominate the general attitude of our respondents towards the new insurance policies, the willingness to disclose and the involved decision process is driven by other considerations.

Previous literature in the context of information disclosure which tries to explain the existence of the paradox, points to the ‘privacy calculus’ as outlined in Section 3.2.2 (Norberg et al., 2007). Confirming these sources, our interviews clearly revealed that expected benefits come into play in the context of the disclosure decision. The respondents engage in a cost-benefit analysis in order to decide whether they want to disclose their information or not. While some interviewees explicitly stated that “you have to make some sort of cost-benefit analysis” (RP5), others implicitly indicated that they are weighing advantages against disadvantages (RP6) and assess the trade-off between perceived risks and benefits. These statements strongly confirm the concept of privacy calculus as defined by Dinev and Hart (2006), and thereby strengthen the argument for the choice of our main structure of the research model. Consequently, the main influencing factors of perceived risks and perceived benefits on the willingness to disclose information are supported by our empirical results. Additionally, other concepts like curiosity (RP2) or trying out new things (RP4) are reported to impact the disclosure decision and highlight the important role of customer characteristics (see Section 6.4) and trust, as introduced by (Dinev & Hart, 2006).

In summary our findings show a negative attitude towards the data-driven insurance approaches. Paradoxically, these concerns do not solely determine the willingness to disclose information to the insurance companies, but instead, people engage in a privacy calculus and are willing to assume some of the risk in return for some benefits. Consequently, our empirical results confirm literature in the context of privacy concerns, the privacy paradox, and the privacy calculus. The theoretical foundation of our research model is verified and the model design justified.

In the following we are shortly going to discuss the findings concerning each factor as present in our preliminary model and derive conclusions for our final research model.

## 6.2 Perceived Risks

In accordance with previous research, as summarized in the literature review (see Chapter 3), our study revealed a broad variety of risks associated with the disclosure of information to health or life insurance companies. Various different aspects and dimensions of risk were proactively mentioned by interviewees and the focus of major concern seemed to differ amongst individual respondents. These findings confirm the statement of Beldad et al. (2011) that “the risks related to the disclosure of personal data are copious and depend on the amount and type of the personal information disclosed” (p. 222).

While no previous research in the context of life or health insurance companies examined the specific risks associated with this particular type of information disclosure, studies in other fields, for example e-commerce, mostly treated risk as a more general concept and summarized it under perceived privacy risks (Dinev et al., 2006) or simply perceived risks (Treiblmaier & Chong, 2012). We deviated from this approach and chose a more detailed examination by deriving six subconstructs from closely related literature. These risk factors are consequently explicitly tailored to the particularities of the scenario on hand, involving the collection of data via wearable devices and the usage of the information by insurance companies for underwriting purposes. The identification, description, and verification of the components forming the perceived risks, therefore fill a research gap and constitute a significant research contribution.

The conceptualization of risk as a multidimensional construct, already proposed by Anderson and Agarwal (2011), is strongly advocated by our findings. Even if not all constructs could be verified, it became obvious that the nature of the expressed concerns is too diverse and complex to be summarized under a single dimension. The conclusions which can be derived from the examination of each and every aspect are valuable and insightful. Each specific risk perceived in the context of information disclosure to health or life insurance companies entails different implications for both research, practice (see Section 7.2) and for our final research model (see Figure 6.1).

### 6.2.1 *Invasion of Privacy*

The identification of an ‘invasion of privacy’ as a perceived risk and the incorporation of the construct in our research model was strongly supported by our empirical results. Confirming previous research which highlighted the importance of privacy concerns and defined comparable constructs (Dinev & Hart, 2006; Wakefield, 2013), our respondents discussed their fears of being constantly surveilled and of the insurance companies observing and interfering in

their private lives. It became very obvious that the interviewees perceive the thought of constantly wearing a tracking device and consequently of the insurance company to know where they are and what they are doing as ‘creepy’, intrusive (RP1), discomforting, and very concerning (RP3). Both dimensions, a loss of control about which data is shared and a feeling of ‘instinctive recoil’ (see Section 3.5.1.1), were reflected in the respondents’ answers.

Thus, our findings confirm that privacy concerns, as described in the related literature, are also relevant in the context of using wearable devices for underwriting purposes and they justify the inclusion as an influencing factor on the decision to disclose information to insurance companies in our research model.

### 6.2.2 Data Accuracy

In stark contrast, the contribution of ‘data accuracy’ to the concept of perceived risks and the negative effect on the disclosure decision could not be verified during the course of our interviews. As the vast majority of respondents did not mention the danger of an insufficient accuracy of data or even stated, when asked, that they do not think it is a problem (RP3, 4), it has to be presumed that this dimension is not of great concern for individual customers.

Neither the lack of common standards and resulting inaccurate measurements as described by Christophersen et al. (2015), nor the reduction to numbers and negligence of other external factors during the health status assessment, potentially leading to inappropriate categorizations (Al-Saggaf, 2015), were mentioned or recognized as a potential peril. Instead the interviewees expressed tolerance for small imprecisions or rely on the insurance companies to account for it (RP4), thereby refuting the statements made in literature. As only one respondent (RP1) expressed a concern for details, it has to be assumed that he is an exception amongst customers. Thus, it is concluded that the risk dimension of ‘data accuracy’ is not going to influence the disclosure decision in a negative way and it is consequently removed from the research model.

### 6.2.3 Manipulation

While the concept of ‘manipulation’ was not brought up often on own initiative during the interviews either, its importance and contribution to the perceived risks could still be confirmed when examining the phenomenon in more detail. The concern that data could be manipulated in a way that customers are re-categorized in an unfavourable way, was clearly expressed (RP2) and all participants acknowledged that the possibility for manipulation exists. Still, the degree to which manipulation is considered as a risk factor seems to differ greatly among respondents. Our findings indicate that this discrepancy can be explained with the moderating effect of trust. Interviewees who trust insurance companies (e.g. RP4), seem to estimate the likelihood of manipulation to actually happen as much lower than interviewees who do not have any trust in the corporations (RP2 or 3) (also see Section 6.4.1).

Since the room for manipulation was recognized by the interviewees, it can be said that the risk of an organization modifying the data or the algorithms in order to change the analytical outcome which was initially described by Christophersen et al. (2015), is supported by our findings. In summary, the incorporation as a risk factor in our research model therefore seems reasonable and justified, considering and accounting for the moderating effect of trust.

#### 6.2.4 *Secondary Use*

More than half of the respondents in our study mentioned ‘secondary use’ as a risk factor when it comes to disclosing information to insurance companies, making it one of the most anticipated or perceived risks in that context. Thereby, the findings and statements of various researchers (Al-Saggaf, 2015; Borna & Avila, 1999; Christophersen et al., 2015; Smith et al., 1996) who describe the usage of collected data for different purposes than initially stated, are confirmed.

Both, internal and external secondary use, as distinguished by Smith et al. (1996), are mentioned by the respondents. A general uncertainty about how information is going to be used and a concern about potential misuse contribute to the former (RP2, 5), while the unsureness about who the insurance company is going to share the data with, or whether the data might even be sold to third parties without consent (RP3, 6, 7, 8), underlines the concern for external secondary use. Thus, the analysis of the conducted interviews clearly shows that ‘secondary use’ significantly adds to the perceived risks. Again, moderated by the trust in the insurance company, it is thereby directly connected to the willingness to reveal information and associated with a negative effect on the disclosure decision.

#### 6.2.5 *Discrimination*

The only construct attracting more attention than ‘secondary use’ is ‘discrimination’. With seven out of nine respondents proactively mentioning this specific danger, it could be shown that the ‘fear of insurance discrimination’ is not only relevant in the context of genetic information disclosure as described by Armstrong et al. (2003), but also in the area of data collected by wearable devices. Previous literature extensively discusses an adverse insurance premium rating (Al-Saggaf, 2015; Borna & Avila, 1999; Christophersen et al., 2015) and exclusion from insurance coverage eligibility (Al-Saggaf, 2015), also called cherry-picking of customers, as possible negative consequences of information disclosure. Both aspects are strongly confirmed by our study’s findings. Interviewees expressed deep concerns that due to their specific state of health or to their fitness habits, they would have to pay significantly more than others and they voiced their worries towards this unfair treatment. Even discrimination as a result of secondary use of information, in terms of employer discrimination, was thematised and described as a “terrible” future scenario (RP2). The fact that yet societal implications were brought up in the discussion (RP3), further emphasizes the importance and relevance of this topic for the interviewees. Thus, it can be said that ‘discrimination’ significantly contributes to the perceived risks and can be expected to influence the willingness to disclose information to health or life insurance companies in a negative way. The empirical findings strongly justify the remaining of the construct in our research model.

#### 6.2.6 *Security Concerns*

‘Security concerns’ as a construct was derived from the literature in the context of wearable devices (Britton, n.d.; Lymberis, 2003). The risk of cybersecurity attacks as outlined by Britton is specifically emphasized and confirmed by RP6. Furthermore, another respondent draws on a scenario in which unauthorized parties gain access to the data collected by fitness trackers and misuse it in order to break into the house while the owner is outside running (RP4). While these two statements express serious concerns, the other respondents were less worried. Still, this limited number of mentions does not affect the relevance for the disclosure

decision as the seriousness is further confirmed by the utterances of respondents, stating that they are aware of security issues, but would disregard it (RP5), or by outlining a lack of technology knowledge to judge the security risks (RP3). RP7 stated that no one is 100% sure that their data is secure with insurance companies, which insistently illustrates the importance of the construct in our area of research and the negative influence on the decision to disclose sensitive information to health or life insurance companies.

### 6.3 Perceived Benefits

The variety of perceived benefits which was mentioned during the interviews, was significantly lower than that of perceived risks. This observation affirms the tendency in previous research to focus on the risks affecting the disclosure decision, rather than the benefits (Smith et al., 2011). Nevertheless, despite an initial focus on potential disadvantages the willingness to disclose sensitive information to health or life insurance companies is influenced by other factors, eventually overruling the concerns of respondents and leading them to reveal their information anyway. This phenomenon of a compensation for loss was described in the literature (Dinev & Hart, 2006; Smith et al., 2011) and is strongly supported by our findings (see Section 6.1). Just like the perceived risks, the specific benefits are believed to be dependent on the research context (Sun et al., 2014). As again no previous studies are available which determine the respective benefits associated with information disclosure via wearable devices to health or life insurance companies, the examination of each and every potential beneficial factor, tangible or intangible, is important and contributing substantially to the body of research. In the following, we are therefore going to discuss our proposed benefits, the interviewees' perception of them, and the implications for our research model.

#### 6.3.1 Financial Benefits

The most obvious benefit of disclosing sensitive information to insurance companies is the financial advantage in terms of a reduced premium. All respondents mentioned and acknowledged the huge contribution of monetary incentives to the perceived benefits and even confirmed a direct effect on their disclosure decision. These empirical results strongly affirm prior research in the field of e-commerce (Hui et al., 2007), as well as in the field of health information (Pickard, 2014) which found similar relations. It is clearly indicated that people are willing to trade their personal health information in exchange for monetary rewards. The prospect of reducing the insurance premium and thereby saving money seems to compensate for perceived risks and has the strongest effect on the disclosure decision amongst all the examined influencing factors. No construct, benefit or risk, achieved more attention and consideration of the interviewees. Even respondents with a strong reluctance towards insurance companies collecting their data stated that they would consider revealing their information, if the financial reward was appropriate (RP5). Surprisingly, even people who claimed not to be too sporty or to be in a bad state of health mentioned the financial advantage as a general benefit. While they did not see the opportunity to benefit on a personal level, they acknowledged the possibility for others to gain. In this context, it has to be mentioned that the extent to which financial savings are perceived as a benefit depends heavily on customer characteristics (also see Section 6.4.2). Those individual differences are strongly moderating the relation between 'financial benefits' and the willingness to disclose information. For example, is the health or fitness status affecting the extent to which financial savings are expected. Furthermore, the

interviewees' responses indicated that individuals with a high income will value the savings less than individuals with lower income (R3, 5), thus the effect on the disclosure decision will differ depending on the economic situation. In summary, the insights gained throughout the interviews impressively confirm previous research, the contribution of financial benefits to the overall perceived benefits, and the strong influence on the willingness to disclose information to health or life insurance companies, taking into consideration the moderating effects. The placement of the construct in the research model is highly justified.

### *6.3.2 Receiving a Fitness Tracker*

The construct of 'receiving a fitness tracker' was added to the research model as it was believed that this device might serve as a benefit, providing value for some customers who might consequently be influenced in their decision to disclose data to insurance companies. While no literature exists in this area of research which could establish this idea, our argument was based on the fact that the wearable device can be rated as a tangible reward whose positive influence on the disclosure decision was confirmed by Hui et al. (2007).

Nevertheless, the interviews showed no evidence that the free distribution of wearable devices contributes to the perceived benefits and consequently no effect on the willingness to disclose information can be derived. The reasons for this deviating perceptions vary amongst respondents. On the one hand, interviewees who do attribute a value to the device already owned a fitness tracker and hence did not see any benefit of receiving another one (RP1, 4). It was even seen as a drawback that a specific device or brand which might not meet the individual demands and expectations, has to be worn and would replace the own fitness tracker (RP1). On the other hand, respondents who are not that sporty, even if technology affine, did not express any interest in the present (RP5, 6, 8). In contrast, it seemed like an opposing reaction is evoked: the interviewees do not want to be lured into buying an insurance policy by being offered free bounties (RP2). In summary, no indications could be found which would justify the remaining of 'receiving a fitness tracker' as an influencing factor in the research model.

### *6.3.3 Health Motivation*

In contrast, the contribution of 'health motivation' to the overall perceived benefits and the associated positive effect on the disclosure decision was verified during the course of our interviews. Three participants proactively mentioned the concept of an increased motivation to be more active and healthier as a personal advantage and thereby highlighted the importance of this concept. Next to a broader social advantage, the interviewees outlined that this extrinsic motivation would help them achieve their goals which is of great value for them (RP5, 6). These findings confirm literature in the area of wearable devices (Handel, 2011; Kranz et al., 2013; Sundar et al., 2012) as outlined in Section 3.5.2.3. Even though some respondents did express that they would not want to be pressured by a third party to exercise (RP2, 3) or questioned the effectiveness in terms of long-term motivation (RP4), the general acknowledgement that 'healthier is better' seems to be prevailing. In this context of 'health motivation' the customer characteristics, especially the preferences for sport and fitness activities, the competitiveness or even the gender, seem to have an especially strong moderating effect on the extent to which it is perceived as a benefit (also see Section 6.4.2). Therefore, it was decided to keep the construct in the research model, despite some respondents not confirming the contribution to the perceived benefits. Building on the analysis, it is concluded that the motivational

value of the new insurance policies constitutes a benefit for many customers and that it consequently is positively connected to the decision to disclose information.

#### 6.3.4 *Increased Fairness*

Similarly to the proposed benefit of ‘receiving a fitness tracker’, ‘increased fairness’ was not mentioned by any respondent on own initiative during our interviews. Derived from the literature (Borna & Avila, 1999), it was believed that the accurate risk assessment and the corresponding charge for exactly the risk measured, namely personalized insurance fees, would be perceived as an intangible advantage resulting from disclosing information to the insurance company. Surprisingly, this perception could not be verified by our findings. Instead, various respondents acknowledged that there might be an increase in fairness, but this notion was not directly connected to a personal benefit. No evidence could be found that the interviewees would derive any advantage from this fairer treatment which would influence the decision to disclose information. As the assessment of fairness thereby involves a comparison to other policyholders, it can be concluded that these kinds of indirect benefits are not of relevance for the decision process. Only benefits with an explicit, direct, and immediate effect on the individual were considered by our interviewees.

Furthermore, it became clear that the understanding of ‘fairness’ is ambiguous, as some respondents struggled to determine what is fair and what is not (RP3). Taking into account the broader implications, the complexity of the construct and the proximity to ‘discrimination’ came to light. Moreover, the benefits in terms of insurance fraud detection and prevention of moral hazard were not mentioned by the respondents, either. Consequently, it can be said that ‘increased fairness’ does not contribute to the perceived benefits influencing the disclosure decision. The construct is therefore removed from the research model.

#### 6.3.5 *Social Image*

Drawing on literature concerned with the adoption and acceptance of wearable devices (Kim & Shin, 2015; Yang et al., 2016), it is believed that social adjustment benefits are influencing the willingness to disclose sensitive information (Smith et al., 2011). This idea was transferred to our research context, assuming that the ‘social image’ could be of equal importance and follow similar rules in the context of data collected by wearable devices which is revealed to health or life insurance companies. But once again, this factor could not be validated through our empirical results. The respondents expressed a general belief that some people might be influenced by expected approval or admiration from peers, but stated that this does not hold true for themselves. Consequently, the effect on the ‘social image’ is not perceived as an individual benefit. Even technology affine interviewees stated that they would not let themselves be guided by peer pressure and that they would not want to be the first mover in this scenario (RP5). Interpreting these statements, it has to be concluded that the decision to disclose sensitive information to health or life insurance companies is too crucial for the respondents to be influenced by the opinion of peers. While it cannot be ruled out that the interviewees’ statements followed a social desirability bias (see Section 7.3), it seems that the approval and admiration of others is not that important, that it would outweigh any of the perceived risks. As a consequence, the construct of ‘social image’ is eliminated from the conceptualization.

### 6.3.6 Improved Services

‘Improved services’ have been mentioned by four respondents who thereby confirm findings in the context of e-commerce which highlight the benefit of personalization (Beldad et al., 2011). Smith et al. (2011) outline that the value of personalization overrides privacy concerns and Al-Saggaf (2015) expects similar reactions to the tailoring of products and services to the needs and preferences of individual customers in the life or health insurance environment. Our empirical results strongly support these pronouncements as the interviewees expect enhancements and benefits based on the information disclosed to the companies. While some respondents specifically expressed that they anticipate benefits in terms of special offers for services related to their individual preferences (RP8) or tailored insurance premiums (RP5), to profit from an easy access to the data which is supposed to facilitate the interaction with the company (RP8), or to benefit from specific health and fitness programs tailored to the individual needs (RP9), others did not have a definite idea how increased customization can benefit them. Still, the value of improved services and tailored offers is acknowledged by all respondents. In summary, our findings illustrate how ‘improved services’ are perceived as a benefit in the context of sensitive information disclosure to health or life insurance companies.

## 6.4 Moderators

As already shown above the relation between perceived risks, benefits and the willingness to disclose is moderated by two main factors. The findings concerning those two constructs are discussed in the following.

### 6.4.1 Trustworthiness of Insurance Company

The important role of trust was highlighted in the literature concerning information disclosure (Anderson & Agarwal, 2011; Bansal et al., 2010; Dinev & Hart, 2006; Gefen et al., 2003; Schoenbachler & Gordon, 2002; Wakefield, 2013) and is as well clearly reflected and reinforced in our empirical findings.

The level of trust in insurance companies as stated by the respondents varies widely. Interestingly, it mainly seems to be based on past experience (RP4) or general beliefs towards private corporations (RP3, 5). While this collected qualitative data does not allow for the derivation of specific patterns and correlations, other comments of the respondents emphasized the relevance of the concept in our research context. As already outlined, the user’s belief that the health or life insurance company will keep its promises and commitments, and cares for the interests of the policyholder has a strong influence on the perception of various risks. For example, the risk for ‘manipulation’ was estimated to be very low by RP4, who explained this by stating that she does trust her insurance company. Similar reasoning could be observed in the context of ‘secondary use’ and ‘security concerns’. Even if ‘secondary use’ is generally believed to be a major problem, customers might not consider it in their decision to reveal information, if they trust their insurance company (RP4, 5, 9). The statement by Culnan and Armstrong (1999) that “trust reflects a willingness to assume the risks of disclosure” (p. 106) is consequently verified. Also in the context of benefits it was stated that the extent to what the customer believes the insurance company is going to deliver on their promises is affecting the disclosure decision (RP7).

It can be concluded that the trustworthiness of the insurance company is significantly influencing the perception of both risks and benefits, and ultimately the decision to disclose sensitive information. The inclusion in the research model as a moderator is therefore vindicated.

#### 6.4.2 *Customer Characteristics*

The second moderator in our research model, ‘customer characteristics’, is composed of various subconstructs and was derived from previous literature (Bansal et al., 2010; Pedersen, 1982; Smith et al., 2011).

The qualitative nature of our study and the limited number of respondents does not enable a quantitative evaluation or confirmation in terms of correlations between specific characteristics and the perception of risks and benefits and their influence on the disclosure decision. These relationships have to be tested in a quantitative manner and are left for future research (Section 7.3). Nevertheless, the assumption that individual characteristics play an important role in our research context could be confirmed with our empirical results. As already outlined in the corresponding sections, various statements by the respondents were connected to conditional premises. In the context of ‘health motivation’ it was stated that the motivational value might be higher for male than female customers (RP2), and with regard to the ‘social image’ it was assumed that the benefit of approval from peers is more relevant for younger people than older ones (RP9). Additionally, RP5 outlined that he would disregard ‘security concerns’ as he is a “gadget freak” and would want to use those devices (RP5). The familiarity with technology, or the prior technological knowledge, also seemed to influence other interviewees’ risk perceptions (RP3) in the context of security threats. Those comments underline the importance of ‘age’, as proposed by Regan et al. (2013), ‘gender’ (Eckel & Grossman, 2008; Sheehan, 1999), and ‘technology affinity’. Furthermore, no explicit evidence could be found that confirms the findings of Bellman et al. (2004) and Gupta et al. (2010), stating that the country of origin or the cultural values influence the willingness to disclose personal information. However, the lack of indications in our qualitative study does not invalidate the prior findings and only strengthen the need for further, quantitative testing of our research model.

In contrast, the importance of the individual ‘health status’ could already be shown in our analysis. In accordance with Bansal et al. (2010), various statements revealed that for example the risk of ‘discrimination’ is perceived as more severe for people in a poor health status and that accordingly the individual assessment of expected ‘financial benefits’ is strongly dependent on the own state of health. Additionally, all interviewees stated that they would be less comfortable to share their information if they were suffering from a severe illness, highlighting the delicate nature of the health information to be shared.

Our gained insights additionally indicate that another factor, not considered in our preliminary research model, is significantly affecting if or to what extent a specific concept is perceived as a benefit or a risk. It became obvious across all participants that the economic situation, or the ‘income’, is influencing the disclosure decision. The respondents’ utterances implicate that especially the assessment of ‘financial benefits’ is strongly dependent on the individual economic situation. Furthermore, people with financial problems might be more willing or even pressured to assume or disregard perceived risks in exchange for some benefits, thus majorly influencing their decision to disclose sensitive information to health or life insurance companies. Therefore, all these customer characteristics, including the new concept of ‘income’ are believed to moderate the relationship between perceived risks, perceived benefits and the willingness to disclose health information to insurance companies. The moderating nature of ‘customer characteristics’ is strongly confirmed by our findings.

## 6.5 Revised Research Model

After conducting and analysing the semi-structured interviews, our preliminary research model was revised and the gained findings incorporated on the grounds of the above presented discussion. The consolidated model is slightly modified and more compact as several dispensable construct whose effect and relevance for the willingness to disclose information could not be confirmed, were excluded. The perceived risk of ‘data accuracy’ as well as the perceived benefits of ‘receiving a fitness tracker’, ‘increased fairness’, and ‘social image’ were eliminated from the preliminary research model, while the additional dimension of ‘income’ was added to the moderating factor of ‘customer characteristics’.

Our final research contribution, consisting of a solid conceptual model, developed based on an extensive, thoroughly conducted literature review and a carefully analysed qualitative study, is depicted in Figure 6.1.

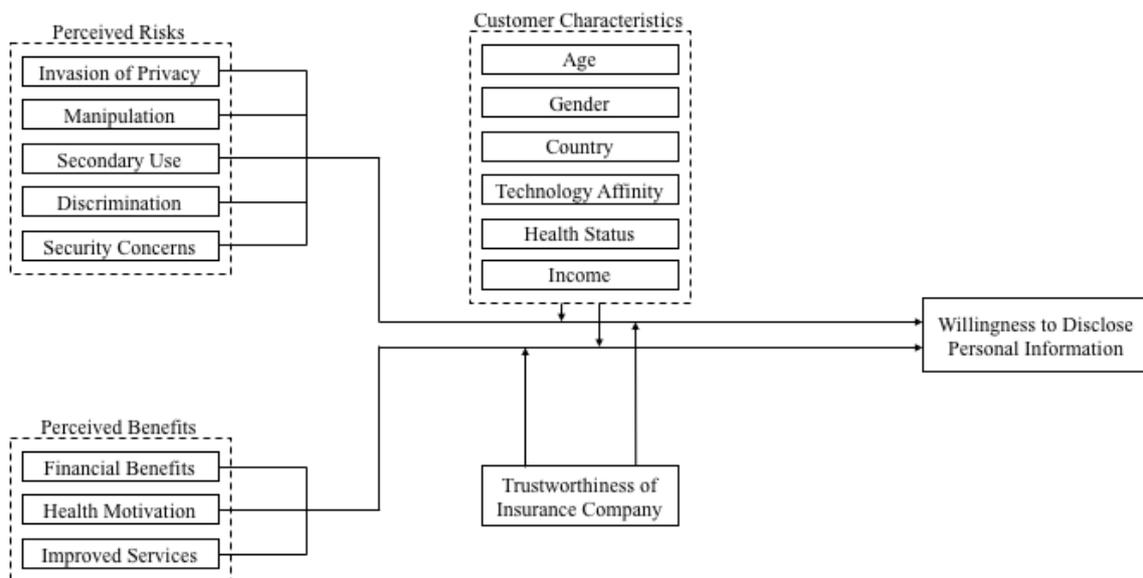


Figure 6.1: Revised research model

## 7 Conclusion

Our study, concerned with the factors influencing the willingness to disclose sensitive health information collected by wearable devices to insurance companies, comprises an extensive literature review which constitutes the theoretical background of the inquiry as well as the collection and analysis of numerous qualitative interviews. It spans several areas of research, including information privacy, wearable devices, the insurance industry, and information disclosure.

In the following, we are going to conclude this thesis by summarizing the underlying phenomenon and answering the research question with our findings, by stating the theoretical and practical implications, and by outlining the limitations and directions for future research.

### 7.1 Summary and Main Findings

The advent of the Big Data phenomenon creates tremendous opportunities for companies, organizations and governments. The increasing ability to collect, store, and process vast amounts of data is enabling major changes in business processes and promises to transform whole industries, including the insurance sector (Schroek & Shockely, 2015).

Since underwriting and consequently risk assessment is the core of the insurance business, the industry has always been data intense (Marr, 2015). The prospect of having even more precise and greater amounts of information available to enhance risk assessment and predictive models, to improve coping with uncertainty, or to uncover insurance fraud, is highly endorsed by industry insiders (Marr, 2015). Therefore, insurance companies have been looking for ways to gather more information about their current or potential customers. In the context of health and life insurance, the adoption of wearable devices has been considered and is already implemented in various countries (Christophersen et al., 2015). With their ability to track fitness efforts and various different health related values in real-time (Yang et al., 2016), they are able to provide valuable information which can be analysed and used for underwriting purposes. As a result, insurance policies can be tailored to individual customers and meaningful insights can be gained. While manifold benefits, not only on the company but also on the customer side, are expected, moral and ethical concerns exist and initiated a public discussion about the appropriateness of the approach. Consumers and activists are highly concerned about privacy and security issues, especially given the sensitive nature of the data. Since these concerns towards the data collection efforts could pose a main impediment for the further adoption and dissemination of data-driven insurance policies, they are highly relevant for the concerned companies, but also for policymakers who are trying to protect consumers.

The main prerequisite for making these new insurance models work is that customers are willing to share their sensitive information with the corporations. Therefore, a heightened interest exists in research determining what makes people disclose their information or what keeps them from doing it. Our study specifically aimed at filling this research gap by carefully ex-

aming the customer side in the context of the adoption of wearable devices for underwriting purposes. By conducting nine qualitative interviews we could confirm that major concerns exist, resulting in a negative opinion and reluctant attitude towards the new insurance policies. Nevertheless, our empirical results also prove that the privacy paradox holds true in our research context. Despite major concerns, some of the respondents expressed their willingness to disclose their information. Explaining this inconsistencies, it was shown that the initial judgement of the insurances' approach is dominated by the assessment of expected risks, while the actual willingness to disclose is subject to a more complex system of influencing factors. Confirming previous literature, customers are engaging in a privacy calculus, weighing the risks against the benefits of disclosure, carefully performing a cost-benefit analysis. Accounting for the particularities of the research context, including the sensitivity of the information to be shared and the medium of transmission, wearable devices, the specific risks and benefits as well as the moderating factors influencing the willingness to disclose data to insurance companies, were derived from the literature and confirmed during our interviews. The results are summarized and illustrated in our empirically and theoretically induced research model (see Figure 6.1) which is also answering the initially posed research question:

*What factors influence the willingness of customers to disclose sensitive, personal information collected by wearable devices to health or life insurance companies?*

The willingness to disclose sensitive, personal information to health or life insurance companies is, according to our research findings, influenced by the assessment of perceived risks, including an invasion of privacy, manipulation, secondary use, discrimination, security concerns, as well as perceived benefits, comprising financial benefits, health motivation, and improved services. These relationships are further moderated by the trustworthiness of the insurance company and the individual customer characteristics.

This valuable and highly relevant conclusion provides implications not only for the insurance companies, but also for policymakers and other researchers.

## 7.2 Theoretical and Practical Implications

Our qualitative study caters for several important theoretical contributions to the existing body of research. Firstly, the developed conceptual model fills a significant research gap as no prior work was concerned with the willingness to disclose information in the context of health or life insurance companies and wearable devices. Despite similarities to other research areas, like e-commerce or digitization of healthcare, it was shown that the specific characteristics and peculiarities of the context differ significantly. Consequently, our developed model is a valuable addition and lays a solid foundation for further investigation and motivates future research (Section 7.3).

Secondly, our empirical results contribute to and enrich general privacy research as well as wearable devices research by connecting it to a specific scenario. In general, the knowledge in terms of Big Data adoption in specific industries is extended, as the findings could as well be of relevance for other industries trying to adopt approaches which require the collection of customer data. Furthermore, the need for the connection and merging of various research areas is highlighted. It is not enough to study wearable devices, privacy concerns, and specific industries in isolation. In fact, emerging technologies in the context of Big Data, have to be linked to established theories.

But not only for the research community are the findings presented in this thesis of great relevance. Also practitioners and professionals in the insurance industry can benefit and draw on our contributions. The thorough assessment of each and every perceived risk and benefit provides for a solid basis on which the offered insurance policies can be revised or marketing efforts adjusted. For example, actions could be taken in order to guarantee the customer's privacy, and measures installed to ensure security. Additionally, trust building initiatives, and local marketing campaigns accounting for cultural differences, could mitigate the perceived risks of discrimination, manipulation, and secondary use. Furthermore, as financial incentives were identified as a major benefit, the pricing and reward system should be carefully examined and fitness and health programs implemented. Thus, by building on our empirical findings, customers might be more willing to disclose their information and insurance companies able to improve their risk assessment. At the same time, customer satisfaction would increase as their concerns are actually understood and answered, eventually resulting in benefits for both the customers or potential customers and the health or life insurance companies.

For policymakers once again the importance of privacy and security, especially in the context of sensitive data like health information, was highlighted and broken down to a more detailed level. The empirical results stress the need for laws and regulations to prevent misuse of the collected data and to protect customers.

### **7.3 Limitations and Future Research**

Despite these meaningful contributions and implications, the study does entail some limitations. Firstly, it has to be stated that the risk of a social desirability bias amongst the respondents cannot be completely ruled out in our qualitative interview approach. As we have to trust on the interviewees' self-disclosure, their statements might not directly reflect their actual opinion or disclosure intention. Although we were trying to set a trust encouraging atmosphere (see Section 4.3.4), we cannot guarantee that the respondents were not influenced by what they think is social desirable. Furthermore, their actual behaviour might substantially differ from their reported willingness to disclose, following the privacy paradox (see Section 3.2.1). While these issues are common for qualitative inquiries in the field of information disclosure, they can be translated to a suggestion for future research. Further studies, examining the actual disclosure behaviour as opposed to the willingness to disclose, could significantly enhance the understanding of the phenomenon. Additionally, as suggested in Section 4.1.3, a quantitative study is highly recommended in order to test the correlations between the different factors. Especially, the moderating effects of customer characteristics could not be adequately confirmed during our analysis. While our sample does contain various nationalities and persons with varying state of health, these manifestations are not exhaustive and therefore insufficient for a categorical answer. A quantitative analysis could explicitly test those relationships and clarify uncertainties.

Moreover, as financial benefits were identified as the strongest influencing factor, other new research directions are conceivable. For example, it could be very interesting to investigate how much privacy is worth to the customers.

Our study provides a solid foundation on which future research can be based on. Given the pioneering character of the study and the great relevance of the topic on hand, it can be expected that this field of research will continue to attract a lot of attention in the future.

# Appendix 1

## Auto Insurance

Amongst the different types of insurances, the auto insurance is one of the most developed in terms of Big Data adoption or data-driven risk assessment and management. So-called “pay as you drive” insurance models are being introduced and in contrast to traditional insurance policies, they charge customers “depending on where and when they drive, instead of a fixed amount per year” (Troncoso et al., 2011, p. 1). By relying on vehicle telematics and by installing a device, also called on-board unit (OBU), in a motor vehicle, the collection and transmission of “usage-based driving information” (Vaia et al., 2012), is enabled. The collected personal driving data, such as vehicle speed, acceleration and location, is subsequently used to “calculate a more precise and fair insurance premium, provide feedback to drivers to optimize their driving style and stimulate customer engagement and interaction” (Vaia et al., 2012, p. 113).

Two main variants of the policies are available: pay as you drive (PAYD), the more popular term, and pay how you drive (PHYD) (Vaia et al., 2012). While in the past, insurance premiums were based on static demographic data, e.g. age, gender, or past accidents, the PAYD approach now allows for a usage-based insurance, thus a variable premium, where costs only occur “according to the distance driven by an individual” (Vaia et al., 2012, p. 114). In the second approach, PHYD, the premium is not only calculated based on distance driven, but on actual driving behaviour (Vaia et al., 2012). This includes detailed information about “the roads the driver uses [...], the time of day the vehicle is being driven [...], whether the vehicle is driven in bad weather and the frequency of “hard cornering” (taking very sharp turns fast), excessive acceleration and heavy braking incidents” (Vaia et al., 2012, p. 114). The “level of insurance premium [is consequently tied] to the risk level associated with driving behaviour of the policyholder” (Bolderdijk, Knockaert, Steg, & Verhoef, 2011, p. 1182).

“Insurance-oriented telematics technology began to emerge in the early 2000s” (Vaia et al., 2012, p. 114) and the first telematics-based insurance policy in Europe was implemented by an Italian insurer. Nowadays various insurance companies in the EU, Brazil, South Africa and the U.S. offer analogues policies. Those approaches are described as “the future of car insurance” and “gain popularity or even dominate the car insurance market” (Troncoso et al., 2011, p. 8) mostly due to their advantages for users and companies (Litman, 2015; Troncoso et al., 2011). The potential benefits can be grouped into three main areas: financial, environmental and societal (Vaia et al., 2012). The policies are believed to be substantially cheaper for customers and insurance companies (Litman, 2015). At the same time they are socially beneficial, “as they encourage responsible driving, decreasing the risk of accidents” (Troncoso et al., 2011, p. 1). Bolderdijk et al. (2011) show that the new insurance policies form an incentive to significantly reduce speed violations of young drivers and thereby improve drivers’ behaviour in a favourable way. This “in turn saves money for users and insurers” (Troncoso et al., 2011, p. 1). The environmental benefit can be described in terms of reduced pollution emissions and energy consumption as a result of improved driving style or reduced usage (Troncoso et al., 2011).

Despite the manifold benefits, Vaia et al. (2012) mention that it was the “creepiness factor of being monitored that has deterred broader public acceptance of vehicle telematics” (p. 115). These customer privacy concerns are confirmed by Troncoso et al. (2011) who state that the current implementations of Pay-As-You-Drive insurance systems “entail a serious privacy invasion” and “a fundamental disregard for the privacy of car owners, which might even slow or limit their deployment” (p. 8). They propose to “limit casual surveillance by the insurance company or any third parties [...], as well as preventing the aggregation of masses of location information in centralized databases” (Troncoso et al., 2011, p. 4). While Vaia et al. (2012) agree that “privacy and intrusive monitoring were a concern from the start”, they also mention that “there is a significant population of drivers in Italy and elsewhere who are willing to trade-off privacy for a bundle of insurance discounts and potential safety and protection benefits” (p. 116).

While auto insurance is not the topic of this work, it still entails significant similarities to our field of research and valuable insights into the problem area can be gained. By relying on usage-based driving information, various benefits are provided, but simultaneously the new policies entail the same moral and ethical concerns, especially concerning user’s privacy, as inherent in the Big Data or IoT phenomenon. Just as in the health and life insurance context the question is how people are valuing and perceiving the trade-off between potential risks and benefits. In the end, the success of the approaches is dependent on the customer’s willingness to disclose their information to the insurance companies.

## Appendix 2

### Structured analysis approach complementing Section 3.4

	From a customer perspective		
Publication	Arguments in favour of disclosing data	Arguments against disclosing data	Developed construct
(Christophersen et al., 2015)	discourage employees' unhealthy behavior		Health motivation
	improve users awareness about personal health		Health motivation
		wearable health-tracking devices in organizational settings risk disciplining employees, by tempting or penalizing them financially	Invasion of privacy
		health concerns are reduced to numbers	Data accuracy
	motivating people to get healthier		Health motivation
		future abuse of personal health data collected from wearable health-data tracking devices	Secondary use
		bring health surveillance into the everyday lives of people jeopardizing privacy	Invasion of privacy
	financial incentives to reduce costs		Financial benefits
	users begin to self-regulate their behavior toward becoming healthier		Health motivation
		health-tracking devices risk surveil and compromise privacy	Invasion of privacy
	By sharing health data they can collect rewards and avoid fines		Financial benefits
		health data could potentially lead to higher insurance premiums if the individual becomes classified as unhealthy	Discrimination
		The readings made by wearable health-tracking devices fail to factor in social, psychological, environmental and physical circumstances [32], which can all influence the readings and the state of a person's health	Data accuracy
		wearable health-tracking devices on today's market lack common standards and practices as they have not gone through any validation process [9]. Thus, each device or sensor could potentially collect different data even when measuring the exact same situa-	Data accuracy

		tion; they do not follow common standards	
		When health data is analyzed there is a possibility for manipulation, and the algorithms used can potentially be modified by an organization wishing to change the analytical outcome	Manipulation
		Surveillance and privacy  invade the privacy of employees as the wearable health-tracking devices are being used as a form for surveillance tools	Invasion of privacy
		Wearable health-tracking devices, operating as a form for surveillance tools, endanger individual's privacy	Invasion of privacy
		In the slipstream of wearable health-tracking technology lays privacy concerns on how wearable health-tracking provider's access and use individual's health data	Invasion of privacy
		The collected health data may be used for other purposes than what was originally intended	Secondary use
		the insurance industry could again turn to the health data wearable health-tracking devices collect and re-categorize what is considered healthy and unhealthy	Manipulation
		wearable health-tracking technologies. Since their birth they have not undergone any official tests and do not have to comply with a specific rule set  Companies providing wearable health-tracking technologies can, to some extent, make up their own rules in relation to how their specific device is measuring and collecting health data.  a risk that the lack of standards for wearable health-tracking devices could mean that a person's health data set might vary depending on which tracking device is used to measure and collect it	Data accuracy
		Wearable health-tracking devices cannot account for such external factors and contexts, they only collect the numbers, which could mean that a perfectly healthy employee find their health insurance priced unjustly.	Data accuracy

	In a sense it could be considered fair that obese individuals would have to pay a higher premium until they get healthier		Increased fairness
		By agreeing to one's health data being collected by wearable health-tracking devices it may affect future insurance options and prices, even if annulled, because the data has already become part of the digital health sets immortal memory	Secondary use
		wearable health-tracking technologies are invading the privacy of individuals by constantly monitoring and surveil them	Invasion of privacy
(Al-Saggaf, 2015)		Data mining also allows these companies to cherry-pick customers	Discrimination
		major privacy concern	Invasion of privacy
		potential misuse of information arising from data mining	Secondary use
		in reality, the included customers may not actually fall into the discovered classifications or categories, the criteria used for assignment may not be appropriate	Data accuracy
		makes it possible for people to be labeled and discriminated against or stigmatized	Discrimination
		data mining does involve the secondary use of personal information, which is one of the areas of major privacy concern. Secondary use is when information provided for one purpose is used for an unrelated purpose. Corey Angst notes that information gleaned from linked databases can be used in new and unanticipated ways, often without the knowledge of customers	Secondary use
		electronic personal information has the potential to be easily duplicated and shared with others who are not party to the original disclosure, often without the individual's knowledge	Secondary use
		this information may eventually be used by a number of other interested parties, such as potential employers	Secondary use
		may influence employment and employability, credit worthiness, and one's ability to get health insurance—in some cases it may affect the rates paid for coverage	Discrimination
		using data mining techniques in	Discrimination

		this way can encourage businesses to engage in discrimination against their customers	
		Data mining has the potential of allowing insurance companies to cherry-pick only those people who are healthy and require fewer health services.	Discrimination
		may even be denied insurance coverage	Discrimination
		A further challenge of data mining is that it is often not clear what patterns will be revealed from the data. This would make it impossible to clearly specify in advance the exact purpose of data collection in order to notify the data subjects.	Secondary use
	the use of data mining by PHI companies in Australia can help improve the products and services		Improved products and services
	the use of data mining by PHI companies in Australia can help with fraud detection		Increased fairness
	the use of data mining by PHI companies in Australia can facilitate the provision of tailored products and services and help improve products and services		Improved products and services
	reduce premiums for customers		Financial benefits
		the use of data mining by PHI companies in Australia can violate customers' privacy	Invasion of privacy
		the use of data mining by PHI companies in Australia may involve the secondary use of data  Secondary use of data breaches customers' right to have control over their own data.	Secondary use
		the use of data mining by PHI companies in Australia may involve using data for unintended purposes  using data for an unintended purpose could expose data to abuse, causing harm to individuals	Secondary use
		data mining can be used to classify a customer as belonging to a group that is likely to default on payments, a classification that may not be fair. What if, in reality, the customer does not belong to the group the classification	Data accuracy

		assigned to him or her?	
		The inability of the customers to correct their information contravenes their right to control their own data, thereby violating their privacy	Invasion of privacy
		data mining can be used by PHI companies to classify a customer as belonging to a group that is likely to develop a certain disease. If this is true, a customer may not want others to know this. For this reason this classification violates the customer's privacy.	Invasion of privacy
(Borna & Avila, 1999)		genetic information can be used to exclude an individual or an entire family from health or life insurance coverage eligibility	Discrimination
		The individual with an indicator trait may also be subject to a significant adverse premium rating	Discrimination
	Fair discrimination: applicants associated with low risk factors, both environmental and personal, will be assessed lower premiums than individuals with higher risk factors		Increased fairness
		insurance will only be afforded by those people deemed to have "healthy" genes and the rest of the population will either be deemed "uninsurable" or will be forced to pay a higher premium because they are considered a higher risk	Discrimination
		denial of health insurance  Insurance companies do not deny the possibility that when genetic testing becomes both reliable and accurate, individuals who carry defective genes may be subject to higher premiums or at worst be denied insurance coverage.	Discrimination
		if the applicants are forced to disclose this information to the insurance companies, it also will be more readily accessible to other insurance companies [...] and eventually to a number of other interested parties such as potential employers.	Secondary use
		Medical records are subject to subpoena, and thus may be used for purposes other than insurance underwriting (For a discussion of potential abuse of genetic data in	Secondary use

		context of employment discrimination see Schatz, 1987, and Strudler, 1994)	
		individuals with defective genes either will be denied insurance coverage or their insurance premiums will be equal to the morbidity and mortality costs plus administrative costs  This scenario is analogous to the situation when an individual knows that approaching flames will engulf his house within a few hours. An insurance company having knowledge of the owner's predicament will either deny the insurance coverage on the house or will set a premium equal to the value of the house plus administrative costs.	Discrimination
		insurance rates will be adjusted for the high risk categories	Discrimination
(Armstrong et al., 2003)		access will increase discrimination in life insurance premiums and discourage individuals from undergoing genetic testing that may provide health benefits	Discrimination
		fear of insurance discrimination	Discrimination
	so that they can price individual policies appropriately		Increased fairness
		insurance industry access to genetic information will lead to discrimination	Discrimination
		concerns about insurance discrimination may prevent individuals from pursuing genetic testing, thereby hindering them from adopting measures that may reduce disease risk	Discrimination
		almost one half of the women we studied expressed concern about future life insurance discrimination if they underwent genetic testing	Discrimination
		concern about insurance discrimination is an important barrier to the use of genetic testing despite the absence of evidence that such discrimination actually occurs	Discrimination

## Appendix 3

### Summary of all the factors contained in the preliminary research model

Construct	Definition / Explanation	Key supporting literature
<b>Perceived Risks</b>	“the user’s perceived expectation of suffering a negative outcome as a consequence of [...] disclosure of personal information”	(Dinev et al., 2013) (Dinev & Hart, 2006)
Invasion of Privacy (IP)	“the ability of the individual to control personally information about one’s self” <i>complemented by a general fear of being surveilled and “instinctive recoil”</i>	(Stone et al., 1983) (Solove, 2006) (Dinev et al., 2013)
Data Accuracy (DA)	“Each device or sensor could potentially collect different data even when measuring the exact same situation” (lack of common standards) <i>as well as</i> “The readings [...] fail to factor in social, psychological, environmental and physical circumstances, which can all influence [...] the state of a person’s health”	(Christophersen et al., 2015) (Al-Saggaf, 2015)
Manipulation (MP)	“possibility for manipulation [...] by an organization wishing to change the analytical outcome”	(Christophersen et al., 2015)
Secondary Use (SU)	“when personal information collected for one purpose is subsequently used for a different purpose”	(Culnan, 1993) (Christophersen et al., 2015) (Smith et al., 1996)
Discrimination (DM)	“treating a person or particular group of people differently, especially in a worse way from the way in which you treat other people” <i>especially adverse insurance premium rating</i>	(CambridgeDictionaries, 2016) (Armstrong et al., 2003) (Borna & Avila, 1999)
Security Concerns (SC)	Concerns about “the processes and methodologies which are designed and implemented to protect [...] confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption”	(SANS, 2016) (Britton, n.d.) (Lymberis, 2003)
<b>Perceived Benefits</b>	“Perceived benefits include all the benefits brought by the information disclosure behavior”	(Sun et al., 2014) (Dinev & Hart, 2006) (Smith et al., 2011)
Financial Benefits (FB)	“consumers exists who are willing to sell their de-identified personal health information”	(Hui et al., 2007) (Pickard, 2014)
Receiving a fitness tracker (FT)	the free wearable device is valuable for customers and constitutes a tangible reward whose positive influence on information disclosure was confirmed	(Hui et al., 2007)
Health Motivation (HM)	“pleasure or enjoyment derived from adopting and using a technology” <i>extrinsic motivation to be more sporty and healthier</i>	(Gao et al., 2015) (Christophersen et al., 2015)
Increased Fairness (IF)	“individuals with different risk factors [...] bear different costs for their insurance” <i>and</i> “measure as accurately as practicable the burden shifted to the insurance fund by the policyholder and to charge exactly for it, no more and no less”	(Borna & Avila, 1999) (Worham, 1985)
Social Image (SI)	“the extent to which user’s decision making is influenced by others’ perceptions”	(Gao et al., 2015) (Yang et al., 2016) (Kim & Shin, 2015) (Smith et al., 2011)

Improved Services (IS)	“the ability to proactively tailor products and product purchasing experiences to tastes of individual consumers based upon their personal and preference information”	(Chellappa & Sin, 2005) (Al-Saggaf, 2015)
<b>Moderators</b>		
Trustworthiness of Insurance Company	the user’s belief that the health or life insurance company will keep its promises and commitments, and cares for the interests of the policyholder <i>and</i> “trust reflects a willingness to assume the risks of disclosure”	(Wakefield, 2013) (Dinev & Hart, 2006) (Culnan & Armstrong, 1999)
Customer Characteristics	“individuals' intention to disclose such information depends on their trust, privacy concern, and information sensitivity, which are determined by personal dispositions”	(Bansal et al., 2010) (Anderson & Agarwal, 2011)

# Appendix 4

## Interview Guide – Semi-structured interview

### Introduction

- Inform about voluntary participation and confidentiality
- Confirm if it is ok to record conversation
  
- Introduction of interviewers and interviewees
- Explain what this interview is about
- Present new model of health and life insurance policies based on data collected by wearables

### *Warm up questions (Consumer Characteristics)*

To start off we would like to get to know you a bit better. Could you tell us a little bit about you:

1. How old are you?
2. Where are you from? Where have you lived most of your life?
3. Do you have a health or life insurance?
4. Do you own a wearable device?  
(If yes: do you wear it regularly?; if no: would you generally wear a health tracking device if it was given to you for free?)
5. Would you describe yourself as technology affine?  
Do you always have the newest devices?
6. Would you describe yourself as generally concerned about your privacy?  
Do you worry a lot about your privacy?

### Main session

#### *Attitude (7)*

1. What is the first thing that comes to your mind when you hear of this new concept of insurance?
2. Do you think it is a good idea to use wearables in the context of health or life insurance?

#### *Perceived Risks (8)*

1. Can you think of any negative consequences resulting from disclosing your information to the insurance company?

2. Do you think there are any risks affiliated to disclosing health information to insurance companies?
3. What do you think are the risks of disclosing your health information to insurance companies?

If not mentioned by the interviewee, ask about specific risks:

- Do you think an invasion of privacy could be a concern?
- Data accuracy
- Manipulation
- Secondary use
- Discrimination
- Security concerns

#### *Perceived Benefits (9)*

1. For what reasons would you disclose your health data to insurance companies?
2. Do you think there are any benefits affiliated to the disclosure of health information to insurance companies?
3. What do you think are the risks of disclosing your health information to insurance companies?

If not mentioned ask about specific benefits:

- Do you think that financial benefits could positively influence your willingness to disclose information?
- Receiving a fitness tracker
- Health motivation
- Increased fairness
- Social image
- Improved services

#### *Willingness to disclose information*

10. So considering all these aspects, would you be willing to disclose your health information to an insurance company?

#### *Moderators*

Can we ask you something about your health status? If participant is not comfortable with that: change question 11 and 12 to: Do you think your health status would affect your decision to disclose information to insurance companies?

11. How would you describe your health status? Do you have any severe illness?
12. Do you think your opinion towards the issue of wearables in the insurance context would change if you were in a different state of health?
13. Would you say that you trust your insurance company?  
(if no insurance: Do you trust insurance companies in general?)

## **Closing**

14. Is there anything you'd like to add in terms of the adoption of wearables for health and life insurance that you feel we should consider?

## **Debrief**

Thank participant for their time and inform about further procedure.

# Appendix 5

## Informed Consent Form

Qualitative Research conducted for a Master Thesis at the  
Department of Informatics  
Lund University

### Research Team Contact

---

Annina Oelschläger  
Ali Chehab

[gif15aoe@student.lu.se](mailto:gif15aoe@student.lu.se)  
[ali.chehab.813@student.lu.se](mailto:ali.chehab.813@student.lu.se)

### Context

---

The study is conducted in the context of health and life insurance companies. With the advent of Big Data approaches as a competitive strategy across all industries, also insurance corporations are starting to offer policies which are based on collected, personal data.

In particular, this means that clients receive a free fitness tracker when purchasing an insurance policy and agree to disclose the collected data to the insurer. The insurance premium is then individually and constantly calculated based on the personal fitness values and achievements. Starting from a baseline premium the customer might be able to reduce costs by achieving specific fitness goals such as increasing the number of steps taken or by reducing weight. Depending on the company, other comparable reward systems might be implemented. There might as well be risks associated with this disclosure of sensitive information.

### Description

---

The objective of this study is to assess the public opinion towards the usage of wearables for underwriting purposes and to identify and describe factors which influence customer's willingness to disclose sensitive information to their health or life insurance companies.

This study is being conducted as the Master Thesis in the programme of Information Systems at the Department of Informatics, School of Economics and Management, Lund University.

### Participation

---

Your participation in this project is voluntary. If you do agree to participate, you can withdraw from participation during the project without comment or penalty.

This interview has been designed for the general public, which means that anyone is welcome and encouraged to participate.

Your participation in this study will consist of taking part in a face-to-face interview, approximately 40 minutes long, although note that this may depend on individual elaboration on each question.

You will not be asked to disclose any confidential or sensitive information about you.

---

### **Expected Benefits and Risks**

---

There are no benefits or risks beyond normal day-to-day living associated with your participation in this project.

---

### **Confidentiality**

---

All responses will be treated confidentially. The names of individual persons will not be disclosed in the project or any related publication. You will not be identifiable from any outcomes of this study. No one outside the research team will have access to the information you provide.

---

### **Voice Recording**

---

The interview will be voice recorded for the only purpose of transcribing the conversation afterwards.

---

### **Consent to Participate**

---

By signing below, you are indicating that you:

- . have read and understood the information about this project;
- . have had any questions answered to your satisfaction;
- . understand that if you have any additional questions you can contact the researcher;
- . understand that you are free to withdraw at any time, without comment or penalty;
- . consent that this interview will be voice recorded.

---

### **Questions / Further Information about the Project**

---

Please contact one of the research team members named above to have any questions answered or if you require further information about the project, or have concerns about the ethical conduct of the project.

---

Date, Signature

## Appendix 6

### Transcription of Interview No. 1

Date: 26.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP1  
 Interview format: Face-to-face interview  
 Interview duration: 46:08 min  
 Transcribed by: Ali Chehab  
 Transcription date: 26.04.16

Question	Speaking	Text	Code
Q1	AO	For the demographics, we would like to know how old you are, if you are comfortable with telling us about it?	
	RP1	47.	
Q2	AO	You are from Sweden, right? Have you lived in Sweden your whole life?	
	RP1	Yes basically yes, minus 5, 6, 7 years. Yes, in Sweden.	
Q3	AO,	You already talked about the system in Sweden, that means you have a health or life insurance, right?	
	RP1	Yes, well again what you mean is everybody in Sweden has health insurance, even migrants begging on the streets have a Swedish health insurance. They are probably covered better than somebody in the U.S. who is not even working. So yes, I have health insurance and I have private insurance as well.	
	AO	So this is on top of that?	
	RP1	Yes, yes, well we have different insurances. I mean you have, incapacity insurance, if something happens, you get money if you are incapacity, and of course the state wouldn't pay money, they would just help you. So we have this type of insurance through trade unions and so on, if your hurt or if you have hospital expenses and so on this can be reinburst. Even in Sweden hospitals expenses are not very high, but there are some expenses, so those can be covered by insurance. These health insurances are very different from the U.S. basic health insurance. Lets say I have cancer, I dont have to pay anything. In the U.S. you pay everything in cash or your company does it. So that's basically, paying millions in cash compared to here. We don't pay anything and I don't need any insurance against cancer cause nobody would give me that. So all the insurance that I have is sort of cash reinbusrment, or cash premiums for different types of invalidities. It is a different system.	
	AO	I mean for example life insurance does also fall under it. They are also offering life insurance that is based on fitness trackers and so on that would apply for Sweden as well, right?	
	RP1	Life insurance yes, now here you fill in a health certificate, pretty basic, and it is basically calculated based on your health, and I think all insurance companies have access to, you need to check this, in	

		Sweden they have access to the health system. So they can check my journals. I know because my daughter has kids insurance which is quite expensive, and they check if something happens to her, or she had a disease when she was born so they check the patient system centrally, let say i try to find an insurance for her, and she has some sort of birth defect, they will see that in the system, again this wouldn't happen in the U.S. or most countries, but in Sweden they have access to patient system in some way. So you can't really lie to them, so it is based on that and not on fitness.	
Q4	AO	We see you're wearing a wearable device. Can you state what kind it is and what you are using it for?	
	RP1	Yes, it is an Apple watch, and I use it as a watch, not so much for fitness, I have another watch for that and lots of other wearables for fitness. Actually this is a bad fitness device for real fitness, I mean I run and you can't have this, I need to watch this all the time for example. I have another thing when I run, this wouldn't actually catch it because I charge this when I run, but then I use it for sleep tracking as well, it is not one of the intended features, it should be charged while sleeping, but I like the sleep tracking because it checks the pulse, and I've never had that type of metric, because it is very interesting to see your pulse at night. That's a way of tracking your fitness. Yes anyway and I use it for all usual things, notifications, I can see traffic, breaking news, whatever.	
Q5	AO	So you said you had other devices, like fitness trackers as well, so in general would you describe yourself as a technology affine?	
	RP1	Yes.	
	AO	So you always have the newest devices? And try out new things?	
	RP1	Yes sure, some of them.	
Q6	AO	Would you describe yourself generally as concerned about your privacy?	
	RP1	Yes and no. Not very, medium if you have a scale, so no, in certain senses yes but not in others. Depends on what you're asking about.	
Q7.1	AO	If we are coming now more to the concept that we just introduced with the health insurance, what is the first thing that comes to your mind when you hear about this new policies and concepts established in the U.S.? What do you think about it?	
	RP1	Yes, again they are not applicable here. Companies could do it, and I think there are companies, we have a former colleague here who has written a book about this. Yes, it would benefit me if that is what they're looking for. I mean, I run marathons and stuff like that, so from a U.S. perspective I will be an outlier I guess most companies in terms of fitness, but if I have lived in the U.S., I wouldn't have the time to do the fitness I do here, so I don't know. So I wouldn't mind, but principally I think it is a bit intrusive, yes for other people who are not very fit. So, I don't like the policies pretty much.	IP DM
Q8	AO	If we dig a bit deeper there, you were talking about the intrusiveness. What specifically do you think are the risks coming with this device? What negative consequences would you expect?	
	RP1	I would need to see it case by case, what companies, what are they doing, you said they're handing in fitness trackers, well I would hate that because I don't want to wear crap, they're handing in crap arm bands and stuff like that. They are incorrect, they are in-	FT DA

		trusive physically, cause I don't want to wear it. It is like BYOD (bring your own device) where you work in a company where they hand you a computer and the phone, or a tablet and whatever and it is all crap, I don't want to use. People today have certain interests and preferences of hardware, we live with this 24 hours and this is like 'now you have to use our crap'. So it would be intrusive in that sense. I don't want to wear their lousy cheaply purchased fitness devices. And having to wear them as well I don't want to have something on me that I don't trust my self. So that is estatically intrusive in that way if that's what it is, I don't know and you havn't told me what it is.	FT DA
	AO	Yes, basically you are obliged to wear the device, they provide you with.	
	RP1	So it would be physically intrusive, and also silly cause you can't know who is wearing it. You can put it on your dog, and get lots of steps from him or give it to you kids while they are playing, I just find it a silly idea	FT MP
Q8.3	AO	So you were talking right now about room for manipulation from the customer's side, what do you think about manipulation from the company side? Do you think there will be a risk that the company is actually messing with your data? Because you can't really control what they are doing	
	RP1	Ya, I don't know in what context, this is something you can see and get feedback because really when you use those devices like fitbit and so on there is a competition or a gamification aspect where people pit people against each other, and they compare. There is a peer pressure to start moving more, and people do this voluntarily of course through apps and so on. What you are implying is that you get something that is a blackbox and no body sees the data but the company, so there is no social component or self control.	
	AO	You also have an App, one example ist hat you have to reach a specific level of steps taken, and you can see that in your app and if you achieve this level, then you premium will be lowered, for example.	
	RP1	I think, it is silly use of technology. I don't know how they can track this. I mean steps is just steps, those cheap devices can't tell who is using it, maybe they have some biometrics, am too concerned about details. So I would have to know exactly what the case is too be able to answer about it. Maybe some companies do this as it will be fun and will have a social benefit. Everybody will start moving more, and will have sort of thing that people can compete and so on. Trying to do it in the positive way, maybe thats like what you have, you give out. University gives some premiums to do sports. You can sign up for the gym and get 2000 Kr or something per year. So you can do whatever any sport activity, but you bring a reciept and say this is my wellness or sports activity I want to do and I want the premium. So you can have it in sort of positive push, or you can do it in a negative way, and connect it directly to the premium and state that if you don't move enough you will have liability, so it depends on the exact case. But in general it sounds stupid on many levels.	DA HM
Q8.4	AO	Another risk we were thinking about was, secondary use, so that the insurance company might give the data to third parties, is that a	

		concern, you would consider in that context?	
	RP1	Again it is completely US. perspective. But yes it would be a concern if a company owned my fitness data or stored my fitness data, yes that would concern me. I mean there are companies that have my fitness data like run keeper, they can sell it, I don't mind. To sports manufactures or whatever and they probably do, and i don't mind that, but i would mind that especially if I wasn't very fit. I mean for my next job if it goes out to some sort of general data base that you can tap into or employers can tap into, you have to realize that fitness is not the measure. Lets say you are a hacker, you work at apple, programming or something. Then you can't be a marathon runner, cause you need to spend so much time doing those sports. So, it is better for a company like apple to have someone working 16 hours a day in front of the computer. They use him for 10 years, and then they waste him, let him go before he is too old. You just take in somebody young use them for 10 years, 16 hours per day and then you let them go. Then somebody else will have to take the health insurance thing. Before that you only have minor problems ergonomical issues. It is more complicated than that. Somebody who is into fitness is typically quite egoistic and actually prioritizes training and stuff like that. You can't be fully productive. I know people who train a lot, and all they do is try to decrease their work time they work 75% and then 50% and they try to get jobs that are not demanding, so I don't know, that is not the type of person you want either. So there is sort of correlation where fitness or you need someone who is sort of fit, but then again maybe not you want a fat guy who might have no interest but the computer for that job. And doesn't move at all, and thinks it is difficult to move, and he is happy to sit. Then you can let him go at a certain age when he starts getting problems, and get somebody young.	SU
	AO	So what you say is that you are in a very good state of health and very keen to fitness. If you had another status would you think this would influence your perception of this whole thing?	
	RP1	Yes, I would be more, of course yes I would be more, on one hand from a swedish system, yes I think it is good if you motivate people to take responsibility for your fitness and more people should do it. That is more from a societal perspective, from a company perspective, I don't think it is the companies business to do that, they should not.	HM
	AO	We are actually interested in your own perspective so the customer side.	
	RP1	It depends on who is doing this, giving away data to somebody who then can control me with incentives, or create different types of schemes that punish me, for example I have to pay more, and from a state perspective I can see this a bit, I mean works for me but not from a company perspective, because I don't think it is the companies business to do that. It shouldn't be the company that is in charge of health insurance. So it is totally different philosophical systems you could today, and it will come in the future the things in the car like a complete GPS system in Sweden or in any country should be registered and tracked at all times. And every thing you do could be tracked and the data is sent so you can know that this guy is speeding, these roads are limited to 70 where he is driving	

		90, so you can get big data from that. And that should go directly to the police as well as the insurance companies. I would be all for that, even if I run the risk that those people would know exactly where am going, how much am going, if I have a mistress that I am visiting. They can see all those things, I wouldn't mind. The benefits of that are far upway. I already get lower premium cause I don't drive like that and half of malmo would get premiums that they couldn't even pay. And I will be fine with that and the streets will be empty. In certain instances if the streets state monitors their citizen, for example how they drive even if it is intrusive, I am all for it. The benefit is huge for the whole society, and the same thing here if the company is doing it, I wouldn't like it, but if the state, I would be too happy.	
Q9	AO	Going back to the benefits. You mentioned that in the context of the car, what would you say are the benefits in the health and fitness context. Already you said that the premium will be lowered for you...	
	RP1	Am not sure if the premium would be lowered because as I said, have you talked to any insurance companies like how they calculate their premiums?	
	AO	We researched over the internet, and yes we have an idea.	
	RP1	For health, yes I mean from a state perspective, if I am going to stay in Sweden and that is likely because most people do, mostly because of the health system. Doesn't really make sense to move. So from the state perspective, looking at my whole life, yes it is important that am fit from a whole life perspective. From a company perspective, if they don't plan to employ you for your whole life, then it is a different perspective. And also I am not sure, if there is a correlation here, if you are so active and into sports and things like that. I don't do it as much but lots of people they travel and do cycling in the alps, these people from insurance perspective they are actually at higher risk of something dramatic happening like crashing with your bicycle and there is a huge cost involved with that, transporting them by airplanes back to Sweden. The better person for an insurance company, not looking at the whole life aspect for insurance perspective might be a sedentary person that isn't extremely overweight but keeps a slow life watches TV, goes to job and back, have a low key interest and so on or maybe walks his dog. An average person that you might not think, but the extreme sports person, I don't think he is a good profile for the insurance company. The states perspective over the whole life, is very different, cause then the cost of cancer or even the cost of transporting the bicycle racer back from Italy is very small compared to someone getting cancer at a young age because of lifestyle choices. So, there you have a different perspective, again insurance companies in Sweden don't pay for cancer medication. So they just see the risk basically.	
Q9.4	AO	For you basically the car context, you said you really liked that because people who are behaving in an inappropriate way have to pay more and you stick to the rules. So is this increasing fairness?	
	RP1	I wouldn't actually pay less, but it is that other people might pay more. No, but it is the safety thing I mean for kids and for my self. I would like to see these people of the street basically or constantly	

		fined to change their behavior.	
	AO	In the health insurance context, you would'nt see like increased fairness as a benefit for yourself? People who are not sticking to any healthy life styles?	
	RP1	It is a difficult question. It's more about morality and imposing it on other people. For example people who smoke, shouldn't or even eat certain stuff and never work out despite all the knowledge we have now, you should do this at some level, but it is a different morality, because driving a car might have great consequences on other people when misbehaving with the car, but the problem with the life-style choices is that in the swedish system where the state pays for that it becomes more problematic than the US. where nobody pays. Well the company pays if you are employed, because in the US. if you don't have a job or if you have a low paid job, they don't provide insurance. It is complicated now, cause now they have the Obamacare, but lets say in other state where you don't have health insurance at all, so if you make bad health style choices, okey you will die young of cancer or something like that, but that's your choice, you won't get any treatment unless you do a kickstart campaign, people who start online charities cause they have cancer and so on, or what they do typically is ask the family to pay, distant uncles, and aunts, so that can happen of course. In Sweden it is different, everybody pays for the life choices of other people, there is a certain aspect where you want people to be responsible, you have to be careful with your system, we already do that, we spend lots of money we have compulsory sports in schools, so state does lots of things like I said every state employer like the university will give money for sports activities and so on we have incentives for this.	
Q10	AO	All in all, considering all these risks and benefits now, if there would be an option like for example an additional insurance here in Sweden which is employing these new things, would you buy a premium policy?	
	RP1	Again you have to talk to those people am not sure that they want, I would be worried that they think am doing so much exercise too many races. I don't think it the perfect, again that ist not the state that is insuring me against cancer or long term health, so it could be intrusive, or negative for me, they could see that am doing too much or crossing the threshold, so I am at a higher risk of getting injured or having a heart attack during a marathon or something, so you actually have to pay more so am not sure it would benefit me. On average i don't think it would be very beneficial, cause they are looking for more talking about the swedish context here, every insurance wants somebody who does everything in moderation and sits at home and walks the dog. And thats it. I don't know how they reason about this, anything you do even if it is sports or whatever you do, it is negative from their perspective. Again their perspective is not the state perspective that covers me from birth to death it is a very different perspective having to pay for cancer and heart disease and diabetes and all those things is not the insurance companies problem, thats the state's problem. It is very difficult to ask these questions having a fixed context which is the Swedish system, considered a unique system in the world or is it the Us. or is it something else.	

	AO	Actually we are considering asking a lot of people from different countries. As we are only taking the customer perspective, we are not taking into account those legal frameworks and stuff. We are just trying to examine the general attitude of the people towards those behavior and if it would be good to implement such things or not.	
	RP1	Everybody is aware of who is their customer, am a customer of the swedish state in a way that in the Us. I don't know. What is your home country?	
	AC	Lebanon	
	RP1	Yes I guess your not state funded.	
	AC	No, usually we pay for insurance. It could be an added value to have wearable devices, to exersice and retain better health.	
	RP1	Not necessarily in Lebanon but in the midle-east you have diabetes problems, everybody is getting diabetes at 30, in Qatar KSA.	
	AC	In Lebanon this is not the case.	
	RP1	Ya i guess ya, but it is different everywhere, like in Germany is it like the Swedish system? But not fully, right?	
	AO	We still have to choose an insurance company. It is not the same as in Sweden.	
	RP1	You don't have complete health coverage, but you have some, what happens if you get cancer?	
	AO	You have to have an insurance, there is difference between private and state insurance basically you choose which one to have, and which is offering you more services than the other.	
	RP1	Okay, you have to choose, but is it for free?	
	AO	No, if you choose the state, you still have to pay	
	RP1	If you are a homeless person, or somebody who doesn't give a shit, just live your life	
	AO	Am actually not sure, but I think then you don't have anything.	
	RP1	Nothing? You die on the street?	
	AO	No, I don't think so.	
	RP1	That's very complicated. In Sweden it is not complicated, you don't die on streets. I mean if you are swedish, it is not complicated, you can be homeless or whatever the state will pay for every thing and now for example migrants, yes they pay for dental, so if you are a migrant from Romania, you will pay for dental care. And your medical urgencies and child care if you have a baby. But I don't know about cancer in these things, if they get complete cancer treatment in Sweden, so basically we are covering both, Sweden and other and there is a political discussion if we will cover the world actualy. But it will be difficult based on the Swedish tax to do that. Again Sweden is completely different context from all the others. I am a customer to the Swedish state and then I also have private insurance, but these things are more topups. You know the most important thing is that if you get canseris not to get a bag of cash from an insurance company, you know your insured against bad accident. The most important is that you live, and you dont have pain, and the swedish state covers that, but yes if you dont have the swedish state as i know from the US. Your in trouble, i mean basically you have to slowly die in pain, take your life, people do that, or you typically get something coveredbut then you need a lot of extra cash to get	

		better treatment, a higher quality traetmets or seek advice from second opinion, so you have to run to your family, someone in your family might have money, and you really have to go down on your knees to do a fund raise do fund raise with your company or where you work, so its really tough. And that is a completely different perspective	
Q13		From an american perspective do you think that insurance companies can be trusted?	
	RP1	I don't know I don't live in the US. In the US. People don't trust people very much there. Thats why they have this system. The U.S. system is based on you don't fall ill. If you do that, fuck it you die, it's bad luck and you know who cares then. So it is based on that, and I don't know, I wouldn't trust companies in the US. No, not much. But i don't live in the U.S., am not American, and if I went there, I would know that, else I would go here and this is you know, but am still Swedish of course lets say you can renounce your citizenship. What happens typically is people get ill, they go back to Sweden. So people immigrate for usual reasons, success luck, and love and then they go back if they fall ill. Swedish base, they don't get the taxes, I have a friend, she went to Australia and married somebody there. She is a researcher, then she had a baby, and then she got cancer at the same time, so she had to move back. But it was benine, not benine it was real cancer, she was cured so when she was over she went back. So that's what people do, they move back when they get sick, if you have an extreme accident its more difficult. I mean Sweden is totally an outlier here.	
Q14	AO	Besides this different context is there anything you would like to add to the general topic of the adoption of wearables in this insurance cotext? What do you think we havnt considered? Or anything you would like to add?	
	RP1	I don't think it will be a big thing for insurance companies. It will be a big thing for the health industry and for people in general, so the health care system I should say and not the industry cause people have this, i mean data that I have now about my sleep patterns and so on That's data that researches look at, which is one way of tracking heart health, I have seen the studies so you track people through their sleeping and their heart rate, which is really interesting to see what is going on. Typically we are talking about resting our grade and so on to determine these things. Iam already doing experiments at home that researches have trouble doing. If i can do it, anybody can do it with an apple watch or something similar. So in the future when most people have something like this you can gather all these data and then you can do it for personal perspective or for big data perspective. You can have all those data feed into a sort of system, again in Sweden its not a good, we don't have a good system for this since we don't have our personal medical records, I don't know in Germany if you have personal doctors, you go to family doctor or something like that you choose I guess or you have a family doctor, the person you go first of all that can do typical checkups. In Sweden we don't have that, we just go to a central and could be anybody there. So we don't have a personal relationship, but if I had a personal relationship I could ask him some time in the future when we have systems for this. I do I have blood pressure monitor at home, I have a scale that is connected to wifi, so	

		<p>every time I step on the scale, the weight is most important, of course it calculates BMI, and tries to do sort of fat, but I have the blood pressure monitor, it is accurate to a medical degree, all that data is already being collected, it goes to different places like within a company doing those devices, it's already there, but I could tap the data straight in my, and I would like that to have my doctor see this data. So next time i meet him he can pull down all the data from last year, he can see my sleeping data, blood pressure at different points my weight and in the future, I guess we will get some more. Sure you can do blood tests at home and stuff like that, and send in, you can do it already today.</p>	
	AC	It is already there where you have the jack and plug it in the USB.	
	RP1	<p>Yes for diabetic people, yes they can do that. That would be revolutionized things you could do with the already collected databut not used like my sleeping my heart rate during training so all that data could be used by doctors and its not being used at all so if we revolutionize the health system but this will take a long long time and actually this will work better in places where you have connection with one person or somebody who takes care of you so you have one way communication, but yes, it could work in sweden as well if I allow my data to go to a central system and every body or if i charge into a hospital they could see my data, and make sort of sense of it, but its long long, were really not there and we would need probably an artificial intelligence strenght software to process all that data and make it relavent for somebody, you know you come into an accident, and they can get all you data, so they say okey this person is fit, that means something for treatment. He will probably he will take a higher dose of whatever medicine, you can get all those data quite quickly if you have all these things going on, maybe some one who is older and he's got heart problem he wears something like this and the data is automatically is fed into some database if he gets some trouble the emergency doctor can see all these data, the last couple of days his heart rate has been elevated, his blood pressure has been strange, there is something going on, and they know that, so all these things will and other sensors, and other type of data will become available, right now its just heart rates, blood pressure, you have to put on the cuff, I dont do this very often, its not an automatic thing, but then we have the types of sensors am sure so that will transform the health system which inturn, again in sweden the health system, the insurance system is tight into the health system. So they communicate, I dont know exactly how transparant it is, but my daughter, I know its transparant they can get into her patient journals, what ever you can call them in english, so health system will be transfered by this eventually which inturn will ofcourse build applications for insurance and for states such as Sweden as you can see more clearly what people are health state of individual is and you could apply different schemes, programs, and so on at more individual basis but it is very far in the future.</p>	
	AC + AO	We would like to thank you for your time.	

**Transcription of Interview No. 2**

Date: 26.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP2  
 Interviewer: Ali Chehab  
 Interview format: Face-to-face interview  
 Interview duration: 22:14 min  
 Transcribed by: Ali Chehab  
 Transcription date: 26.04.16

Question	Speaking	Text	Code
Q1	AC	We will start our interview by asking you some questions about your characteristics, and if you don't mind telling us your age.	
	RP2	Yes, I am 62.	
Q2	AC	Where are you from? and Where did you live most of your life?	
	RP2	From the southern part of Sweden.	
Q3	AC	Do you have a health or life insurance?	
	RP2	No.	
Q4	AC	Do you own a wearable device, like a fitness tracker?	
	RP2	No.	
Q6	AC	Would you describe yourself as generally concerned about your privacy? Do you worry a lot about your privacy?	
	RP2	No, not really. I think, it is okay to make a conclusion of my state.	
Q5	AC	Would you describe yourself as technology affine? Like a person who buys the latest technology products.	
	RP2	No, not really.	
Q7.1	AC	What is the first thing that comes to your mind when you hear of this new concept in the insurance industry and wearable devices in the insurance industry?	
	RP2	The first feeling is a bit unsecured, in terms of how the data is going to be used. Are they going to be used correctly and of course all these... how do you say? When they take your data and use it for other things.	SU
	AC	So you mean like secondary use of data?	
	RP2	Yes.	
	AC	Other than that, do you have any threats?	
Q8	AC	Other than that, do you have any threats?	
	RP2	No, not really.	
Q7.2	AC	Do you think it is a good idea to use wearables or fitness trackers in the insurance context?	
	RP2	Yes. Well, it could be.	
	AC	How?	
	RP2	I don't know really, but it could be some benefits of that.	
Q8	AC	Can you think of any negative consequences resulting from disclosing your information like giving out your information to the insurance company?	
	RP2	Well, it is money. Money talks, money sells, money buys.	FB
	AC	So you think money is a negative consequence?	
	RP2	It could be, speaking of using it to get more money for the companies not mainly for doing things better for me. Just making profit for their company.	

Q8	AC	Do you think there are any risks affiliated to disclosing health information to the insurance companies?	
	RP2	There could be risks, yes. Like for example they make the data so that they would make more profit instead of me getting any good out of it.	MP
Q8.1 + Q8.2	AC	Do you think there are problems with an invasion of privacy, or data accuracy?	
	RP2	Yes.	
Q8.1	AC	How can they invade your privacy?	
	RP2	Well my privacy, well maybe I don't understand it, but I am thinking of that they could use it. For example we have this in Sweden right now going on with the dentists.	
	AC	Can you tell us about it?	
	RP2	They look through all your teeth and see what state you are in, and because of what state you are in, you are going to pay a certain amount of money every month for a year and then they will do everything that you will need. But at the same time, you can a bit manipulate things, so that they could put you in a level that you shouldn't be. So, they make you pay more than you really should. And, it could be that when you are there and they are doing that status of you, maybe it is a bad day, because they are not only looking about how the teeth are, just today, they are also asking lots of questions: Are you smoking? Are you drinking wine? Do you eat proper three meals a day or whatever... so it concerns to what you are giving them for an answer and that could be not really okay for just that day. It could be.	MP
Q8.2	AO	You were also talking about the fact, that it is measured at one specific date, and that might be inaccurately reflecting your health status. Do you think the same problem would persist when you have the fitness tracker which is measuring every day what your doing?	
	RP2	But then this is a bit more sure.	
Q8.2	AO	But it is also measuring specific things for example the number of steps taken, and it is not measuring any other external factors. So, do you think this will also affect the assessment of the insurance company; how they rate you?	
	RP2	Maybe not if it is taken that often. Then it makes it a bit more sure, I should say.	
Q8.5	AC	Do you think it could be considered discrimination to provide you an insurance policy based on your health status? For example, if you are healthy, they will provide you with a lower health premium, whereas if you are not healthy or you might have a chronic disease, you might have a higher insurance premium? Do you consider this as discrimination or consider it as fairness?	
	RP2	More like fairness, I should say. Because, for example, if a guy is going to employ somebody, he could get hold of this record. He might say that he is a bit risky because he got that and that disease. I won't employ him. So again, it is more fair about how the state is going to be used and how safe the data is. That would be terrible if someone wouldn't get a job because he would be diabetic or whatever. Because they say that "ooooohh he's going to be away from work for this and this amount of days" and yes, this is no good. That would be terrible. Maybe you could call that discrimination.	DM

	AO	In the insurance context it would be like, you won't get an insurance because the company sees that you are a high risk, so they won't assure you.	
	RP2	Yes, it is the same for example if you are a female and you are 25 years old, they would know that you would probably have a child in the next five years, so they won't employ you, because you are a female. That's really discrimination. It is not only fair.	
Q8.6	AC	Do you have any security concerns regarding the wearables or fitness trackers or the insurance?	
	RP2	No.	
Q9	AC	Do you think there are any benefits affiliated to the disclosure of health information to insurance companies? What benefits would you take as a customer?	
	RP2	I thought this was going to give me some good in the end, if I was sick or help me with those kind of things. Not get a benefit in the beginning. You mean that they will give me something, if I say ok I would do this?	
	AC	What would you benefit from for giving your data to the insurance company?	
	RP2	Well, I don't know.	
	AC	You make sports, right? You go swimming.	
	RP2	Yes. You mean that they would thank me and pay my swimming for a year or something?	
	AC	Maybe they can give you something in return for the activities you are doing. Could it be an incentive?	
	RP2	Well, it wouldn't be that I should say yes or no, it shouldn't be because of a present. Either I want it or I don't want it. It is not that I'll do it, because I do get a pen or whatever.	FT
	AO	What would make you want it? What would influence your decision to buy such an insurance policy?	
	RP2	Then it would be, if I could get more specific health care. If I could come to the doctor and say I am not feeling okay, and he says 'okay, have you got this?', and I say 'yes, I have got it here', then he can take the data and look it up. Then they can use it.	IS
	AC	So you think using data for better health systems?	
	RP2	Yes, not going from one doctor to another, before I get to the right one. Then, I could go to the right one directly, because they know my history.	
Q9.1	AC	Do you think that financial benefits would positively influence your willingness to give away the data? So, if you receive a 5% discount on your premium, would you mind giving your data out to the insurance companies?	
	RP2	Well, because it will cost me any how. So, of course if I can get a lower cost, that is always interesting.	FB
Q9.2	AC	You would receive a free fitness tracker, a free fitbit so you can track your exercise and sleeping habits and all those..	
	RP2	No, but I want to do it my way anyhow.	FT
Q9.3 + Q9.4 + Q9.6	AC	Don't you think it leads to health motivation, and increased fairness or improved services? Through providing your data? Like you want to reach the specified target the 10000 steps...	
	RP2	No, I don't think so. We have had this at my work. We all got one of these you know, you should walk, and the young guys they start-	

		ed directly to compare with each other. But we girls, no.	HM
	AC	So it created a sort of competition at work?	
	RP2	But only among the young boys actually.	
Q9.6	AC	Do you think through this data they can improve their services, like the company can provide you with a specific service for you, based on the data you have provided?	
	RP2	Oh yes, I think so, yes.	
	AC	What type of services can they provide?	
	RP2	I don't know, I was just thinking, because at work right now, we have for example massage, every second week a girl is coming. This is of course making things for us feel at least a bit better. They are taking care of us, and they want us to feel healthy, and that is a kind of benefit from both sides. They give me the time that I am lying on the bench, and I am feeling better... Maybe that is not correct, but maybe that is the kind of benefit I should say.	
Q10	AC	So considering all these aspects, would you be willing to disclose your health information to an insurance company? Having the risks of your privacy and the benefits you will get, if you weigh them together... Will you be willing to provide your data?	
	RP2	I do think I would.	
	AC	Can you please clarify it? Why would you come to that decision?	
	RP2	Curiosity a bit. And of course, I would like to have a kind of insurance that the data will stay there and it won't be spread. Nowadays, I know everything is spread. This is the future we are talking about. I think mostly it would be curiosity. There is nothing wrong with me now. It is not because I want to check up this and that. It is nothing like that. It is just a bit of curiosity.	
Q11	AC	How would you describe your health status?	
	RP2	It is good.	
Q12	AC	Do you think your opinion towards the issue of wearables in the insurance context would change if you were in a different health status?	
	RP2	Maybe, yes. I think it could, because I don't think then I would be that positive to tell everybody about any illness that I had.	
	AC	Even the insurance company?	
	RP2	Yes, I think so. I would be more careful.	
Q13	AC	Would you say that you trust your insurance company?	
	RP2	Well, not really. It is something that you need to have. You need insurance companies for lots of things, to be able to have the same status that I have today, and if anything happens... so, it is a kind of give and take. If anything happens, they will probably help you, and if nothing happens, I have lost the money or whatever, you can see it from 2 sides.	
	AC	Yes, but your holding the risks by yourself, so you need those insurance companies.	
	RP2	Yes, yes I do.	
Q14	AC	Is there anything you would like to add or you feel that we should consider, and we did not shed light on?	
	RP2	Well, I was thinking that we are only talking about some very small things and maybe few things that should be taken care of is nothing more heavy things like what kind of medicine you take or things like that...	

	AC	Actually the new device are able to check glucose level in the blood and the future of those devices is promising.	
	RP2	During the questions, I was very much thinking of my mom who died a couple of years ago and had Alzheimer. And she forgot all the time all the time... it would have been very nice, if anything could call out and ask her: "have you forgotten to take your pill?" or "did you remember to take your pill?", something that could tell her and give her hints that something was truly happening. I was thinking further on that line.	
	AC	I think, it would be a good idea as well, because once you told me that she was lost, so if you can track her location through the wearable device...	
	RP2	Absolutely, it was something that I talked about very much at that time which is about 10 years ago. Or something 8 or 10 years ago. They wanted to put those watches to track where the nurses were, to check if they didn't really do anything like went and have a cup of coffee when they went from one patient to another. And I thought that was really silly, because they should put these on the sick people instead as my mom went out walking and she couldn't find her way back home. That could be so easy for them to check. "Ohhhhhh look now she is out walking again" and when I talked to the police when mom was out walking once, the police said this is a very big thing for them. They are very often out, looking for these old people without shoes and without any coats. And that really shouldn't be the police work. So put the watch on them.	
	AC	Thank you very much for your time and answering our questions.	

**Transcription of Interview No. 3**

Date: 26.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP3  
 Interviewer: Annina Oelschläger  
 Interview format: Face-to-face interview  
 Interview duration: 20:06 min  
 Transcribed by: Ali Chehab  
 Transcription date: 28.04.16

Question	Speaking	Text	Code
Q1	AO	To get started, we would like to know some things about the demographics: So, can you tell us how old you are?	
	RP3	24.	
Q2	AO	And where are you from? Or where have you lived most of your life?	
	RP3	Born in Sweden to a Scottish dad and a Swedish mom and I've lived in Sweden until I was 19 and then I moved to Scotland and lived there for 4 years.	
	AO	So you mainly identify as Scottish?	
	RP3	I identify as half half and I have never fully identified with either nationalities.	
Q3	AO	Do you have a health or a life insurance?	
	RP3	Not that I know of.	
Q4	AO	Do you own a wearable device or a fitness tracker?	
	RP3	No.	
Q4.1	AO	Have you ever considered buying one or would you be willing to wear one?	
	RP3	No.	
Q6	AO	Would you generally describe yourself as concerned about your privacy in any context, like the internet or whatever?	
	RP3	Sometimes, it depends on which site am at. Facebook: no. Because it is such a big part, but like Instagram: a bit more concerned. Depends on where really.	
Q5	AO	And would you describe yourself as technology affine? So do you always have the newest devices or are you more like a bit conservative?	
	RP3	I am a bit conservative.	
Q7.1	AO	So then coming to the main concept, what we just talked about, the insurance industry and the fitness trackers: What is the first thing that comes to your mind when you hear of these new insurance policies?	
	RP3	Why? I instantly question why anyone would suggest introducing this in the field.	
Q7.2	AO	So you think it is not a good idea to do that?	
	RP3	I think, it is a great idea for the business, I don't think it is a great idea for the individual.	
Q8	AO	So if we elaborate on that a bit: What do you think might be a negative consequence for you from a personal perspective?	
	RP3	I just don't think that how I choose to live my life should effect	

		what I pay for my insurance more than a generalization aspect, because, there comes a part where businesses try to micro manage what we do as individuals and how can they save money on certain individuals while others don't. We also know that health particularly is connected a lot to your economic background and your socio economic surroundings, so we already know that rich people have to pay even less because they can afford to live healthier lives, whereas working class people who can't afford to live as healthy, would have to pay more. So that kind of what I mean, that micro management aspect but also the fact that it would further rig the system against the people already disbenefited by it.	IP DM DM
Q8.5	AO	So that would refer to a kind of discrimination against poor people...	
	RP3	Yes, we could say discrimination, but also just further making it difficult for vulnerable groups to kind of make the class journey, the transcending of class, because it's just a further obstacle on to both their economy but also their personal life.	DM
Q8	AO	So maybe more from a personal perspective, from you: What do you think could be negative consequence for you?	
	RP3	I don't like to exercise and I don't want to have to pay more for my insurance. Because I don't. It is like I exercise to a reasonable extent, once or twice a week and try to walk but it just comes to this point where I don't think that because anyone has a different interest, like if a friend of mine loves to go to the gym all the time, I don't see why it would be fair that they pay less insurance than I do. Also, it is stupid that they have to pay less for the insurance, because you know there are more accidents that happen in the gym than just staying at home, so...	DM
Q8.1	AO	Do you think transmitting data to the insurance company will also mean an invasion of your privacy? Will you be concerned about that?	
	RP3	Yes, I would. I would be concerned about which data will actually be transferred. If you wear something, and they tell you, "oh, we are only taking this information; this is the only information that is being send", I would feel like I don't have enough control to know what kind of data is actually being sent to them, and yes I think I would be concerned... But this is also the consent part. Because I am assuming that I already consented to sending the information to them by wearing the device. And at that point it is also kind of transcend the privacy. So I agreed to send them my data, so in a way I already made that decision. But I would probably still be sometimes, you know, lying awake at night suddenly the thought would strike me "Oh my god what if they are recording me right now? Would they know I am masturbating right now?" It is like "Oh my god" and I would be very concerned about these kinds of things; about what they could find out about my private life.	IP IP
Q8.2	AO	So a bit more from a technical perspective: Do you think the accuracy with which the fitness tracker is measuring your fitness level, is appropriate to base the insurance on that or do you think it might not be precise enough?	
	RP3	I don't think it is enough, but I also think that we know that no system is perfect and no model is perfect. And everything is always based on not enough. Like, a data that we find accurate or satisfac-	

		tory, but not 100% guaranteed. So, I supposed it could be done better, but in terms of the accuracy, I don't think that would be an issue for me.	
Q8.3	AO	Do you think there might be the danger that the insurance company could manipulate your data? Like you send it to them and then they asses your health status based on that, but they could just change the criteria, however they want, right?	
	RP3	Yap. Changing the rules. I mean Facebook does it all the time, when we have to agree to new user agreements, and it is just automatically done. So, I suppose that is a very good point, it is another thing for future discussions.	MP
Q8.4	AO	Would you be concerned that the insurance industry actually gives away your data to third parties?	
	AB	Not just my data, if my name with my data, I could be concerned about that. But just my data I wouldn't care about, if it is just numbers on a page.	
	AO	Do you think that is like a realistic scenario that they will give it away to maybe future employers?	
	RP3	Very realistic. Maybe not future employers, I don't think they will be that individual about it. But I think, giving my data to other companies that want to use the data for other purposes of research or market research, I think that could be. I think, you just have to acknowledge that that is what is happening currently, like our data is being sold on without our knowledge, this is part of the information society.	SU
Q8.6	AO	Concerning the wearable, like a fitness tracker, would you be concerned that it is not secure? That somebody else might break into it and steal the data?	
	RP3	I'd assume it is safe enough, but it is because I don't know anything about technology. So, I just... ya sure.	SC
Q9	AO	So, we have been talking about all those risks. Could you also imagine something positive as an outcome of disclosing your information to the insurance company? Can you think of any benefits for you, personally?	
	RP3	I mean, if you are a somewhat healthy person, who like to do exercise, yes you could pay a bit less, but I think on an aggregate level what it would mean for society, I think everyone except for companies would disbenefit from it.	FB
Q9.2	AO	So it wouldn't be an incentive for you that you get the free device for example from the company?	
	RP3	If the only use of that free device is to record data that I do not want recorded, I see no personal use for it. No, I wouldn't care.	FT
Q9.3	AO	You already said that you wouldn't be too keen on having such a device, but could you think that it increases your motivation to do more sports activities, to become healthier?	
	RP3	I don't think it will increase my motivation to be healthier. It might increase my motivation to be healthier, because I want to get less money. But 'my' motivation to exercise will still be on the same level, I still wouldn't want to do more exercise. I wouldn't be healthy, because I want to be healthier. I would exercise, because I want a cheaper price. So it is like that. So I don't think you can say it increases incentive to be healthy. Maybe I'd be healthier to save money, but not because I think healthy is good.	HM/ FB

	AO	So that is not really a benefit for you then?	
	RP3	Well, it benefits you still if you become slightly healthier, but I also think you could imagine it being a stress factor. If you think about how much you beat yourself up, because you didn't go to the gym that day, because you weren't feeling well. And imagine you get sick for a long time, and you know you're going to get a higher bill for your insurance in the mail and that increases your stress level which is not healthy for you. So, I think this idea of being constantly surveilled and always knowing that whatever little action I don't take might become an economic problem for me in the future. I don't think that that would be healthy in the end. So yes, it could be beneficial, but just the mental state I would be in knowing that am always surveilled, I think that in the end would not be good at all.	HM  IP
Q9.4	AO	Again, if you compare yourself to others: Would you think that this new policies might increase the fairness among policyholders? Because someone who is intentionally not involved in healthy lifestyle choices should he pay more? So that is fair then or not?	
	RP3	Yes, I could probably say that fairness would increase. If you smoke for example, I personally believe that if you smoke maybe you should pay a bit more knowing that it's bad for your health. So yes, but then like I mentioned before we also know that there are other variables that effect your health. And there are variables that you can't affect yourself. So let's say you're a smoker, but you're a smoker because you grew up in a house where lots of people smoked, because you grew up in a neighbourhood where people smoked. And then you can't really pull that down to individual choice. So, it becomes a question whether or not you believe in free choice and that every individual ultimately responsible for their own actions. I don't think a 100% I am. So, it really depends on which perspective I view this from. But yes, pure and simple numbers: fair much fairer. When you add the complexity of life: it is not much fairer.	IF
Q9.5	AO	Do you think it would have an effect to buy such a policy and then receiving the wearable on your social image? Do you think you will earn approval from your friends, because they think that it's a cool thing or something?	
	RP3	In my group of friends: no. They would think I was a sell out. No, I think it depends on which groups of people you hang out with. There are people who then want the newest technology and who think that's cool. But as I already said: I am not that person, most of my friends aren't, so I actually don't think that it would give me any kind of social advantage.	SI
Q9.6	AO	Do you think the insurance company could offer you improved services based on this data?	
	RP3	No.	
Q10	AO	So okay, now we have discussed the risks and benefits you would expect from this. Considering all those aspects would you finally be willing to disclose your data to a health insurance company or would you not consider that at all?	
	RP3	Given the choice, given that my economy is quit poor at the moment, I would consider it, but I think ultimately I would say no.	
	AO	So the money is still a strong factor.	
	RP3	The money is a strong factor, and once again that's because I don't	FB

		earn a lot of money. So again I think it only benefits the rich people because they don't have to be concerned with it to the same extent that a person who doesn't have a lot of means would have to. So I'd probably just say no cause of principle reasons, that is like I am not going to play the insurance companies game.	DM
Q11	AO	Okay, how would you describe your health status right now?	
	RP3	Completely fine.	
Q12	AO	Do you think your opinion about this whole issue would change if your health status was different?	
	RP3	Mmmm no.	
	AO	Makes sense as you already said no.	
Q13	AO	Would you in generally say that you trust insurance companies? Are they trustworthy?	
	RP3	I mean it feels unfair to say this, because I only had to use an insurance company once and they were very nice and very kind, but I generally don't trust big business at all. I mean, I still use them, but trust... that I don't. I am always suspicious whenever I am in contact with a private company or big business. So, I suppose that has to apply to insurance companies.	
Q14	AO	Okay, is there anything you would like to add to this topic of fitness trackers in health and life insurance which we didn't cover and you feel is important and we missed out on?	
	RP3	No, no. I don't know enough about the subject. 'Capitalism' might be a word I should throw in there. Makes me sound like a super Marxist. I am not a super Marxist, but I am more of a liberalist and I believe freedom is important when it comes to those choices. But no, I don't know enough about insurance to add a question, I trust your expertise.	
	AO	Thank you for your participation and your time.	

**Transcription of Interview No. 4**

Date: 27.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP4  
 Interviewer: Ali Chehab  
 Interview format: Face-to-face interview  
 Interview duration: 21:49 min  
 Transcribed by: Ali Chehab  
 Transcription date: 28.04.16

Question	Speaking	Text	Code
Q1	AC	We are going to start the interview asking about some characteristics. If you don't mind us asking: how old are you?	
	RP4	23.	
Q2	AC	Where are you from? And where did you lived most of your life?	
	RP4	Sweden and just outside Lund.	
Q3	AC	Do you have any health or life insurance?	
	RP4	Yup.	
Q4	AC	Do you own any wearable device?	
	RP4	Yes. Two of them.	
	AC	Can you tell us more about those devices?	
	RP4	I have one just recording all the steps, a fitness tracker, a Fitbit, and then for my orienteering running I have one GPS clock that will track all the steps I am taking in the forest and afterwards I can look at my pulse, and see how fast I have ran, and exactly where I have been running so I can evaluate and be better.	
	AC	Do you wear it regularly or do you just wear it when you're running?	
	RP4	Only when I am running or when I am exercising.	
Q6	AC	Would you describe yourself as generally concerned about your privacy, do you worry a lot about it?	
	RP4	No, not that much. After returning, I will just sync it up to a webpage and I have an open profile so everyone can look at my training and exercising instead of just having a high profile as Instagram for example. So, I am not so concerned about my privacy. If people want to track me, they can track me easily.	
Q5	AC	Would you describe yourself as technology affine, like people who always buy the latest technology devices? Like latest wearable, latest phone?	
	RP4	I don't know actually. I have an iPhone of course, but I don't have the latest wearables, because I just have that one that fits my needs. The latest ones are more expensive and have more functionality. They can track bicycle and swimming, but I just need it for running. So, I am not up for the latest, I am just up for the stuff in it.	
	AC	So you care more about the specification and what it can do?	
	RP4	Yeah, exactly.	
Q7.1	AC	What is the first thing that comes to your mind when you here about the new concepts of insurance? Like having the integration of technology in the insurance industry to track your health, and accordingly provide you a premium based on how much you exercise.	
	RP4	I think, if this can help me to pay less I think it's good, but on the	FB

		other hand if I am not a fitness person, it will be maybe a disadvantage, because health insurance can see that I am not so active, and can have it more expensive. But if I am an active person, I think it will be easier, then I can pay less. If it will be based on my fitness.	DM
Q7.2	AC	Do you think it's a good idea to use the wearable device in the insurance industry?	
	RP4	Yes, I think it will be cool at least to try it. We will have to see if it works. But on the other hand, maybe I can have 4 watches on my hand and then I can track some other people's training instead, I don't know, if they will figure it out.	MP
Q8	AC	Can you think of any negative consequences resulting from providing your data to the insurance industry or the insurance company?	
	RP4	No, I don't think this will be a specific negative consequence. Maybe if they can see exactly where I am walking, tracking me since I have a GPS they can see exactly where I am going. Maybe some other people can break into the system and see where I am and get into my house when I am outside running.	IP SC
Q8.2	AC	Do you have any data accuracy concerns? Like wearable devices not collecting the right data, for example sometimes it might record extra steps or less steps than you actually do.	
	RP4	I know every watch has like a 10% difference, so at least I am aware about it. I think mine is a little bit wrong, too.	
	AO	Do you think that will have an influence in the insurance context, if it's not accurate?	
	RP4	Maybe not, because when I bought it said in the manual that it has 10% differences. So as long as I am aware of it, it will be ok. And they will probably be aware of it as well. I saw that the most expensive watches has still 10% differences, so I don't know. I don't think it will be a problem.	DA
Q8	AC	Do you think there are any risks affiliated to disclosing your information to insurance companies?	
	RP4	No.	
Q8.3 + Q8.4	AC	Not even data manipulation or giving out your data to another company for other purposes?	
	RP4	No.	
Q8.4	AC	Haven't you thought about the possibility that your data might be sold to other companies?	
	RP4	No why should I? As long as it hasn't happened yet, I don't think it's a problem. Maybe, I will trust the company, but I don't know it now. As long as they will not show me another side of it, I don't have any trust issue with them.	
Q8.5	AC	Do you think it leads to discrimination? Like if your healthy you are getting a better offer, whereas if you are sick or you have a chronic disease or cancer you might be subject to a higher insurance policy.	
	RP4	Yes, I think there will be some discrimination. Because if you have like cancer, you cannot exercise as much as when you don't have it, and they will automatically pay more, but on the other hand if they can collect data, and see that this person needs more training, maybe they can help the person instead like this person needs a personal trainer for example.	DM IS
Q9	AC	Okay, so we are going to move on to the perceived benefits. For what reasons would you disclose your information to insurance	

		companies? Do you think there are any benefits affiliated to disclosing your information to insurance companies?	
	RP4	Yes, it depends on the salary [premium] I am going to pay. If it is just a small difference, there might be no benefit of having like a wearable. It will be like good looking.	FB
Q9.2	AC	Is receiving a free wearable from the company a benefit?	
	RP4	Yes, then everyone will have the same.	FT
Q9.3	AC	Do you think it will impact your health motivation, if you have this wearable device?	
	RP4	I think, it will be motivating in the beginning and then, you have seen other companies that have step competitions in their jobs, so in the beginning people are walking every time, counting steps, and then one month later they will be tired out of it. I think it will be great in the beginning and then you need to work out to get a good business model that people will continue with it.	HM
Q9.4	AC	Regarding the fairness, do you think it's fair that people who exercise more get a lower price, and if you're not exercising you're getting a higher quotation? Do you consider it as fair or discrimination?	
	RP4	I think it is fair, because if I am more healthy, I will have like less visits to the hospitals and I will not be there as much as the non-healthy person, for example, and if they pay more, and they will use the hospital more, I think its fair.	IF
Q9.6	AC	Do you think that the insurance companies, through the data you provide, can improve services?	
	RP4	I don't know. Why should they?	
	AC	You never know, like providing it to the hospital, and if you go to the hospital, and they know that this person exercises so much so we can give him a specific medicine.	
	RP4	I think it's too far in the future, I haven't been thinking about it.	
Q9.5	AC	Do you think that there is a social image regarding the wearable device, like you go to your friends and show them that you have a Garmin watch, or a Fitbit?	
	RP4	Yes, I just chose mine because it is good looking and smaller than the other ones, but on the other hand if they are going to hand it out for free, everyone will have the same and the social image will be the same. It will not be about the price.	SI
	AO	So buying an insurance policy like that, would it also be like "Oh guys, I am having this new insurance policy which is connected to my fitness". Will that improve your social status among your friends or would you not care about that?	
	RP4	Personally I wouldn't care. But I don't think it will make so much difference between them. Most of them are just the same. They are collecting like GPS, pulse and steps.	SI
Q10	AC	Considering all the aspects that we discussed about the risks and benefits and weighing them both: Would you be willing to disclose your health information to the insurance company?	
	RP4	Yes, I will do it, I will try it. I like to try new things. At least as I am just wearing a wearable right now, I would definitely try and see if it will be a benefit, and then see if the risks are high, I don't know.	
	AC	Based on your training and exercise that you do, you will get a free premium.	

Q11	AC	How would you describe your health status?	
	RP4	I think it's quite good. I am training and am eating some sweets, I think it's great.	
Q12	AC	Do you think your opinion towards the issue of wearables in the insurance industry would change if you were in a different health condition or if you had a disease?	
	RP4	Yes, probably. I don't think I would be so much like: "yeah, let's try something new", I would probably more like "okay, probably I will have to pay more". If I am motivated to be more healthy, I would maybe chose it, but if I am just so comfortable in being in my couch and eating my ben and jerry's, maybe I wouldn't be so enthusiastic.	
Q13	AC	You already said before that you trust insurance companies. Can you elaborate in what sense do you trust those companies?	
	RP4	I think, I have too small knowledge to not trust them. Because I think they fix everything. I think it's like good to have insurance if anything will happen to me, they will just fix it, and I will not have any costs, but I have never used my insurance so I don't know actually what will happen.	
Q14	AC	Is there anything you would like to add that we didn't shed light on regarding the health insurance and wearable devices you would like to consider or talk about? Maybe we missed something.	
	RP4	It depends on what they are collecting, are they just going for the steps, or are the insurance going for...	
	AC	It can be steps, stress, heart rate, sleeping habits.	
	RP4	So basically they see everything am doing right?	
	AC	Probably and this will evolve with the devices.	
	RP4	What happens when my wearables need to be charged? Will it affect the life insurance? Because it takes 2 to 3 hours, and sometimes I charge it during the nights so they won't see my sleeping habits or my heart beats, maybe I will get a heart attack in the middle of the night and they will never know. Maybe.	
	AO	Fitness trackers don't have to be charged that often. Right?	
	RP4	Yes, once a week. It depends on how much you use it. If you just use it or you can answer text message, otherwise no	
	AC	Thank you for your time and your participation.	

**Transcription of Interview No. 5**

Date: 27.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP5  
 Interviewer: Annina Oelschläger  
 Interview format: Face-to-face interview  
 Interview duration: 23:17 min  
 Transcribed by: Ali Chehab  
 Transcription date: 28.04.16

Question	Speaking	Text	Code
Q1	AO	So we would like to start with some questions about the demographics, just to get to know you a bit better. How old are you?	
	RP5	33.	
Q2	AO	Where are you from, or where have you lived most of your life?	
	RP5	I am from Lund and also from a small town in the middle of this region called Hörby, but I am born in Malmö. Basically, I have lived here in this region my whole life.	
Q3	AO	Do you have a health or life insurance?	
	RP5	I have a life insurance, yes.	
Q4	AO	Do you own a wearable device like for example a fitness tracker?	
	RP5	No, I don't.	
Q4.1	AO	Would you generally be willing to wear one or have you ever thought about buying one?	
	RP5	I thought about buying it for exercising purposes like a running watch which can gather GPS locations and measure my pulse and something like that	
Q6	AO	So in general you are open towards that. Would you generally describe yourself as concerned about your privacy in all context not only with insurance companies?	
	RP5	Depends from an ideological perspective: yes. But when it comes to using services I like, I tend to not, you know I tend to actually disregard some of my believes, about the importance of privacy, because I see a value in using some services like I have a google phone and I use facebook and stuff like that. I have some kind of concerns, but if the use of the service is more important, then my ideological believes I would disregard the privacy aspect.	
Q5	AO	So you actually behave different from your believes then. Okay. Would you describe yourself as a technology affine? So do you have a lot of gadgets and stuff like that?	
	RP5	Yes, I would say so.	
Q7.1	AO	So you're interested in always the newest stuff. In the introduction, I told you about the new insurance policies with the wearable. What is the first thing that comes to your mind when you hear of that?	
	RP5	It's the ideological concerns that a private company would use the information about me in a way that could be of importance to me, because I get lower fees or lower costs, but it could also hit back quite hard in another situation which is unexpected when I signed the contract. Cause then they have a lot of information about me, but I don't know how they will use it. If I later on become sick or if	SU/ IP

		they can use the information to see that or conclude that before you signed this contract you actually broke some clause in the agreement which makes you non illegible to use the insurance.	
Q7.2	AO	So in general do you think it's a good idea to introduce the fitness trackers in the context of the insurance?	
	RP5	No, I would say I am a little bit reluctant. I think I can see the benefit from the public perspective. I mean the public services in Sweden could use this as a good way to motivate people to improve their health. But I am a little bit reluctant to impose a private company with that.	HM
Q8	AO	If we dig a bit deeper in that topic: what do you think or what are your fears or the negative consequences of disclosing your data to an insurance company? What do you think of the risks?	
	RP5	I think the risks in general to turn the insurance business into a data driven business, is that you would enhance the problems with some individuals falling outside the insurance system, because it's like some children that are born with disabilities, and people who have well documented kind of diseases, they can't sign any insurance because they are regarded as higher risk. So, I think making insurance business more data driven is dangerous because at the end of the day it would only benefit the insurance company not the individual.	DM
Q8.5 + Q8	AO	So this is kind of referring to discrimination with you saying that. Okay, and additionally for you personally, do you think there could be some specific risks? Do you have another idea what could happen?	
	RP5	I mean it is a little bit like what I said before that, I don't know how they aggregate data, it could reveal, I mean if I use a fitness tracker or something, I give them a lot of data, and I don't know how is that aggregated in relation to other data the insurance company have which could reveal new patterns that might not be very beneficial for me. So I am a bit hesitant.	SU
Q8.1	AO	Does that also include general privacy concerns, or that you feel like the company is surveilling you?	
	RP5	Both yes and no. I actually don't have any problems with giving away my data, but it depends on the context. I would say that I have more concerns giving it away to insurance companies than to Google, because I think that the agenda is more clear from the insurance perspective that it will be used to improve their risk analysis, and that is something that might not be beneficial for me at the end of the day.	
Q8.3	AO	So do you think there is room for manipulation? I mean basically it is very fact based, because you are collecting your data and sending it to the insurance company, but then you don't really know how they treat your data and what they take from this data. So, do you think there might be a problem?	
	RP5	Yes, it might. I mean I don't know if they use my data, and that might affect my daughter's option to get an insurance, because they might say you have a certain lifestyle and her health issues is directly related to how you live, so and maybe something with that will affect her in the future.	SU
Q8.4	AO	Do you think there is also a risk that the insurance company gives away your data to third parties?	

	RP5	It depends, I mean you obviously have to read the terms and conditions quite clearly and if I sign a contract that says that they won't do it, maybe or obviously I have to trust that, but you never know, of course. Because it is somehow you sell your information, and then it's not yours anymore, so there is always a room for that.	SU
Q13	AO	You just mentioned trust. Do you trust insurance companies?	
	RP5	No.	
	AO	Would you elaborate on that?	
	RP5	I mean they capitalize on the risks of injuries, so it's somehow it's a business, and the business end goal is to earn money. And they earn money based on people's fear of getting an injury. So, I think their business model is a little bit... I think if you could organize the society in another way, maybe you wouldn't need the insurance companies. So I think their agenda from an ideological perspective it is a little bit difficult. I don't know, but questionable, so I have little trust.	
Q8.6	AO	About the wearable, do you think there are security concerns about that? Would you be afraid if someone breaks into your device and steals the data?	
	RP5	The thing is that I know that there are a lot of security issues, but I think since am a gadget freak I would probably disregard it, because I would like to use it.	SC
Q9	AO	We are switching the sides and thinking about the benefits. You said already that of course it might be cheaper for you, could you think of any other benefits for you personally, if you would buy such an insurance policy or could you elaborate on how this would benefit you?	
	RP5	I like the concept of encouraging people to track their health, because you know if you get a lot of people to do it, it could be something that really improves the general health of the population, and that is an obvious benefit. So from that perspective, I like it.	HM
Q9.3	AO	Do you also think it would motivate yourself to be healthier?	
	RP5	Yes, probably. I mean as now I don't do that much exercise, but I always have it in the back of my head that I should. So, if I would wear a gadget and I would be engaged in some kind of program and I have a target and then track my activity and stuff like that in real time, yes I think it would be beneficial for my health actually, so yes.	HM
Q9.2	AO	You will also receive a fitness tracker from the insurance company. Would that make you happy? And make you actually decide in a positive way for this policy?	
	RP5	I don't know, I mean of course it's always like that, it's the same case as with Google, you have to make some sort of cost-benefit analysis. What is the benefit and what is the drawbacks? So, maybe that could be a case, where I would regard the benefits as higher than the concerns, but probably not in the insurance context. Because I have such a strong reluctance against the insurance companies so probably even if they would offer me very low premiums and also to get it, I would probably not go for it, maybe it depends, I think it will depend on your economic situation.	
Q9.4	AO	Do you think it would increase fairness amongst all the policy holders?	
	RP5	No, I don't think so, because I think that people with less money	DM

		would be more forced to do it, if low premiums is what comes with the package. So those economical aspects will force some layers in the society to go for this and actually go against their believes in privacy. So, I think that could be certain dangers in it.	
Q9.5	AO	Thinking about receiving the fitness tracker and wearing it then, and having a very innovative service here: do you think the opinion of your friends and peers would maybe influence your decisions, saying that you are feel innovative or like an early adopter, because you're buying such an insurance policy connected to your device?	
	RP5	That is always the case of peer pressure, I think. So I mean, if suddenly all my friends might go for it, if they see there is no drawbacks, maybe after a while I start to question my believes. It is natural, I think.	
	AO	But you won't be the one who gets it first?	
	RP5	I would not be the first mover in this case.	SI
Q9.6	AO	Do you think the insurance company could provide you with improved and tailored services based on this data?	
	RP5	Yes, probably. Because they would know exactly the status of my health and then of how I lived my life. But I think, it also comes with lots of dangers, but I think, yes, from the insurance perspective it would be useful, because they could actually tailor your insurance and probably enhance your life with this insurance.	IS
Q10 + Q11	AO	So you already said you will, right now, not be willing to disclose your health information to the insurance company, right. If you don't mind could you say how would you rate your health status right now?	
	RP5	Using a scale from one to five?	
	AO	Just if you think it's good or bad.	
	RP5	I mean it is regarding my age, I think, it is okay. There is room for improvement, but I think there are worse cases.	
	AO	You don't have any major illness or something?	
	RP5	No, I am in a good health actually.	
Q12	AO	Do you think your opinion towards the whole issue of the insurance companies using those data would change if you were in another state of health?	
	RP5	Maybe, I would. Maybe I could see the benefits of it more, if I were in a bad shape.	
	AO	If you were in a bad shape you would see the benefits more?	
	RP5	Maybe, I don't know, it's hard to say.	
	AO	But it might change the perception?	
	RP5	Yes, it's hard to say.	
Q14	AO	Lastly, do you have something that you think we should consider in that context and we haven't covered?	
	RP5	I think it was good questions, I don't know, I don't think I have anything to add.	
	AO	Thank you very much for your participation.	

**Transcription of Interview No. 6**

Date: 27.04.16  
 Present Persons: Ali Chehab (AC), Annina Oelschläger (AO), RP6  
 Interviewer: Annina Oelschläger  
 Interview format: Face-to-face interview  
 Interview duration: 22:00 min  
 Transcribed by: Ali Chehab  
 Transcription date: 29.04.16

Question	Speaking	Text	Code
Q1	AO	Okay, to begin with we would like to ask you a bit about the demographics. So if you don't mind us asking: How old are you?	
	RP6	23.	
Q2	AO	And where are you from, or where have you lived most of your life?	
	RP6	In Albania, capital Tirana.	
Q3	AO	Do you have a health or life insurance?	
	RP6	No. Sorry, but it's also the part that I am insured by the university. Does it count?	
Q4	AO	Yes, then your covered. That's fine. Do you own a wearable device like a fitness tracker?	
	RP6	No.	
Q4.1	AO	Have you ever thought about buying one, or would you be willing to wear one?	
	RP6	Yes, I thought about buying one, in order to keep track of my physical activity, since I'd like to be healthier, in a better shape.	
Q6	AO	So, you would generally be open to that. Great. In general, would you describe yourself as concerned about your privacy? Not only in an insurance context, but overall.	
	RP6	Yes, usually I am very concerned about my information. I don't give away my information easily.	
Q5	AO	And would you describe yourself as technology affine, meaning that you are always buying the newest devices and you're very interested in those things?	
	RP6	No, usually I buy things that I find that I need or I find reasonable to have. It is not because something new is coming that I am willing to buy it directly.	
Q7.1	AO	Now we are going to the main part. In the introduction I told you about the new approach of insurance companies. What is the first thing that comes to your mind when you hear of this new policies offered by insurance companies?	
	RP6	Well, from a business perspective, it is that they want to make profit out of it, and I feel like "Mh I am going to release a lot of information". It is about releasing information, and your information being used, in the first idea, it is beneficial to you, but I am concerned that it is more than that.	
Q7.2	AO	So you think it's not a good idea, to use wearables in the context of health and life insurance?	
	RP6	Mmm... It is a good idea in case of health problems, or administered by people who work in health care systems, but in the insur-	

		ance I would be more keen on disclosing less information than is usually required, because they usually track a lot of activities.	
Q8	AO	So if we are digging a bit deeper there: Can you imagine some negative consequences or risks coming with the disclosure of your information in that context?	
	RP6	Well, the first thing that comes to your mind in this case is that the company would probably be... there would be a cyber-attack, but probably the company sets the right security infrastructure that probably will assure you. But however not knowing what the big data is going to bring to people, I would see that it is something unknown and probably, it might have a power that we don't know yet.	SC
	AO	So the first thing you mentioned was the cyber-threat. So that means like someone from outside the insurance company is attacking their database and stealing the data?	
	RP6	Exactly. Or, it can be also the part that the insurance companies might sell the data to other parties, sell or I don't know, kind find a forum to make the data useable for other purposes.	SU
Q8.1	AO	Would you generally feel like it is an invasion of your privacy?	
	RP6	Maybe this is only my personal concern and I am more concerned than I should, but yes.	
	AO	Okay, will that mean that you feel surveilled, like they are watching you all the time?	
	RP6	Well this is contradicted, because on one hand you decided to buy the wearable on your own. You know that your data is going to be collected, but on the other hand, you don't like the fact that you are somehow being tracked, and yes you have the feeling that you are surveilled, because someone else has your data, and based on that data they take decisions, of course they need data in order for the business to go on, but still yes	IP
Q8.3	AO	Do you think there is room for manipulation on the side of the insurance company? So, you send you data there, and then they can do whatever they want with that data. Right?	
	RP6	Yes I have this concern, that probably if they are measuring my..., or they have a track of my activity or at least my data, they might have let's say another connections with a company with pharmaceuticals, and another stuff and probably get advertisement on that or in another form, and that would be something that I wouldn't like.	SU
Q8.5	AO	Do you think there could also be room for discrimination, meaning that some people are treated different than other?	
	RP6	Yes, this is also because, okay it's the part that when someone is really healthy, they will have to pay less and the other ones will have to pay more, but this goes in line with the mission of the company, because if your healthy, you're not supposed to pay, so I am not sure about that.	DM
Q9	AO	And then on the other side, do you think there are any benefits for you personally included, if you give away your data? What are you expecting to get back as a positive benefit?	
	RP6	As a positive benefit from the insurance company... Well, assuming that I will be healthy, it is a good thing that I will have to pay less. This is probably one of the benefits.	FB
	AO	And you don't see any other benefits?	
	RP6	Any other benefits? Mh, for the moment no. I don't recall any.	

Q9.2	AO	So would you say that the fact that the company is giving you the fitness tracker for free, is that an incentive for you to disclose your information, and buy that policy?	
	RP6	I didn't get this part.	
	AO	If they give you the wearable for free, right? Is that an incentive to buy that policy or is it not relevant for you?	
	RP6	No, it wouldn't make any difference.	FT
Q9.3	AO	Would it motivate you to do more fitness exercises and to get healthier?	
	RP6	Well, from a personal experience, keeping track of my activities helps me to get better in some stuff. So it also motivates me to achieve my goal.	HM
	AO	And would you want to be motivated? So is that a benefit coming with that whole package?	
	RP6	No, I find motivation in other parts. It would be just like a good way to keep track and also the part of economical benefits where you have to pay less, cause in some places you need to have health insurance and if you are going to purchase that as an individual, not having to do with the employee or the state, then you have to take into consideration those things.	HM
Q9.4	AO	And considering all the different policyholders from one insurance company: do you think procedures like this would increase fairness? Like because someone who is not doing any fitness exercises has to pay more than someone who's doing a lot. Do you think that is fair?	
	RP6	Well, I guess that the ones that are buying the fitness related policy are interested somehow, and there are not just buying the policy, okay yes your right because it's an insurance... Well, from the company perspective, I think it's there.	
	AO	And from your personal perspective?	
	RP6	I am not sure about that.	
Q9.5	AO	Okay, that's fine. Do you think this whole thing will have an effect on your social image, meaning that your friends or your peers will give you approval or would be jealous that you have a fitness tracker or you have this innovative insurance policy?	
	RP6	Probably, this would lead to discussions of advantages and disadvantages of these kinds of trends. And probably, they might be willing to have this in the insurance company, sorry this insurance policies, or they might choose to not, but it would be more marketing if they see the wearable, like brand. Which I think is a smart thing from the insurance companies giving the wearables.	SI
Q9.6	AO	And do you think that with this data the insurance companies can improve their services for you like having specific tailored offers for you?	
	RP6	Can you repeat the question? I wasn't paying attention.	
	AO	If you think that the insurance company based on those collected data, are able to improve their services for you. So, they can tailor their offers and basically be better in what they are doing?	
	RP6	Yes, I think yes. It would be helpful, because when you have the human contact or you discuss your concerns probably in person, it would be better. Better than just purchasing a single policy, because it is needed, and maybe we can discuss more if we have any concern or about some parts of the policies, you can discuss that.	

Q10	AO	So now we've talked about the risks and benefits for you personally. If you take into account all of this different things, would you finally be willing to buy such an insurance policy and ultimately give away your personal data to the insurance company?	
	RP6	In the phase that I am in, I am not going to do that now. Later on maybe when I will need to have an insurance on my own, I will consider doing that.	
	AO	Mainly for what reason? Is it because it's cheaper? Or you have other things?	
	RP6	Well, you mean if I am going to consider later or why I don't need it now?	
	AO	Why you're considering it for later.	
	RP6	Yes, because, well it's a part of when you get older probably you might start having health issues, so we need like an insurance.	
Q11	AO	So if you don't mind would you tell us about your health status? How would you describe your health status right now?	
	RP6	My health is stable, I don't have any issues.	
Q12	AO	Do you think your opinion toward the issue of wearables in the insurance context would change if you were in a different state of health? So if you were sick, for example.	
	RP6	Yes probably, probably.	
Q13	AO	Then we come to the last question which is: would you generally say that you trust insurance companies, or your insurance company?	
	RP6	If I would be between strongly agree and disagree, I would be not sure.	
	AO	Okay, in the middle. So you don't really have an opinion about that?	
	RP6	Yes.	
Q14	AO	I think we have covered all our questions. Now we would like to ask you if you have anything to add to this, anything you think we should have covered in the context of fitness trackers and insurance companies?	
	RP6	Ah, any comments... Do you have like example if this kind of technology is applied by insurance companies?	
	AO	This is already happening in the US and in the UK. It is more often adopted in life insurance companies. So, they are actually giving away the wearables, and you are measuring your steps, and sending it to the company, and then they lower you premium for that.	
	RP6	I would comment that, from my personal perspective, I say that this is the trend, one of the trends of IoT. Because there is the opportunity to measure and to track, then let's find a way to make profit out of it. And the insurances were smart and probably they will continue and in Europe it will also evolve.	
	AO	Thank you very much for your time and participation.	

**Transcription of Interview No. 7**

Date: 28.04.16  
 Present Persons: Ali Chehab (AC), RP7  
 Interviewer: Ali Chehab  
 Interview format: Face-to-face interview  
 Interview duration: 27:48 min  
 Transcribed by: Ali Chehab  
 Transcription date: 29.04.16

Question	Speaking	Text	Code
Q1	AC	I am going to start the interview by asking you some questions about your characteristics, if you don't mind answering them. How old are you?	
	RP7	I am 35 years old.	
Q2	AC	Where do you come from? Where have you lived most of your life?	
	RP7	I come from India and I lived most of my life in India.	
Q3	AC	Do you have a health or life insurance?	
	RP7	I do have health and I do have life insurance.	
Q4	AC	Do you own any wearable device such as Fitbit or an Apple watch?	
	RP7	Unfortunately till now, I do not own a wearable.	
Q4.1	AC	Would you generally wear a health tracking device, if you were given one for free?	
	RP7	I would definitely.	
Q6	AC	Would you describe yourself as generally concerned about your privacy? Do you worry a lot about your privacy?	
	RP7	I worry a little bit about my privacy, especially when it is not too probing. But if it is for general health care and it will do good to people then a little bit of questioning will not matter.	
Q5	AC	Would you describe yourself as technology affine? Do you always have the newest devices in technology? You have the latest iPhone as I can see.	
	RP7	Well, you have actually caught me. I do have the latest iPhone, I do have the iPad and if I have the... I mean if the device is within reach and it is not too freakily expensive, I will possibly try and have it.	
Q7.1	AC	What is the first thing that comes to your mind when you hear of this new concept of insurance and wearable devices in the insurance industry?	
	RP7	I'll be very honest in the first go insurance and wearable devices were 2 separate entities in my mind, but recently with fit bits and these devices, I think that we should pay more attention to our health and in return, we might get some benefits. So my outlook is: why not, why not get some benefits.	
Q7.2	AC	Do you think it is a good idea to use wearable devices in this context?	
	RP7	I do think it is good.	
Q8	AC	I am going to move on to the part of perceived risks. Can you think of any negative consequences resulting from disclosing your health information to insurance companies?	
	RP7	Yes, of course. It is like if I have got some kind of disease which	DM

		can be later on creating issues, and these can be taken into consideration by the corporate world, corporate organizations, and they might use this disease, and might ask me for more medicines and the insurances... If they would try to push me towards it, then I would not be very happy. I would not be very happy, if I am pushed towards it beyond my will or my wish. To a certain extent it is ok, it's part of the game, but not beyond the limit.	
Q8.4 + Q8	AC	You just mentioned one of the risks which is secondary use of data or handing the data to a third party. Do you think there are risks of disclosing your data?	
	RP7	Okay I'll give you a small example. I have got glasses, at distant vision, I have issues with distant visions. I do like wearing fancy lenses, and fancy eyeglasses and sunglasses, but I would not want the insurance company to promote all the time every new kind of contact lenses that are coming to the market and every new kind of sunglasses that are coming to the market. Once or twice it's acceptable, but I wouldn't want that to run after my life. No.	SU
Q8.1	AC	Do you think it is a type of invasion of privacy by giving your data to the insurance company?	
	RP7	It is after a certain point of time, it is an invasion of data.	IP
	AC	Can you please elaborate more about it?	
	RP7	Just as I said, suppose I have caught my ?? and there is a track record of getting new sunglasses every time. So, when I go to these synoptic or these glasses shop and the moment they see my record, they start along with treating me, they start going for sales, and they start of saying "Madam, would you be interested in this, and the other product?", I mean the approach should not be like this, it should be like, you should let the patient in this case start of on his own and if he is not willing at the first go, we should not even start off with the questions, with the private data the company already has. It should be the initiative of the person and it should be the initiative of the patient and it should be respected, I think.	
Q8.2	AC	Regarding data accuracy. Do you trust that those wearables are accurate to collect precise steps, or the exact heart rate, and do you trust that those data will reach exactly to the insurance company?	
	RP7	I think a lot of things depend on the state of the wearable is in. Because the wearable is also battery driven and there is the status, I mean the state if it's being well maintained by the person, whether it is being kept properly and they are not tampered by children and you drink a glass of water and suddenly somebody pushes you and water splashes on the wearable. If this is how the wearable is being maintained, I think there might not be as much accuracy and the data, the wearable might be tampered, and with regards to the data going to the right insurance company, well I have got doubts about that. I have got at least 2% doubts about that.	
Q8.5	AC	Do you think there is a sort of discrimination when the insurance company offers someone who is sick a higher insurance premium compared to someone who is well fit and in a good health status who receives a lower price. Do you think this is discrimination?	
	RP7	Of course it is a discrimination, of course.	DM
Q8.6	AC	Do you have any security concerns? In terms of wearable devices that your data is secured and like nobody would steal you data.	
	RP7	No. Especially after starting to know that the big data and the data	

		is being utilized in the E-commerce and there is a possibility of this data being used elsewhere, I am not 100% sure that my data is secured with my insurance company. No.	SC
Q9	AC	Then moving on to the other part: we are going to talk about perceived benefits. For what reasons would you be willing to disclose your health data to insurance companies? Do you think there are any benefits affiliated to disclosing your health information to insurance companies?	
	RP7	Look this world is very uncertain and we are being brought up in this way that everybody must have health insurance. Now the only way to get health insurance is disclosing some kind of data even if it is little bit, even if we do not want the data to be disclosed, it will be. And even if we find that it is being used elsewhere for whatever reason, or whatever purpose, if it is business or something else, we do not have any reason, we do not have any choice, we have to get health insurance to insure the safety of our future, and the security has to be compromised at a certain point.	SU
Q9.1	AC	Do you think that the financial benefits could positively influence your willingness to disclose your information? If you get like a 5% discounts on the premium?	
	RP7	Well, if I see that what I am being promised, I am getting, then I will be ready to disclose. And I will be ready to tradeoff something in return. But I must get what I am being promised.	
Q9.2 + Q9.3	AC	Receiving a free fitness tracker using it as a health motivator, as having the bracelet and the target of 10000 steps for example per day... Do you think it will motivate you to exercise and get in a better shape?	
	RP7	It's not only as small and as simple as that. I mean motivation is good in a way, yes definitely, but when I am in crisis, if my health insurance company is there beside me, helping me and giving me all the benefits at the time of crisis, if that is being taking care of, then I think it is going to drive me more towards disclosing my data. I am ready to disclose my data, to a certain extent of course, when I see that my insurance company is there supporting me during the time of crisis.	HM
Q9.5	AC	One more thing that I would like to know: Do you think it affects your social image, if you get a free wearable device showing it to your friends like "look what I have got from my insurance company", would it give you a social image?	
	RP7	It all depends on you and how you portray yourself and what motivates you and what is your driving factor and what is important to you. So, if your health and staying well is important, then I am pretty sure that you will be very proud of your Fitbit, of your wearable, and definitely if you are proud of something, you will talk about it and try to motivate your beloved ones. So, in a way it is positive, in a way, it is going to influence the people around you, and it all depends on the people around you, how they are going to take it, if they are going to take it as bragging it might be so, if they are going to take it as something they want to take up and start on their own life, it will do them good, so I think it all depends on the person.	SI
Q11	AC	If you don't mind answering that question: how would you describe your health status?	
	RP7	Well, when I was... it was around 6-7 years ago... when I was not	

		so much busy with my work and studies and everything else, I used to spend at least 2 hours in the gym doing physical exercises every day. You don't have to call me fitness freak, but yes, I was...	
	AC	Just to align it with my question, do you have any illness? You don't have to talk about it.	
	RP7	I do have an illness, but I do not want to talk about it.	
Q12	AC	Do you think your opinion towards the wearable devices in the insurance context would change, if you were in a different health state?	
	RP7	I don't understand this question. Can you please repeat it?	
	AC	Do you think your opinion towards the wearable devices in the insurance industry would change, if you were in a different health state?	
	RP7	Okay, you mean that if I am unwell, and still wearing the Fitbit, is that what you mean?	
	AC	Exactly, would it change your perspective?	
	RP7	It is like what purpose will it serve to me if I am wearing it and I am not fit enough? If you could explain that..	
	AC	Let's say you have a disease and at that time you don't want the company to know, because you have a disease. You don't want to let the company take your data, but let's say that you are in a good health state, you could think that it is safer to give the data, because you are in a good health shape. So, do you think your opinion towards the wearable devices in the insurance industry would change, if you were in a different health state?	
	RP7	If my health state, I mean if my illness is for a shorter period of time, I would rather not let the insurance company know about it. I know this is not right, but at this moment I think this is right. So, yes I think so. The opinion of the customer might change depending on the health state.	
Q13	AC	Would you say you trust your insurance company?	
	RP7	Not 100% but 98% maybe.	
Q14	AC	If there is anything you'd like to add in terms of wearable adoption and life insurance that I haven't shed the light on and you feel you want to consider: Can you please tell me about it?	
	RP7	Well, it is like whatever be it what I feel is the insurance company should be giving benefits to the customers. That's okay, but they should also do some really beneficial things for their customers. I mean, they should really think about their customers, everything should not be business oriented.	
	AC	Unfortunately, everything in this world is money, and profit oriented.	
	RP7	Yes, unfortunately. But, this is what I really think.	
	AC	I would like to thank you for your time.	

**Transcription of Interview No. 8**

Date: 28.04.16  
 Present Persons: Annina Oelschläger (AO), RP8  
 Interviewer: Annina Oelschläger  
 Interview format: Face-to-face interview  
 Interview duration: 18:40 min  
 Transcribed by: Ali Chehab  
 Transcription date: 29.04.16

Question	Speaking	Text	Code
Q1	AO	So to get started, I would like to gather some information about the demographics: how old are you?	
	RP8	27.	
Q2	AO	And where are you from or where have you lived most of your life?	
	RP8	South Africa.	
Q3	AO	Do you have a health or life insurance?	
	RP8	Yes.	
Q4	AO	Do you own a wearable device?	
	RP8	No.	
Q4.1	AO	Have you ever thought about buying one or would you be willing to wear one?	
	RP8	Define wearable device.	
	AO	For example a fitness tracker or bracelet.	
	RP8	No.	
Q6	AO	Would you describe yourself as generally concerned about your privacy, also in different context like in the Internet?	
	RP8	Yes, moderately.	
Q5	AO	And would you describe yourself as a technology affine, so your always having the newest gadgets and stuff?	
	RP8	Iphone6, yes sort of.	
Q7.1	AO	So, in the beginning I introduced you to the new concept of health and life insurance companies. What is the first thing that comes to you mind when you hear about this new concept of insurance?	
	RP8	Using wearables? That they sell it to me... the other wearables.	
	AO	The insurance companies are trying to sell more policies by giving you the wearable or?	
	RP8	Might be, this is such a tricky question.	
Q7.2	AO	So, okay I will rephrase it: Do you think it is a good idea to use wearables in the context of health and life insurance?	
	RP8	Yes, I think it is a good idea.	
	AO	Can you elaborate on that?	
	RP8	Yes, because you can use a wearable to track your insurance stuff and all your health data is on the wearable, and then I can use it or the health insurance companies can access it. It will make access easier.	IS
Q8	AO	Can you think of any negative consequences resulting from disclosing your collected data by the wearable to your insurance company?	
	RP8	Yes, because than they know about all your health problems. So maybe that is not good, because then they can see something and	DM

		then they push up your premiums.	
	AO	So this is a risk of disclosing your information, right?	
	RP8	Yes, they can use it against you.	
Q8	AO	Okay, are there any other risks you can think of besides that they use the information against you?	
	RP8	Right now I can't think of another risk. Just that they can use the information against you.	DM
Q8.1	AO	Okay, would you feel that your privacy is invaded by this approach of the insurance?	
	RP8	Yes.	
	AO	In what sense?	
	RP8	Because they have access to all your health data and you don't know how they are going to share it and with who.	SU
Q8.4	AO	So, do you think there is the possibility that they might share it with third parties like other companies?	
	RP8	Yes, they always sell your information to make more money.	SU
Q8.3	AO	Would you also say that there is a risk that the insurance company could manipulate your data?	
	RP8	Yes, because they have access and they put stuff in data that you might have not done. So, it is a big security risk.	MP
Q9	AO	So apart from these risks which we have just talked about. For you personally, do you think there are any benefits involved with you disclosing your information to insurance company?	
	RP8	I think the benefits are, if you are a very healthy individual and you are already healthy and then you disclose all the information, then it can be beneficial, because then it can lower your premiums for the month. But, I think if you are not that healthy, then I don't know why you would go for it. If you are like an active person, then it is beneficial.	FB
Q9.1	AO	So you say only the financial benefit is an incentive for you?	
	RP8	Yes.	
Q9.2	AO	Okay, so the fact that they are giving you the fitness tracker, the wearable, for free wouldn't be an incentive for you to buy such a policy?	
	RP8	For me personally, no. For healthy people, probably yes.	FT
Q9.3	AO	Do you think that it might motivate you to be healthier?	
	RP8	Yes, I think if they sort of force you to get it, and you are being tracked like you don't have a choice, then you will start like see how many steps did I take today and then you will probably be more active. And you will do the things they want you to do.	HM
	AO	Would you appreciate that? Would you like to be more active?	
	RP8	No, not me personally.	HM
Q9.4	AO	Do you think this approach would increase the fairness amongst all the policyholders, because for example some people do not engage in any activities, and conscious fitness lifestyle choices, while others put a lot of effort in?	
	RP8	It will improve it for everyone. I guess it will be fairer, yes. Because then everyone has to do something to improve their health, so that the premium stays low. But if there is a high risk group that is not doing any exercise, then the healthy people pay for them. But if everyone gets tracked and you pay according to your health, then it is fairer, yes. It will be a benefit of fairness.	IF

Q9.5	AO	Do you think if you buy such a policy and then you receive the wearable, that will give you approval from your group of friends or peers? You said that you are normally always having the newest gadgets, would that have an influence on your decision?	
	RP8	Yes, because they do look cooler than you are. So, they would think that you are really tech savvy, always using the newest technology.	SI
Q9.6	AO	Okay, do you think that the insurance company could improve their services and their offering by collecting this data?	
	RP8	I think so, because then they can customize what they sell you. So, it will improve customization. So they see that you are doing a lot of, I don't know... running marathons, then they can send you specials for marathons. Maybe, I don't know.	IS
Q10	AO	Considering all of these risks and benefits we just talked about: in the end, would you be willing to buy such an insurance policy and disclose your health information to the company?	
	RP8	No.	
	AO	So, the risks outweigh the benefits here, you think?	
	RP8	Yes, because I am not a healthy person, so it won't be beneficial for me.	
Q11	AO	So this is actually the next question: how would you describe your health status?	
	RP8	I am not that active, so I don't think that such a device would be efficient, and they track my health and charge me a really high premium.	
Q12	AO	And if you were in a different state of health you think your opinion would change?	
	RP8	Yes, if I was healthy and active, and going to the gym, then I would definitely gotten one.	
Q13	AO	Okay, would you say in general that you trust insurance companies?	
	RP8	Yes, in general yes.	
	AO	So you never had any bad experience?	
	RP8	No, no bad experiences.	
Q14	AO	So we already covered all the questions. Is there anything you would like to add, or do you think we missed something in this area of investigations about wearables in health and life insurance?	
	RP8	No.	
	AO	Okay, thank you for your time and participating.	

**Transcription of Interview No. 9**

Date: 29.04.16  
 Present Persons: Ali Chehab (AC), RP9  
 Interviewer: Ali Chehab  
 Interview format: Face-to-face interview  
 Interview duration: 21:55 min  
 Transcribed by: Ali Chehab  
 Transcription date: 26.04.16

Question	Speaking	Text	Code
Q1	AC	Starting the interview, I am going to start to ask you some personal questions, if you don't mind answering them: How old are you?	
	RP9	32.	
Q2	AC	Where are you from and where have you lived most of your life?	
	RP9	I am from Lebanon and I have lived most of my life in Lebanon.	
Q3	AC	Do you have a health or life insurance?	
	RP9	Yes, I do.	
Q4	AC	Do you own any wearable device?	
	RP9	No, I don't.	
Q4.1	AC	Would you be willing in general to wear a health tracking device, if you were given one for free?	
	RP9	Yes.	
Q6	AC	Would you describe yourself as generally concerned about your privacy? Do you worry a lot about your privacy?	
	RP9	Yes, in general: information to be shared with public, I don't encourage that on Facebook, Twitter. I use Twitter and Facebook just for fun. On the other side, if my information is being not in public... like I mean, let's say a company needs to use some data just to study some trend or patter, I don't mind.	
Q5	AC	Would you describe yourself as technology affine? Do you always have the latest devices or gadgets?	
	RP9	I do, but depending on my budget. But I do, yes.	
Q7.1	AC	As discussed before: What is the first thing that comes to your mind when you hear about the new concept of insurance?	
	RP9	Well, better health plans.	IS
Q7.2	AC	So you think it's a good idea to have the wearable device in the insurance industry?	
	RP9	I think, it would help, yes. Especially, that we cannot run away from the fact that the insurance and the health care is being totally privatized, and its more convenient, for people to watch out for their health, knowing that they will pay a lot of money to insure. So, it is like forcing people to be healthy by doing that. Sometimes, it feels not democratic, but this is a very useful way to push people to be healthy. Especially when they know that they will pay a lot of money, people usually when they pay a lot of money, they will tend to do something about it.	HM
Q8	AC	Moving on to the perceived risks. Can you think of any negative consequences resulting from disclosing your information to the insurance company?	
	RP9	Well, this would be a little bit tricky: if you're talking to a person	

		who is 12 years old, probably to his parents, so he will tell you no, because he still have the time I mean to benefit from such a system, but if you're talking to people like me 32 years old, I have a lot of health issues right now, so such a thing will kill my opportunity to get a fair health care during my elderly or at least right now, I will have to pay double the amount of a healthy person in my age or even more.	DM
Q8.1 + Q8.2	AC	Do you think there is any invasion of privacy that could be a concern, or data accuracy in the device itself, for example it might count extra steps or less steps that you actually do?	
	RP9	No, I don't think when you install such a system it's really hard for tech geeks to really know that the gadget you are wearing is not reliable or its lying. I mean you have seen Uber before, they created the bot system for their location services for the taxis, and it was totally based on nothing. It was not real and people knew, I mean tech geeks knew about it. So they just hacked the app and they knew that there is a bot that is randomly locating cars around you. However there is no cars around you. There might be 2 cars away 20Km, but on the map you see "oh there is a car in central Lund", and there is actually nothing there, but they were exposed immediately.	MP
Q8.3	AC	So this is sort of data manipulation?	
	RP9	Yes, this is data manipulation, but it's not easy right now to do anything.	MP
Q8.3	AC	So let's say you have this wearable device, and your tracking your health or whatever your tracking, do you think that the company itself has the opportunity to change your data or manipulate it, so they can provide you a higher premium?	
	RP9	I cannot say they cannot do that, they can. But which company is going to do that, I mean the reputation of the company and the risks the company is taking just for doing such a big project, and then killing it by stupid acts like that. At the end of the day, manipulation of data can happen without even doing a project.	MP
Q8.4	AC	Do you consider secondary use of data as a risk for you? Like providing your data to another company without your consent?	
	RP9	Well, that will depend, if that will happen when you sign on the agreement or something like that, there should be mentioned that your data will be sold to third parties, but if that's the case I won't participate.	
Q8.5	AC	Don't you consider it as discrimination when offering somebody who is not healthy a higher policy premium, whereas actually giving healthy people a lower premium?	
	RP9	That depends on the system your living in, or the country you're living in: if the country is totally based on the free market, this is how it is, your accepting the fact that you are living in such a system. It's not your fault, and not the business fault, it's not the insurance company fault, this is the system that you accepted living in. But if you are living in a system that considers, ... I am comparing United States to Sweden. In Sweden this is considered a high priority to take a health care, so in United States its privatized, where here it is public. So that's the difference, in the United States, I think it's fine, cause people there are fine with the fact that they have to pay.	

	AC	But from your own point of view, since that you're Lebanese as you said: don't you consider it as a discrimination, to provide people with higher premiums, based on their health status?	
	RP9	Yes, from my country's point of view, I think it is. Because we don't have a system actually at all. So, people actually know why should we run away from the fact that when you fill an insurance form, they ask you if you are a smoker or not, if you are a smoker, you pay around 20% more than any other insurance policy, but that's agreeing actually with the fact that they actually they are letting you pay more money because you smoke. If you are a smoker and a drinker, you will get up to pay for up to 30% higher premiums. If you have already pre-identified diseases, you will have also to pay more, so it's like, it's the risk analysis, I mean if you want to study it logically and objectively it's a risk analysis. From a humanitarian point of view, I think insurance companies should have hard governance, like the governments should put strict restrictions on their behavior and the systems they apply, because if they leave them without regulations and governance, inhuman things may happen.	
Q9	AC	Moving on to the perceived benefits: for what reason would you disclose your health data to insurance companies? Do you think there are any benefits affiliated to disclosing your health information to insurance companies?	
	RP9	Depends if this is with return to me for example for my health assessment, and they can actually tell me. If they have a program that can improve my health quality, they just need my data for the sake of cutting down 10% of my premium, no I will not accept that. There should be a program.	IS
Q9.1	AC	So you don't think that financial discounts would positively influence your willingness to disclose you information?	
	RP9	If it is a significant discount, yes.	FB
	AC	10% is really a significant discount.	
	RP9	No, I don't think that is enough, I am selling my data of every day, of my day life. I will be an experiment subject, if you think about it, you are an experiment subject, you are not being harmed, but somebody is actually gathering your data and doing something about it, even if your name is not listed there.	
Q9.2	AC	Even receiving a free fitness tracker, don't you consider it as a benefit, or a motivator for better health?	
	RP9	Am telling you, I would actually be really interested as long as there is a program to help me be healthy. It's not like wear a tracker for free, and we will give you 10%. There should be an incentive, I mean insurance companies should not be looking for 10% premium discount only, they should be looking at how to keep this person healthy to encourage him to be healthy.	IS IS
Q9.5	AC	Do you think that this wearable device would give you a social image to be accepted upon a group of friends by showing your friends that you have the latest wearable device from this insurance?	
	RP9	Yes, it can be a trend, but not in my age. I mean at my age, I don't give a fuck. But it can become a trend, if the wearable is fancy and it matches all the ages, and maybe you have some market segmentation, lets say teenagers, you give them a very fancy gadget which is	SI

		colorful, and has some stuff and music or it links to Wi-Fi, or whatever, I mean you need to target in this case the people, the segments of the social society or the community you are working with. So you can turn it into a trend, that is a good idea.	
Q9.6	AC	Do you think that the insurance company through the data they collect, they can improve services?	
	RP9	What services?	
	AC	Any type of service. Maybe their insurance service by itself, or by providing the data to third parties, offering you something that suits you based on your health.	
	RP9	No, I won't accept that.	
Q10	AC	So considering all the aspects, like weighing the benefits and risks: would you be willing to disclose your health information to an insurance company?	
	RP9	Yes, but as I said based on what I have said before. The if's that I have mentioned: so, if the company has a program for people to get a better health, then it is okay, it is not like wearing a device, getting my data, and giving me 10% premium and leave me.	
Q9.1	AC	You don't think financials is an incentive by itself?	
	RP9	No, I don't. I think they should encourage people to be more healthy. For example, I am a very illiterate person in diets: what to eat and what not to eat and what to do and how to sport, or walk... I am very illiterate. And I think there is a lot of people that are the same. We move normally, but we don't exercise, so I need consultancy or maybe something like an application, that might help me, it tells me today you do 1, 2, 3, tomorrow, you know what I mean? It is a program that you can set for yourself, and it's not very hard.	HM
Q11	AC	How would you describe your health status? Do you have any severe illness or are you totally fine?	
	RP9	No, I am fine.	
Q12	AC	Do you think your opinion towards the issue of wearables in the insurance context would change, if you were in a different health state?	
	RP9	No.	
	AC	If you weren't in a good health state would you be also willing to disclose your information?	
	RP9	Yes.	
	AC	Even if you are going to pay more premium?	
	RP9	Ahhh, you mean if I was actually forced to?	
	AC	No you're not forced, but let's say you're not in a good health, and you want to buy an insurance policy, would you go for that policy?	
	RP9	Yes, I will go.	
Q13	AC	Would you say that you trust your insurance company?	
	RP9	Yes. But trust in what terms? That they will give me the benefits?	
	AC	Trust in everything. They will give you the benefits, they won't discriminate, they won't manipulate your data...	
	RP9	Ah, manipulate data, I don't know about that, I can't say yes or no.	
	AC	So you don't trust them.	
	RP9	No, I don't have an answer for that, because am not sure about it. They say they will not manipulate, and I am not sure, if they don't manipulate.	

---

Q14	AC	The last question: Is there anything you'd like to add in terms of the adoption of wearables for health and life insurance that you feel I didn't shed the light on and you would like to consider?	
	RP9	What I said already before, about the incentive for people to do more about their health, they should take care of their health with programs for exercising, or what they should eat.	IS
	AC	Thank you for your time and participation.	

## References

- Accenture. (2015, May, 5). Accenture Insurance Technology Vision 2015. *Accenture Newsroom*. Retrieved from <https://newsroom.accenture.com/industries/insurance/insurers-set-to-embrace-wearable-technologies-which-they-believe-will-have-a-significant-impact-on-their-industry-according-to-accenture-insurance-technology-vision-2015.htm> [2016, April, 24].
- Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal and Ubiquitous Computing*, 8(6), 430-439.
- AIA. (2016). AIA Vitality. *AIA Australia Limited*. Retrieved from <http://www.aia.com.au/en/individual/our-products/aia-vitality.html> [2016, May, 3].
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179-211.
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs (USA): Prentice-Hall.
- Al-Saggaf, Y. (2015). The use of data mining by private health insurance companies and customers' privacy. *Cambridge Quarterly of Healthcare Ethics*, 24(03), 281-292.
- Alvesson, M., & Sköldbberg, K. (2009). *Reflexive methodology: New vistas for qualitative research*. London: Sage.
- Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.
- Angst, C. M. (2009). Protect my privacy or support the common good? Ethical questions about electronic health information exchanges. *Journal of Business Ethics*, 90(2), 169-178.
- Armstrong, K., Weber, B., FitzGerald, G., Hershey, J. C., Pauly, M. V., Lemaire, J., et al. (2003). Life insurance and breast cancer risk assessment: adverse selection, genetic testing decisions, and discrimination. *American Journal of Medical Genetics, Part A*, 120(3), 359-364.
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138-150.
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270.
- Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society*, 27(4), 220-232.

- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5), 313-324.
- Bernard, H. R. (2011). *Research methods in anthropology: Qualitative and quantitative approaches*. Walnut Creek, CA: AltaMira Press.
- Bhattacharjee, A. (2012). *Social science research: principles, methods, and practices* (2nd ed.). Tampa (USA): Open Access Textbooks.
- Billinghurst, M., & Starner, T. (1999). Wearable devices: new ways to manage information. *IEEE Computer*, 32(1), 57-64.
- Bolderdijk, J., Knockaert, J., Steg, E., & Verhoef, E. (2011). Effects of Pay-As-You-Drive vehicle insurance on young drivers' speed choice: Results of a Dutch field experiment. *Accident Analysis & Prevention*, 43(3), 1181-1186.
- Borna, S., & Avila, S. (1999). Genetic information: Consumers' right to privacy versus insurance companies' right to know - A public opinion survey. *Journal of Business Ethics*, 19(4), 355-362.
- Bottles, K. (2012). Will the quantified self movement take off in health care. *Physician Executive*, 38(5), 74-75.
- Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, 15(5), 662-679.
- Britton, K. E. (n.d.). IoT Big Data: Consumer Wearables Data Privacy and Security. *ABA Section of Intellectual Property Law*.
- Bryman, A. (2004). *Social Research Methods*. New York: Oxford University Press Inc.
- CambridgeDictionaries. (2016). Definition: discrimination. Retrieved from <http://dictionary.cambridge.org/dictionary/english/discrimination> [2016, April, 10].
- Cardon, J. H., & Hendel, I. (2001). Asymmetric information in health insurance. *RAND Journal of Economics*, 32, 408-427.
- Chan, M., Estève, D., Fourniols, J.-Y., Escriba, C., & Campo, E. (2012). Smart wearable systems: Current status and future challenges. *Artificial Intelligence in Medicine*, 56(3), 137-156.
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2-3), 181-202.
- Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36(4), 1165-1188.
- Christophersen, M., Mørck, P., Langhoff, T. O., & Bjørn, P. (2015). Unforeseen Challenges *Universal Access in Human-Computer Interaction. Access to Learning, Health and Well-Being* (pp. 288-299): Springer.
- Corbin, J., & Strauss, A. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, CA: Sage Publications, Inc.
- Council. (2008). *Six Technologies With Potential Impacts on US Interests Out to 2025*. Retrieved from <https://fas.org/irp/nic/disruptive.pdf>
- Crawford, K., Gray, M. L., & Miltner, K. (2014). Critiquing Big Data: Politics, ethics, epistemology. *International Journal of Communication*, 8, 1663-1672.
- Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks, CA: Sage.
- Culnan, M. J. (1993). "How Did They Get My Name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341-363.

- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115.
- Davenport, T. H. (2006). Competing on analytics. *Harvard Business Review*, 84(1), 98-107.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.
- De Mauro, A., Greco, M., & Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. *AIP Conference Proceedings*, 1644(1), 97-104.
- Di Pietro, R., & Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, 46(9), 74-79.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – A study of Italy and the United States. *European Journal of Information Systems*, 15(4), 389-402.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316.
- Eckel, C. C., & Grossman, P. J. (2008). Men, women and risk aversion: Experimental evidence. *Handbook of Experimental Economics Results*, 1061-1073.
- Economist. (2015, March 14). Data and technology are starting to up-end the insurance business. *The Economist*. Retrieved from <http://www.economist.com/news/finance-and-economics/21646260-data-and-technology-are-starting-up-end-insurance-business-risk-and-reward> [2016, March, 14].
- Endt, C. (2014, December 12). Wollen wir wirklich in dieser Welt leben? *Süddeutsche Zeitung*. Retrieved from <http://www.sueddeutsche.de/digital/datensammlung-von-versicherungen-wollen-wir-wirklich-in-dieser-welt-leben-1.2260345> [2016, April, 10].
- FBI. (2016). Insurance Fraud. *Federal Bureau of Investigation*. Retrieved from <https://www.fbi.gov/stats-services/publications/insurance-fraud> [2016, April, 27].
- Frambach, J. M., van der Vleuten, C. P., & Durning, S. J. (2013). Quality Criteria in Qualitative and Quantitative Research. *Academic Medicine*, 88(4), 552.
- Fritz, T., Huang, E. M., Murphy, G. C., & Zimmermann, T. (2014). Persuasive technology in the real world: a study of long-term use of activity sensing devices for fitness. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 487-496.
- Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137-144.
- Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, 115(9), 1704-1723.
- Gaulding, J. (1994). Race Sex and Genetic Discrimination in Insurance: What's Fair. *80 Cornell Law Review*, 1646.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 27(1), 51-90.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645-1660.
- Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the US and in India. *Journal of Electronic Commerce Research*, 11(1), 41-52.

- Hancock. (2016). Life Insurance. *John Hancock*. Retrieved from <http://www.johnhancock.com/products/life-insurance.html> [2016, April, 20].
- Handel, M. J. (2011). mHealth (mobile health) - Using apps for health and wellness. *EXPLORE: The Journal of Science and Healing*, 7(4), 256-261.
- Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). *Online information privacy: Measuring the cost-benefit trade-off*. Paper presented at the International Conference on Information Systems, Barcelona, Spain.
- Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, 31(1), 19-33.
- HumanaVitality. (2016). HumanaVitality - a wellness and rewards program. *Humana Inc*. Retrieved from <https://www.humana.com/vitality/> [2016, May, 3].
- Janker, K. (2014, November, 26). Wir werden manipulierbar und unfrei. *Süddeutsche Zeitung*. Retrieved from <http://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generalmodell-wir-werden-manipulierbar-und-unfrei-1.2232147> [2016, April, 9].
- Jurgens, B. (2015, August, 17). How IoT will change your relationship with insurance. *TechCrunch*. Retrieved from <http://techcrunch.com/2015/08/17/how-iot-will-change-your-relationship-with-insurance/> [2016, March, 28].
- Kim, K. J., & Shin, D.-H. (2015). An acceptance model for smart watches: implications for the adoption of future wearable technology. *Internet Research*, 25(4), 527-541.
- Kranz, M., Möller, A., Hammerla, N., Diewald, S., Plötz, T., Olivier, P., et al. (2013). The mobile fitness coach: Towards individualized skill assessment using personalized mobile devices. *Pervasive and Mobile Computing*, 9(2), 203-215.
- Kvale, S. (1996). The 1,000-page question. *Qualitative Inquiry*, 2(3), 275-284.
- Kvale, S. (2007). *Doing interviews* (Vol. 2). London (UK): Sage.
- Labrinidis, A., & Jagadish, H. (2012). Challenges and opportunities with big data. *Proceedings of the VLDB Endowment*, 5(12), 2032-2033.
- Langley, M. R. (2014). Hide Your Health: Addressing the new privacy problem of consumer wearables. *130 Geo Law Journal*, 1641-1659.
- Lapadat, J. C., & Lindsay, A. C. (1999). Transcription in research and practice: From standardization of technique to interpretive positionings. *Qualitative Inquiry*, 5(1), 64-86.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22-42.
- Lewis, M. (2004). *Moneyball: The art of winning an unfair game*. New York (USA): WW Norton.
- Lin, C. P., & Bhattacharjee, A. (2010). Extending technology usage models to interactive hedonic technologies: A theoretical model and empirical test. *Information Systems Journal*, 20(2), 163-181.
- Lincoln, Y. S. (1995). Emerging criteria for quality in qualitative and interpretive research. *Qualitative Inquiry*, 1(3), 275-289.
- Litman, T. (2015). Pay-As-You-Drive vehicle insurance: Converting vehicle insurance premiums into use-based charges. *Victoria Transport Policy Institute*. Retrieved from <http://www.vtpi.org/tdm/tdm79.htm> [2016, April, 4].
- Long, J. D. (1990). *Ethics, Morality, and Insurance*. Indiana University, Graduate School of Business.
- Lu, Y., Tan, B., & Hui, K.-L. (2004). Inducing customers to disclose personal information to internet businesses with social adjustment benefits. *Proceedings of International Conference on Information Systems*, 272-281.

- Lymberis, A. (2003). Smart wearables for remote health monitoring, from prevention to rehabilitation: current R&D, future challenges. *Proceedings of 4th IEEE Conference on Information Technology Applications in Biomedicine*, 272-275.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
- Manral, J. (2015). IoT enabled insurance ecosystem - Possibilities, challenges and risks. *arXiv*(1-18).
- Marcus, G., & Davis, E. (2014, April 6). Eight (No, Nine!) Problems With Big Data. *The New York Times*. Retrieved from <http://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html> [2016, April, 27].
- Marr, B. (2015, December 16). How Big Data Is Changing Insurance Forever. *Forbes*. Retrieved from <http://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/> [2016, March, 10].
- Martin, A. (2015, May, 21). Step and save: The truth about wearables and health insurance. *Wearable*. Retrieved from <http://www.wearable.com/wearable-tech/step-and-save-the-risks-of-using-fitness-tracker-to-save-on-your-insurance-premium-1163> [2016, April, 17].
- Mason. (2014). Smart wearables: worldwide market trends, forecasts and strategies 2014-2020. *Analysys Mason*. Retrieved from <http://www.analysismason.com/Research/Content/Reports/Smart-wearables-forecast-Sep2014-RDMD0/> [2016, April, 28].
- Mayer, C. P. (2009). Security and privacy challenges in the internet of things. *Electronic Communications of the EASST*, 17.
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. London (UK): Houghton Mifflin Harcourt.
- Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the Internet of Things, *The Internet of Things* (pp. 389-395). New York (USA): Springer.
- Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. *Proceedings of the 8th Annual International Conference of the IEEE Engineering in Medicine and Biology*, 5453-5458.
- Merriam, S. B. (2002). *Qualitative research in practice: Examples for discussion and analysis*. San Francisco (USA): Jossey-Bass Inc.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), 1497-1516.
- Müller, C. D., & Zimmermann, H.-D. (2003). Beyond mobile: research topics for upcoming technologies in the insurance industry. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*, 197.
- Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, 17(1), 2-26.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.
- Olson, P. (2014, June, 19). Wearable tech is plugging into health insurance. *Forbes*. Retrieved from <http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/-3237357a5ba1> [2016, April, 5].
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, 2(1), 1-28.

- Park, J., & Zeanah, A. E. (2005). An evaluation of voice recognition software for use in interview-based research: A research note. *Qualitative Research, 5*(2), 245-251.
- Pedersen, D. M. (1982). Personality correlates of privacy. *The Journal of Psychology, 112*(1), 11-14.
- Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*(85), 85-178.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.
- Pickard, K. T. (2014). Exploring markets of data for personal health information. *IEEE International Conference on Data Mining Workshop* 477-480.
- Recker, J. (2013). *Scientific research in information systems: a beginner's guide*. New York (USA): Springer.
- Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research, 26*(1-2), 81-99.
- Sandelowski, M. (2000). Focus on research methods - whatever happened to qualitative description? *Research in Nursing and Health, 23*(4), 334-340.
- SANS. (2016). Information Security Resources. *SANS Institute*. Retrieved from <https://www.sans.org/information-security/> [2016, April, 19].
- Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research methods for business students*. Essex: Pearson Education.
- Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2-16.
- Schroeck, M., & Shockely, R. (2015). Analytics: Real-world use of big data in insurance. *IBM Institute for Business Value*. Retrieved from <http://www-935.ibm.com/services/us/gbs/thoughtleadership/big-data-insurance/> [2016, March, 22].
- Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization, 21*(1), 1-16.
- Seale, C. (1999). Quality in qualitative research. *Qualitative Inquiry, 5*(4), 465-478.
- Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24-38.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.
- Solove, D. J. (2006). A taxonomy of privacy. *154 University of Pennsylvania Law Review, 477-564*.
- Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459-468.
- Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8*(3), 349-411.
- Sun, Y., Wang, N., & Shen, X.-L. (2014). *Perceived benefits, privacy risks, and perceived justice in location information disclosure: a moderated mediation analysis*. Paper presented at the Pacific Asia Conference on Information Systems (PACIS'14).
- Sundar, S. S., Bellur, S., & Jia, H. (2012). Motivational technologies: a theoretical framework for designing preventive health applications. *Persuasive Technology, 7284*, 112-122.

- Sundar, S. S., Tamul, D. J., & Wu, M. (2014). Capturing “cool”: Measures for assessing coolness of technological products. *International Journal of Human-Computer Studies*, 72(2), 169-180.
- Sureify. (2016). Personalized Premium Life Insurance. *Sureify Labs, Inc.* Retrieved from <https://www.sureify.com/> [2016, April, 10].
- Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data*, 1(2), 85-99.
- Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online*, 64, 63.
- Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry*, 16(10), 837-851.
- Treiblmaier, H., & Chong, S. (2012). Trust and perceived risk of personal information as antecedents of online information disclosure. *Global Diffusion and Adoption of Technologies for Knowledge and Information Sharing* (pp. 341-358).
- Troncoso, C., Danezis, G., Kosta, E., Balasch, J., & Preneel, B. (2011). PriPAYD: Privacy-friendly pay-as-you-drive insurance. *Proceedings of WPES 2007*, 99-107.
- Uilenberg, A. (2015). *Willingness to disclose personal information when shopping online: a comparison between consumers from the Netherlands, Germany, and Indonesia*. University of Twente.
- Vaia, G., Carmel, E., DeLone, W., Trautsch, H., & Menichetti, F. (2012). Vehicle telematics at an Italian insurer: New auto insurance products and a new industry ecosystem. *MIS Quarterly Executive*, 11(3), 113-125.
- Van Dijk, J. (2012). *The network society, Social aspects of new media*. Thousand Oaks, CA (USA): Sage.
- van Rijmenam, M. (2016). Big Data impacts society, but what will be the impact of society on Big Data? *DATAFLOQ*. Retrieved from <https://dataflog.com/read/big-data-will-have-a-big-impact-on-society/212> [2016, April, 23].
- Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157-178.
- VitalityLIFE. (2016). Life Insurance for you. *Vitality LIFE*. Retrieved from <https://www.pruprotect.co.uk/> [2016, April, 20].
- Vroom, V. H. (1964). *Work and Motivation*. New York: Wiley.
- Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, 22(2), 157-174.
- Ward, J. S., & Barker, A. (2013). Undefined by data: a survey of big data definitions. *arXiv preprint arXiv:1309.5821*.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.
- Washington. (2016). 'Big Data' Research and Education. *University of Washington*. Retrieved from <http://www.cs.washington.edu/research/bigdata> [2016, March, 19].
- Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30.
- Westin, A. F. (1967). *Privacy and Freedom*. New York (USA): Atheneum.
- Westin, A. F. (2001). Opinion surveys: What consumers have to say about information privacy. Retrieved from <https://catalog.hathitrust.org/Record/012403933> [2016, May, 10].
- Worham, L. (1985). Insurance classification: Too important to be left to the actuaries. *19 University of Michigan Journal of Law Reform and Legislation*, 349.

- Xu, Y., Tan, B., & Hui, K.-L. (2003). Consumer trust and online information privacy. *Proceedings of the 24th International Conference on Information Systems (ICIS'03)*, 538-548.
- Yang, H., Yu, J., Zo, H., & Choi, M. (2016). User acceptance of wearable devices: An extended perspective of perceived value. *Telematics and Informatics*, 33(2), 256-269.
- Zeh, J. (2014, November 26). Wir werden manipulierbar und unfrei. *Süddeutsche Zeitung*. Retrieved from <http://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generalmodell-wir-werden-manipulierbar-und-unfrei-1.2232147> [2016, May, 2].
- Zikopoulos, P., Parasuraman, K., Deutsch, T., Giles, J., & Corrigan, D. (2012). *Harness the power of big data*: McGraw Hill Professional.
- Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management*, 47(2), 115-123.