Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2016 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 6-27-2016

PRIVACY-RELATED DECISION-MAKING IN THE CONTEXT OF WEARABLE USE

Alexander Wieneke
University of St.Gallen, alexander.wieneke@unisg.ch

Christiane Lehrer
University of St.Gallen, christiane.lehrer@unisg.ch

Raphael Zeder
University of St.Gallen, raphael.zeder@gmail.com

Reinhard Jung
University of St.Gallen, reinhard.jung@unisg.ch

PRIVACY-RELATED DECISION-MAKING IN THE CONTEXT OF WEARABLE USE

Alexander Wieneke, Institute for Information Management, University of St.Gallen, St.Gallen, Switzerland, alexander.wieneke@unisg.ch

Christiane Lehrer, Institute for Information Management, University of St.Gallen, St.Gallen, Switzerland, christiane.lehrer@unisg.ch

Raphael Zeder, Institute for Information Management, University of St.Gallen, St.Gallen, Switzerland, raphael.zeder@gmail.com

Reinhard Jung, Institute for Information Management, University of St.Gallen, St.Gallen, Switzerland, reinhard.jung@unisg.ch

Abstract

The widespread use of wearables for self-tracking activities despite potential privacy risks is an intriguing phenomenon. For firms, the data collected from individuals' wearable use are highly valuable for generating in-depth customer insights. Accordingly, firms have an increasing desire for these data. Despite the undisputed relevance of self-tracking activities in practice, there is scarce knowledge among information systems (IS) scholars about the perceived values of wearables that drive individuals' use and the reasons why these values prevail over the privacy risks. Against this background, our research set out to better understand why people use wearables despite privacy risks by investigating the perceived values of wearables that drive individuals' use and disclosure of data and the reasons why these values prevail over privacy risks of wearable use. Based on the concept of the privacy calculus and concepts from behavioural decision-making, we conducted in-depth interviews with 22 wearable users from Switzerland. As a result, we reveal eight values that individuals perceive through the use of wearable devices. Furthermore, we illustrate the low awareness regarding privacy risks and explain how the reliance on prominent dimensions and heuristics are influencing individuals' value-risk assessment.

Keywords: Information privacy, Laddering, Privacy-related decision-making, Wearables

1 INTRODUCTION

Recent advances in battery longevity, cheap massive storage and low-cost sensors have spawned a new generation of devices, so-called wearables (Trickler 2013). Wearables are digital devices in the shape of watches, wristbands, glasses or textiles with the ability "*to monitor the minutiae of our everyday lives*" (Newell & Marabelli 2015, p. 3). The embedded sensors track daily activities or vital parameters and collect personal data (Buchwald et al. 2015; Sjöklint et al. 2015; Trickler 2013). Individuals often use wearables to quantify various aspects of their lives with the objective of generating *"insight and even predict certain realities about oneself"* (Trickler 2013, p. 197). In fact, this individual activity, also called self-tracking, has become an emerging trend in society (Sjöklint et al. 2015). The use of wearables is constantly increasing, and it is forecasted that the worldwide wearables market will grow from fewer than 20 million units in 2014 to more than 126 million units in 2019 (IDC 2015). However, the use of wearables, especially in the context of self-tracking, is a double-edged sword, simultaneously presenting value and risks (Buchwald et al. 2015; Xu et al. 2009). The overall values are "*built upon the explanatory power of continuously collected data*" (Buchwald et al. 2015, p. 3). The risks arise from individuals wearing the devices whenever possible and becoming a "*walking data generator*" (McAfee & Brynjolfsson 2012, p. 5). New techniques for advanced data analytics (Chen et al. 2012) allow firms to collect the data and compile customers' "*digital footprints into a comprehensive picture of an individual's daily-life facets*" (Zhang et al. 2011, p. 21). Unsurprisingly, much has been written in the press and the scientific community about the possible loss of privacy caused by, for example, stolen data or illegal capture of data (Markus 2015; Markus & Topi 2015). Accordingly, more than 45% of wearable users are concerned about breaches of privacy through wearable use (Mills 2015). The paradox between the increasing diffusion of wearables and the extensively discussed privacy risks illustrates a general phenomenon of digital technology whereby individuals are willing to disclose personal data despite their privacy concerns if the values outweigh the costs (Newell & Marabelli 2015).

Firms, such as insurance companies or sporting goods manufacturers, have developed an insatiable desire for data gathered by fitness apps or digital devices (Newell & Marabelli 2014; Trickler 2013). This type of data provides them with valuable information for the generation of in-depth customer insights (Newell & Marabelli 2014). Despite this undisputed relevance in practice, there is scarce knowledge among information systems (IS) scholars about the perceived values of wearables that drive individuals' use and the reasons why these values prevail over the privacy risks (Markus & Topi 2015; Min & Kim 2015; Newell & Marabelli 2015). Previous studies in the field of information privacy primarily focused on identifying privacy concerns (e.g., Motti & Caine 2015) and how to reduce privacy risks (e.g., Xu et al. 2009). Another stream in this research field investigates how individuals react to information privacy policies (e.g., Zhao et al. 2012), practices (e.g., Xu et al. 2011) and tools (e.g., Sutanto et al. 2013). Further research studied the role of situation-specific considerations influencing the assessment of privacy risks and values (e.g., Acquisti et al. 2012; Dinev et al. 2015; Kehr et al. 2015). Only a small number of studies empirically investigated the influence of perceived values (e.g., personalisation, financial rewards) on individuals' willingness to disclose personal data (e.g., Sun et al. 2015; Zhao et al. 2012). However, most of this research was conducted in the context of e-commerce, social network applications, location-based services (LBS) or mobile apps. Research in the context of wearables focusing on perceived value or individuals' value-risk assessment has been scarce to date. However, there are some pioneering studies about privacy concerns regarding mobile health (e.g., Anderson & Agarwal 2011), individuals' adoption of wearables in healthcare (e.g., Gao et al. 2015) or behavioural change through wearable use (e.g., Sjöklint et al. 2015).

To close this research gap and better understand why people use wearables despite privacy risks, our research focuses on investigating the perceived values of wearables that drive individuals' use and data disclosure and the reasons why these values prevail over privacy risks of wearable use. In the privacy literature, the perceived risks are generally understood as the "*potential for loss associated with the release of personal information*" (Smith et al. 2011, p. 1001). The perceived values are described as the potential for enjoying positive consequences from data disclosure (Wilson & Valacich 2012). For our

research purposes, we focus on wearables in the shape of bracelets and watches used in the context of self-tracking and offered by service providers, such as Fitbit, Jawbone, Apple or Samsung. Together, these types of wearables account for more than 90% of the worldwide wearables market (IDC 2015). The research questions of our paper are:

RQ 1. *What are the perceived values of wearables that drive individuals' use and disclosure of personal data?*

RQ 2. *Why do these values prevail over the privacy risks?*

We address these questions by applying the theoretical lens of the privacy calculus and conducting in-depth interviews with 22 wearable users from Switzerland. To gather detailed information about the actual perceived values of wearables that drive individuals' use and the actual reasons why these values prevail over privacy risks of wearable use, we focus solely on individuals using wearables in their everyday lives. This means that our research primarily focuses on aspects influencing the continuance wearable use. To answer both research questions, we applied different interview techniques. First, we applied the means-end chain analysis approach (Gutman 1982) and used the laddering interview technique (Reynold & Gutman 1988) to examine how individuals translate the attributes of wearables into meaningful value. Second, we used the semi-structured interview technique (Lacity & Janson 1994) to obtain an in-depth understanding of the reasons why the values prevail over privacy risks. With regard to the first research question, our findings reveal eight values that individuals perceive through the use of wearable devices. Regarding the second research question, we illustrate the low awareness of privacy risks and explain how the reliance on prominent dimensions and heuristics are influencing individuals' privacy-risk assessment.

Our theoretical contribution is threefold. First, we identify and illustrate the perceived values of wearables that drive individuals' use. We suggest that hedonic values are dominant in wearable use. Thereby, we contribute to prior research, which has examined perceived values in the context of e-commerce, social networks and LBS. Second, we emphasise individuals' low awareness in terms of how their data are being used and their low interest in obtaining more information on this topic. Finally, our findings suggest that individuals, under normal circumstances, ignore privacy risks and do not base their decisions on a rational value-risk assessment. Moreover, they appear to base their decision to use wearables predominantly on intuitive processes. Thereby, we contribute to IS research in the field of information privacy, which has emphasised the rational process of privacy-related decision-making (e.g., Dinev & Hart 2004; Dinev et al. 2006). Our results inform practitioners about the value that consumers perceive in the use of wearables and the underlying cognitive processes involved in their privacy-risk assessment. This knowledge helps firms configure their services to provide customers with the perceived value and motivate them to disclose their personal data.

The rest of the paper is organised as follows. The next section gives an overview of the general use of wearables and explains the privacy calculus in detail. Then we present our research approach, followed by a presentation of the identified values and the cognitive processes involved in individuals' value-risk assessment. We then turn to a discussion of the results and emphasise why individuals use wearables despite privacy risks. Additionally, we highlight our theoretical and practical implications. The paper ends with a conclusion providing limitations and suggestions for further research.

2 CONCEPTIONAL BACKGROUND

2.1 Wearables

In recent years, several firms entered the market for wearable devices. The majority of these service providers offer wearables in the shape of bracelets (e.g., Jawbone) and watches (e.g., Fitbit, Apple, Samsung) (IDC 2015). Despite slight differences in appearance, wearable devices usually have the same fundamental technical properties, i.e., integrated sensors, massive storage and software applications. Integrated sensors and massive storage afford the gathering of several data types (e.g., pace, position,

step rate, sleep, blood pressure, caloric intake and expenditure, body mass index) over a long period of time (Li & Wu 2014; Trickler 2013). Different technologies for data transfer (e.g., Bluetooth, WiFi network, headphone port) allow the utilisation of these data sets within applications on mobile devices or desktop computers (Sjöklint et al. 2015). These applications use advanced data analytics to generate insights about different aspects of individuals' lives (Buchwald et al. 2015). Based on these abilities, service providers describe wearables as a "*revolutionary system that guides you every step of the way to a better, healthier you*" (Jawbone 2016) or as devices that "*fit seamlessly into your life so you can achieve your health and fitness goals, whatever they may be*" (Fitbit 2016). Accordingly, more and more individuals use these devices for self-tracking activities. Self-tracking is described as the collection of quantitative "*data about the individual's performance in everyday life, such as (...) daily activities, workouts, food consumption, finances or even blood sugar levels*" (Sjöklint et al. 2015, p. 1). Although the activity of self-tracking has already been performed with different tools, such as handwritten notes or smartphone apps, wearables enable individuals to track the activities of their daily lives in a more convenient manner (Buchwald et al. 2015; Newell & Marabelli 2015). When one wears a device in the form of a bracelet or watch all day long, it becomes a part of oneself (Sjöklint et al. 2015). This, in turn, enables service providers to implicitly collect personal data about all facets of individuals' everyday lives (McAfee & Brynjolfsson 2012; Newell & Marabelli 2014). The evolution of business intelligence and analytics allows firms to use mobile, location-aware, person-centred and context-relevant analysis techniques for generating insights about actual market and consumer trends and individual customers' preferences and behavioural patterns (Chen et al. 2012; Setia et al. 2013). Based on these insights, firms are able to provide more individualised products or services and align customer-oriented work practices with customers' needs. Despite the existence of privacy regulations designed for keeping the data safe, firms' use of data gathered through wearables is associated with several privacy risks (Buchwald et al. 2015; Newell & Marabelli 2015). The sensitivity of these data sets (e.g., location-based data, health data) in particular prompt heated discussion about potential privacy intrusion (Buchwald et al. 2015).

It is irrefutable that information gathered by wearables is extremely valuable for several stakeholders, such as businesses and criminals. For example, health insurance companies can use these data sets to assess individuals' health risks to reject potential customers with unhealthy lifestyles or raise the premiums. This could lead to unfair classification or labelling of and unjust discrimination against individuals (Markus 2015; Newell & Marabelli 2014). For criminals, the data can be useful by facilitating analysis of individuals' movement patterns to identify the optimal time for burglary. It is possible that these stakeholders may come into possession of the data sets. Service providers can sell the data to third parties without the explicit consent of the user (Maddox 2016). Additionally, the data can be stolen through a data breach and illegally sold to other people or firms (Markus 2015; Markus & Topi 2015). Moreover, the collected data can be stored for several decades. Over time, "*new laws could be passed that change access to the data that you willingly gave up your privacy rights to share*" (Maddox 2016). Then, it could be legal to use the data for different purposes and share the data with every firm that the service provider wants to share it with. However, paradoxically, the use of wearables is constantly increasing (Buchwald et al. 2015, IDC 2015). According to Newell and Marabelli (2015), "*individuals seem to be likely to accept the 'dark side' of datification through digital traces (always there), and constant monitoring through sensors because they are persuaded that the benefits outweigh the costs*" (p. 11). Thus, to generate scientific evidence about the privacy-related decision-making process, we seek to explore the perceived values of wearables that drive individuals' use and disclosure of data and the reasons why these values prevail over the privacy risks of wearable use. Therefore, in the next section, we discuss the privacy calculus that provides us with a lens suitable to understand the rational and emotional factors underlying people's willingness to disclose data.

2.2 Privacy calculus

In general, information privacy is regarded "*as a human right integral to society's moral value system*" (Smith et al. 2011, p. 992). With the evolution of IT, especially the rise of the internet, the so-called "*general privacy as a right*" concept was reconsidered (Belanger et al. 2011; Smith et al. 2011). The

widespread opportunities to voluntarily disclose information (e.g., on websites) in exchange for several values has eroded the societal tendency to consider information privacy an absolute legal right. For some, information privacy has become "*subject to the economic principles of cost-benefit analysis and trade-off*" (Smith et al. 2011, p. 994). From this perspective, personal data is a currency that can be traded against value-added privileges or advantages (Belanger et al. 2011). Against this background, the "*privacy as a commodity*" concept was established (Smith et al. 2011). According to this concept, many scholars describe the cognitive process of privacy-related decision-making as an economical calculation. They rely on the privacy calculus model, which views privacy-related decision-making as a rational process, "*where individuals weigh the anticipated risks of disclosing personal data against the potential benefits*" (Kehr et al. 2015, p. 607). The privacy risks can be specified as the potential loss of control over personal data due to unauthorised access and theft or transfer of data to other stakeholders (Smith et al. 2011). Moreover, when firms classify their customers, this may lead to discrimination, unfair treatment and even financial disadvantages (Newell & Marabelli 2014; Xu et al. 2009). With regard to the perceived values, prior research typically refers to financial rewards, personalisation and social adjustment as exemplary positive consequences. In summary, the privacy calculus perspective claims that individuals are willing to share personal data voluntarily if they expect to perceive value from data disclosure outweighing the perceived risks (Wilson & Valacich 2012; Xu et al. 2009). However, prior research in the field of information privacy primarily focuses on the identification of perceived risks "*rather than identifying the benefits that people want to gain despite that cost*" (Min & Kim 2015, p. 842). Thus, the perceived values that drive individuals' use of wearables are still underexplored (Min & Kim 2015; Newell & Marabelli 2015).

In recent years, the privacy calculus has become one of the most applied frameworks for analysing the underlying cognitive processes of privacy-related decision-making (Xu et al. 2009). It was widely used by scholars in previous empirical studies (e.g., Dinev et al. 2006; Dinev & Hart 2004; Xu et al. 2009; Zhao et al. 2012). However, as shown by Dinev et al. (2015) and Kehr et al. (2015), the value-risk assessment may not necessarily be based on an objective and rational mathematical calculation. More than likely, the rational assessment process is "*bereft of biased assumptions or cognitive shortcuts*" (Dinev et al. 2015, p. 640). This means that individuals' privacy-related decision-making is affected by psychological limitations. Normally, individuals do not have the ability to process all the information required to make a rational and objective value-risk assessment (Min & Kim 2015). This is reflected in individuals' employment of "*low-effort cognitive processes*" (Dinev et al. 2015, p. 640), such as heuristics, to simplify decision-making (Dinev et al. 2015; Min & Kim 2015). In relation to information privacy, Min and Kim (2015) describe heuristics as cognitive processes "*through which people evaluate costs and benefits (...) by attaching subjective values to them, although those may be completely arbitrary*" (p. 841). In more detail, Kehr et al. (2015) identified the influence of the affect heuristic on individuals' risk and value perception. The affect heuristic emphasises the key role of emotions in decision-making (Bazerman & Moore 2008). Furthermore, Kehr et al. (2013) demonstrated the influence of dispositional factors on the weighing of values and risks (Kehr et al. 2013; Kehr et al. 2015). Dispositional factors may be individuals' subjective sense of privacy concerns and institutional trust (Kehr et al. 2013). Against this background, there has been a call in IS research to scrutinise the assumption of rational decision-making and examine the influence of intuitive processes on privacy-related decision-making (Dinev et al. 2015).

With regard to our research questions, we identify the perceived values of wearables that drive individuals' use. Additionally, we aim to understand why the perceived values prevail over the privacy risks of wearable use. For this purpose, we study the cognitive processes involved in individuals' value-risk assessment.

3 METHODICAL BACKGROUND

3.1 Research approach

This study aims to provide a better understanding of why people use wearables despite privacy risks. For this purpose, we employed a qualitative research approach and conducted 22 in-depth interviews with wearable users from Switzerland. This approach allowed us to gain a deep understanding of the underlying cognitive processes in individuals' privacy-related decision-making (Constantiou et al. 2014). Because research on wearable use has been scarce to date, the interviews were exploratory in nature. To gather detailed information about the perceived values of wearables that drive individuals' use and the reasons why these values prevail over the privacy risks of wearable use, we interviewed actual users of wearables. In our sample, we did not include people who had never adopted wearables or those who had discontinued their use. For our sample, we targeted wearable users of both genders (i.e., 7 females and 15 males) ages 23 to 59 years old (Table 1). Our sample contains an over-representation of males. This is in line with the specific target groups of similar studies examining the use of mobile devices or mobile applications in Europe (e.g., Constantiou et al. 2014). Additionally, the majority of wearable users in Switzerland are men (Statista 2016a). Because the diffusion of wearables in Switzerland is limited, i.e., only 3% percent of the population use wearables (Statista 2016b), the respondents can be described as early adopters (Rogers 1995). Accordingly, most of the respondents described themselves as very health-conscious and technology affine. The interviews were conducted in German from January to February 2016. Each interview lasted between 35 and 45 minutes and was audio recorded and transcribed. In sum, we generated 188 pages of interview transcripts. To answer both of the research questions of this paper, we used two different interview techniques. First, we applied the means-end chain analysis (MECA) approach (Gutman 1982) and the laddering interview technique (Reynolds & Gutman 1988) to identify the perceived values of wearables that drive individuals' use. Second, we used the semi-structured interview technique (Lacity & Janson 1994) to investigate why these values prevail over the privacy risks of wearable use.

Contextual factors	Interviewees' characteristics
Gender	32% female; 68% male
Age	From 23 to 59 years; average 36
Occupational area	18% students; 50% private sector; 32% public sector

Table 1. Descriptive statistics of participants

3.2 Research design

Means-end chain analysis is a qualitative research approach used for in-depth analysis of individuals' cognitive decision-making processes (e.g., Jung 2014; Schäfer 2013; Wagner 2007). It helps scholars uncover the underlying drivers of individuals' decisions, e.g., purchase or use decisions (Reynold & Gutman 1988). The approach is based on the assumption that product and service attributes are associated with consequences and personal values that the product or service can provide to individuals. The MECA approach "*specifically focuses on the linkages between the attributes that exist in products (the "means"), the consequences for the consumer provided by the attributes and the personal values (the "ends") the consequences reinforce*" (Reynold & Gutman 1988, p. 11). Accordingly, the result is a means-end chain linking attributes to consequences to underlying personal values. Attributes are defined as "*perceived qualities or features of products or services*" (Reynolds & Olson 2001, p. 92) (e.g., pulse monitor, altimeter). Consequences "*may be defined as any result (…) accruing directly or indirectly to the consumer (sooner or later) from his/her behaviour*" (Gutman 1982, p. 61). According to Olson and Reynolds (2001), consequences can be separated into functional and psychological consequences. Functional consequences represent qualitative outcomes that are directly related to the use of the product or service (Schäfer 2013; Wagner 2007) (e.g., universally applicable, profiling oneself). Psychological consequences "*reflect the personal and social outcomes of product usage*" (Reynolds et al. 1995, p. 258)

(e.g., self-awareness, self-control). Values "*imply highly abstract motivation that guides usage behaviour*" (Jung & Kang 2010, p. 220) and illustrate the desirable end states of product or service use (e.g., success, health). Designing a means-end chain in the context of wearables allows us to uncover the drivers, i.e., the underlying values behind individuals' decision to use wearables and thereby disclose their personal data despite the privacy risks.

To uncover the means-end chain and define the attributes, functional consequences, psychological consequences and values and the linkages between the key elements, Reynolds and Gutman (1988) proposed the use of the in-depth interviewing and analysis methodology named laddering. Laddering can be described as a "*one-on-one interviewing technique used to develop an understanding of how consumers translate the attributes of products into meaningful associations with respect to self, following means-end theory*" (Reynolds & Gutman 1988, p. 12). The overall objective is the creation of a cognitive hierarchical value map (HVM) illustrating the interrelations between the key elements (i.e., attributes, functional and psychological consequences and values) of a given product or service (Gutman 1982, Reynolds & Gutman 1988, Wagner 2007). Thus, a HVM provides insights into individuals' hierarchical cognitive structures and allows drawing conclusions about the expected values of product or service use. To ensure rigor in qualitative research and avoid potential subjective biases, we followed the established guidelines of Reynolds and Gutman (1988) for conducting and analysing laddering interviews. As a first step in a laddering interview, the interviewee is asked about the relevant attributes of a product or service. The stated attributes then serve as a starting point for the laddering procedure. This means that the interviewer refers to one attribute and asks the responder questions along the lines of "Why is this important to you?" After the interviewee's answer, the question is repeated until the level of the terminal value is reached. This procedure enables the interviewer to ascend the "ladder" of the means-end chain hierarchy. Thus, as a result, the interviewer gains a set of ladders for each interviewee (Reynolds & Gutman 1988). For our research purposes, we began with questions about the contexts of wearable use, the reasons for use and personal experiences. We then asked the respondents "What attributes make wearables attractive to you?" To focus on the relevant attributes, we applied the direct elicitation method, as suggested by Bech-Larsen and Nielsen (1999). In this method, the interviewees note the attributes most important for them without prioritising or assigning the attributes to specific products. The procedure comes close to a "'*natural speech' interviewing technique, which compared to the other techniques is believed to lead to a stronger focus on idiosyncratic and intrinsically relevant attributes and to less focus on extrinsic product differences*" (Bech-Larsen & Nielsen 1999, p. 317). We noted the answers to conduct the laddering procedure for each attribute named by the respondents. To identify the functional and psychological consequences, we asked questions such as "Why exactly is this attribute important to you?" or "What positive consequences do you expect from this attribute?" Finally, to reach the terminal end state, we asked questions such as "Why exactly is this consequence important for you?" or "What value do you expect to derive from this consequence?" If the interviewees were unwilling to answer due to sensitive questions or an inability "*to articulate a 'ready' reason*" (Reynold & Gutman 1988, p. 15), we made use of specific laddering techniques, such as "negative laddering" and "third-person probe". To help the interviewees find reasons why an element is important to them, the negative laddering includes questions "*asking what would happen if the attribute or consequence was not delivered*" (Reynolds & Gutman 1988, p. 16). Using the third-person probe techniques means "*ask[ing] how others they know might feel in similar circumstances*" (Reynolds & Gutman 1988, p. 17).

Following Reynolds and Gutman (1988), we analysed the interview data in three steps. First, we conducted a content analysis "*to develop a set of summary codes that reflect everything that was mentioned*" (Reynolds & Gutman 1988, p. 18) and illustrate the elements of the means-end chain. Two scholars independently analysed the empirical data by carefully reading and reflecting the interview transcripts. To produce consistency, the two scholars compared their results regularly. Differences were discussed with a third senior scholar to seek reliable compromises. Then each code was related to one of the four levels of the means-end chain hierarchy. In an iterative process, similar codes on similar hierarchical levels were combined with the goal "*to achieve broad enough categories of meaning to get replications of more than one respondent saying one element leads to another*" (Reynolds & Gutman

1988, p. 18). After the first coding round, the scholars agreed on 59 elements. By combining replications (e.g., "self-confidence" and "special emphasis" were aggregated to "distinguish oneself"), the number of codes was reduced to 43 relevant elements. Second, the two scholars analysed the interviews for a second time to identify the linkages between the identified elements and define a set of "ladders" for each interview. In sum, we reached a number of more than 200 individual ladders. Third, the ladders of all the respondents were aggregated in an implication matrix. The rows and columns in the matrix contained the elements identified as a result of the content analysis. Accordingly, the implication matrix contains 43 x 43 rows and columns. In the fields of the matrix, we denoted how many interviewees showed a relation between two elements. Finally, we created the HVM to illustrate the hierarchical level of each element and mapped them with each other. For the mapping process, we chose a cut-off level of 6 relations because in our study this level brought about the most stable set of relations (Reynolds & Gutman 1988). The cut-off level determines the minimum number of interviewees illustrating the relations between the elements to be depicted in a HVM (Wagner 2007). With a cut-off level of 6, our HVM contains 28 elements.

In the second part of the interviews, we aimed to examine why the values prevail over the privacy risks. For this purpose, we used the semi-structured interview technique to collect data for in-depth investigation (Lacity & Janson 1994). The interviewees were first asked to describe their awareness of how their personal data were being used by the service provider. Afterwards, we asked them to describe the perceived privacy risks of wearable use. Then we asked why the perceived values outweighed the perceived risks and how this decision was made. As a final question, we asked the individuals whether there were any circumstances in which their opinion on the assessment of the privacy risks would change. Similarly to the first part of the interviews, the data from the semi-structured interviews were analysed through content analysis, which included a coding process (Bhattacherjee 2012). However, to analyse this data set, we followed a three-stage process of open, axial and selective coding (Bhattacherjee 2012). This analysis strategy helps researchers in "*classifying and categorising text data segments into a set of codes (concepts), categories (constructs) and relationships*" (Bhattacherjee 2012, p. 113) to create a chain of evidence and inferences. Each step of the coding process was conducted and discussed by different scholars to avoid subjective interpretation and enhance validity. First, two scholars analysed the interview transcripts line by line looking for privacy risks and salient factors influencing the decision-making process. Thereby, we identified codes such as financial disadvantage, unfair treatment, prior experiences, trust in the service provider, and personal interests. Second, the identified codes were assembled into the dimensions privacy risks (e.g., the code "financial disadvantage" was assigned to the dimension "privacy risks") and concepts from behavioural decision-making, i.e., heuristics and dispositional factors (e.g., the code "trust in service provider" was assigned to the dimension "dispositional factors"). Third, the core categories were built. After several iterations and discussions concerning the avoidance of overlaps, we subsumed the constructs under 6 meaningful core categories.

4 RESULTS

Nearly all the respondents use their wearables in similar contexts. They stated that they wear them with the aim of tracking their daily activities. They monitor their step rate on the way to work, during work or while taking a walk. A respondent additionally stated that he evaluates his pulse frequency during important meetings or presentations. The device is also used by nearly all the respondents during the night to monitor their sleep. Additionally, the majority of the respondents use the wearables during fitness activities. They track their speed, distance, pulse frequency and calorie consumption while jogging, hiking, bicycling or skiing. The respondents also noted wearing the devices in unusual situations. One respondent, for example, wears the device while visiting nightclubs because she is interested in the distance that she covers during the night. Another stated that he wears the wearable to evening events because he is interested in his step rate while dancing. Most of the interviewees also wear the bracelet or watch during their holidays with the purpose of comparing the gathered information with information gathered during their daily activities. The majority of the respondents did not name a

situation in which they are not willing to wear the device. On the contrary, the respondents explicitly emphasised their intent to wear wearables, regardless of the context, during all waking and sleeping hours.

Once we had observed the patterns of wearable use, in a first step, we proceeded to investigate the values that individuals perceive in the use of wearables. In a second step, we examined why these values prevail over the privacy risks.

4.1 Perceived Values

Analysing the laddering data, a total of 10 attributes of wearables were identified. For the next two hierarchical levels of the means-end chain, we identified 5 functional consequences and 6 psychological consequences. Finally, all of the elements were related to 8 values. For the sake of clarity, the cognitive structures captured in this study are shown in the HVM (Figure 1).

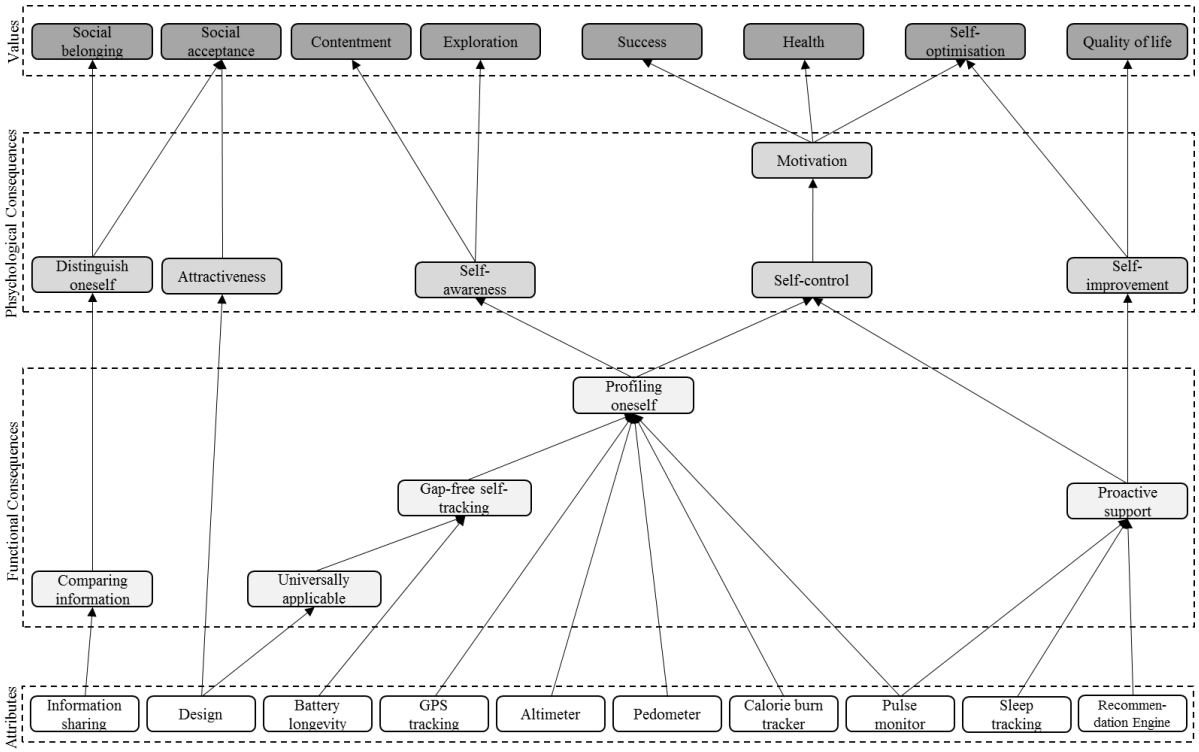

Figure 1. Hierarchical value map of wearable use

Three major means-end chains of cognitive associations can be derived from the HVM.

The first chain of cognitive association is based on the attribute "information sharing". It enables individuals to compare the gathered information ("comparing information"), for example, about their personal physical performance in the last week, with that of friends, family members or other people. This functional consequence provides individuals with the possibility of distinguishing themselves ("distinguishing oneself") from others, which in turn derives the values "social belonging" and "social acceptance".

The second chain of cognitive association is based on the "design" of the wearables, the "battery longevity" and the features that track individuals' activities and physical conditions, i.e., "GPS tracking", "altimeter", "pedometer", "calorie burn tracker" and "pulse monitor". Wearables with an adequate design suit every occasion and situation (e.g., workplace, fitness, visiting nightclubs) and can be universally applied ("universally applicable"). This functional consequence and the attribute "battery longevity" are deemed important for individuals because they enable permanent and gap-free documentation of individuals' activities ("gap-free self-tracking"). The consequence of "gap-free self-

tracking" and the features "GPS tracking", "altimeter", "pedometer", "calorie burn tracker" and "pulse monitor" are related to the desire for "profiling oneself" as accurately as possible. On the one hand, "profiling oneself" is valuable for individuals because it provides the ability to control oneself ("self-control") in terms of the achievement of goals and plans that have been developed before. This, in turn, motivates ("motivation") individuals to start, change or stop things with the aim of deriving the values "success", "health" and "self-optimisation". On the other hand, individuals profile themselves to generate "self-awareness". Being aware of all the minutiae of everyday life provides the values "contentment" and "exploration".

The third chain of cognitive association is based on the attributes "pulse monitor", "sleep tracking" and "recommendation engine". Based on these attributes, individuals receive "proactive support", helping improve sleeping behaviour (e.g., by a recommended bed-time or sleep duration) or increase training efficiency (e.g., by recommended heart rate zones). The "proactive support" is used for "self-control" and for "self-improvement", which is in turn associated with enhancing "quality of life". This means, for example, that individuals feel rested and more agile when following the recommendations.

When employing an overall perspective on the derived values, it becomes obvious that the respondents clearly benefit from wearables in various ways. First, they can satisfy their desire for a healthier lifestyle. As explained by one respondent, the information provided by the wearable allows him to control himself. This, in turn, motivates him to change his behavioural patterns and increase or decrease several daily activities with the aim of improved health and quality of life. "*I always want to live healthier because very often, I felt tired and sick. But in the past, I was really lazy, undisciplined and not motivated to change anything. Since my wife bought me the wristband, I check my profile everyday, control my 'activity level' and read the recommendations, e.g., about the required hours of sleep. Now, I really pay attention to go to bed early, to take a walk or to eat less. Honestly, I feel much better now*" (Male, 57, butcher).

Furthermore, most of the interviewees explained that they derive an opportunity for self-fulfilment through the use of wearables. This means that they have an ideal image of whom they want to be. The continuous use of the wearables helps them identify their own weaknesses and become the best possible version of themselves. "*It sounds strange, but I have a concrete idea about my life, my body and my physical fitness. I defined many goals in order to reach this ideal picture. I am really successful in reaching these goals since starting to use the wearable because it helps me to control my everyday activities and make concrete changes*" (Male, 29, consultant). Additionally, nearly all the interviewees stated that they satisfy their epistemic interest through wearable use. The respondents are very curious to explore whether and to what extent daily activities affect their physical performance (e.g., step rate) or specific bodily functions (e.g., heart rate). One interviewee explained that he checks regularly whether the effects of several activities meet his expectations. "*For me, it is really fascinating to see how many kilometres I have actually hiked and how high my pulse frequency was. Often I realise that I did not hike that far or that my body did not even reach its limits*" (Male, 31, engineer). Additionally, the devices enable the individuals to explore hitherto-unknown relationships between performed activities and personal well-being. "*If I am tired, I check how high my physical strain was and how my sleep rhythm was. Often I realise that I have worked out a lot and slept little. That calms me down because I do not need to conclude that I am sick but rather that I need to take a break*" (Male, 29, financial analyst). Finally, the respondents stated that social values, such as social acceptance, are positive side-effects of wearable use. The possibility of sharing the information, e.g., about their fitness activities, with other wearable users, provides a positive feeling of being part of a community and differentiating oneself from others. One interviewee stated: *"I do not look very athletic. Some of my friends do not believe that I go running twice a week. Since I got the wearable, I have been able to show them my trails and they believe me. However, this function is nice to have. In the proper sense, I use the wearable for myself – not for others*" (Male, 24, student).

4.2 Value-risk assessment of wearables

After observing the perceived values of wearable use, we investigated why these values prevail over the privacy risks.

When asked about their awareness of how personal data is being used by the service provider, almost all of the interviewees stated that they had no idea how firms use the data generated from wearables. This circumstance was justified by two key arguments. On the one hand, the respondents expressed a lack of interest in gathering further information and a lack of time to do so. On the other hand, they argued that it is almost impossible to process all the information given by the firms or other sources. "*I've already tried to get an overview of the risks associated with the use of wearables. As a layman, you have no chance to get into it. I really have to say that, although I have tried to obtain information, I have no idea*" (Male, 29, project manager).

After this first question, we explicitly asked the interviewees about the perceived risks. Notably, most of the respondents needed some time to respond. "*I really have not thought about that so far. Therefore, I cannot give an answer right now*" (Female, 53, pharmaceutical assistant). Some respondents stated a concern that service providers could share their data with third parties, such as insurance companies. In this case, the interviewees were worried about suffering financial disadvantages or unfair treatment. "*For me it would be very strange if insurance companies used my data. Probably, based on this data, the firm would be able to analyse all my activities. Based on this information, it would be possible to adapt the policies because of a lower fitness level*" (Male, 38, department head). Additionally, several respondents saw a risk of unauthorised publication of the gathered data. One interviewee stated: "*Perhaps the service provider will start to publish all our profiles on his homepage. I wouldn't like this because I don't want everyone to know my health status or fitness level*" (Male, 40, human resources manager).

However, almost all of the respondents noted that these perceived risks do not influence their decision-making process in any way. It appears that the interviewees, under normal circumstances, do not base their decisions on a rational value-risk assessment. The respondents' statements suggest that risks are ignored and use is primarily value-driven. It seems that these individuals avoid effortful cognitive tasks and reduce the amount of processed information.

This assumption is based on our observation that many of the interviewees ignored the likelihood of negative consequences and focused on specific and personally important values. "*If I want to benefit from the advantages of self-tracking, I really don't worry about my privacy. I just don't care about that*" (Female, 57, secretary). Accordingly, we suggest that these individuals assessed wearable use based on a prominent dimension (Slovic 1995).

Additionally, in line with Kehr et al. (2015), we found indications of the use of the affect heuristic. Most of the interviewees stated that they used a wearable because it fits their interests or lifestyle perfectly. "*I just enjoy the use because it fits my lifestyle perfectly and I just use it without thinking about any risks"* (Male, 25, student). This finding indicates that the respondents' use decisions are driven by personal interests and the enjoyment of wearable use, i.e., hedonic values.

Furthermore, we observed that the respondents' judgements are evoked by easy-to-recall associations based on the previous use of wearables. In more detail, several interviewees stated that they rely on positive experiences associated with the use of wearables. For example, one interviewee stated: "*For me, there is no reason to be concerned about privacy risks or disadvantages. Neither I nor my friends have had bad experiences with the use of wearables*" (Male, 24, student). This statement indicates the use of the availability heuristic, which asserts that "*people assess the (…) likely causes of an event by the degree to which instances or occurrences of that event are readily 'available' in memory"* (Bazerman & Moore, 2008, p. 7).

The respondents do not only base their judgements on experienced characteristics of the object under investigation. They tend to focus on previously formed stereotypes resulting from the use of other digital

devices. This strategy is known as the representativeness heuristic. It asserts that "*people tend to look for traits an individual may have that correspond with previously formed stereotypes*" (Bazerman & Moore, p. 8). Accordingly, the respondents emphasised basing their privacy assessments on prior experiences with smartphones or social networks: "*If I use my smartphone, I already give away many personal data. So far, nothing bad has happened by doing that, and I cannot imagine what bad things will happen to me. I do not see any reason why I should worry about that when using a wearable*" (Male, 23, student). Other interviewees indicated the use of the representativeness heuristic when generalising the value of their personal data. They attribute only a low level of relevance to their personal data in general and transfer this assessment to data gathered from wearables, which is why privacy risks are not mentioned: "*I don't think that the data gained from wearables are very interesting for companies. Honestly, if someone makes so much effort to collect the data, it is his own fault. There are certainly people whose data would be much more interesting than mine*" (Female, 28, social worker).

Finally, we observed the relevance of dispositional factors influencing individuals' decision-making. The key factor influencing the value-risk assessment was the provider of the wearable. If the provider was no longer one of the established brands (e.g., Fitbit or Jawbone) but rather a larger corporation, then the respondents stated that they would assess the risks in a more detailed way. The respondents thought primarily about insurance firms that could potentially offer the devices and retrieve the data. In this case, they would not be willing to wear the device all the time and in every situation. Due to a lack of trust, they do not want to share their private data, especially health data. The respondents assumed that insurance companies' primary goal is to maximise profit and not to offer added value to the consumer. When imagining an insurance company as the provider of wearables, the interviewees began to evaluate the values and risks in a more rational way. "*Of course, if my health insurance could use the data, I would be more cautious. For them, the data are relevant. If I had to worry that if I do not exercise enough then my premium increases, I would use the wearable more consciously and wear it only when I really need it*" (Male, 55, department head). Notably, we suggest that financial benefits do not have a positive influence on individuals' privacy-risk assessment. Most of the respondents stated explicitly the negative value of being paid, e.g., by insurance firms, for living a healthy lifestyle. One respondent describe it as an intervention in his daily life because it probably led to other-directed behaviour. "*Imagine, after having a busy but very successful day at work, you come home and instead of relaxing on the couch and being content with yourself, you have to go jogging to achieve the goals set by the insurance provider. Otherwise, you have to pay more the next month. This would be very stressful because you don't do it for yourself. You don't want to achieve your own goals. You are acting other-directed and solely focused on paying less*" (Male, 48, professor).

5 DISCUSSION AND CONCLUDING REMARKS

The widespread use of wearables for self-tracking activities despite potential privacy risks is an intriguing phenomenon. For firms, the data collected from individuals' wearable use are highly valuable for generating in-depth customer insights (Zhang et al. 2011). Accordingly, firms have an increasing desire for individuals' data (Chen et al. 2012). However, in research, there is scarce knowledge about the perceived values of wearables that drive individuals' use and the reasons why these values prevail over the privacy risks (Markus & Topi 2015; Min & Kim 2015; Newell & Marabelli 2015). Additionally, there has been a call in IS research to revisit the assumption of rational decision-making and examine the influence of intuitive processes on privacy-related decision-making (Dinev et al. 2015; Newell & Marabelli 2015). Against this background, our research set out to better understand why people use wearables despite privacy risks by investigating the perceived values of wearables that drive individuals' use and data disclosure and the reasons why these values prevail over privacy risks of wearable use. Based on the concept of the privacy calculus (Dinev et al. 2006) and concepts from behavioural decision-making (Kahneman 2003), we conducted in-depth interviews with 22 wearable users from Switzerland.

The contribution of our research is threefold. First, grounded on empirical data, we provide insights into the perceived values of wearables that drive individuals' use and data disclosure. Thereby, we contribute

to prior research in the IS field, which has primarily examined values of data disclosure in the contexts of e-commerce, social networks and LBS. We propose that individuals perceive the values "social belonging", "social acceptance", "contentment", "exploration", "success", "health", self-optimisation" and "quality of life". Interpreting the underlying meaning of the values shows that people pursue enjoyment, happiness and pleasure. Thus, it seems that they use wearables for activities that are intrinsically motivated and provide inherent satisfaction. Consequently, we assume that the values prevailing over privacy risks are distinctively hedonic in nature. This conclusion extends previous findings that emphasised the relevance of utilitarian values, such as financial rewards or personalisation, for sharing personal data with firms (Smith et al. 2011).

Second, our research contributes to the fundamental question of "*the overall awareness of individuals in terms of how their data are being used by businesses and whether people are happy with this*" (Newell & Marabelli 2015, p. 12). Based on in-depth interviews, we show the limited knowledge that individuals have about the consequences of using digital devices everywhere and anytime. Furthermore, our results suggest that many individuals do not want to invest time and cognitive effort to gather more information about how their personal data can be used by other stakeholders.

Third, our results provide a deeper understanding of the cognitive processes involved in privacy-related decision-making. Most research has described this process as a rational and effortful weighing of values and risks (e.g., Smith et al. 2011). Our results propose that individuals, under normal circumstances, do not base their decision on a rational value-risk assessment. Moreover, privacy risks appear to be ignored, and wearable use seems to be primarily value-driven. Few studies have investigated the impact of intuitive thinking, i.e., decision strategies, which reduce the amount of processed information and therefore the cognitive effort (e.g., Dinev et al. 2015; Kehr et al. 2015). Our study contributes to this research by emphasising the primary use of intuitive processes. Compared to Kehr et al. 2015, who focus on affect heuristics, our research suggests the use of further decision strategies. Based on our empirical study, we highlight the use of affective, availability and representativeness heuristics and the reliance on prominent dimensions.

Furthermore, our research can be used by practitioners to motivate their customers to use wearables and disclose personal data. The results give firms an idea of individuals' expectations regarding the perceived value of wearable use. Based on our results, they can configure their services to provide customers with the desired value. Additionally, our study provides firms with an in-depth understanding of the cognitive processes involved in consumers' decision-making. Using these findings, firms can adapt their communication or marketing strategies to motivate their customers to make use of heuristics or rely on prominent dimensions so that privacy risks do not influence their decision-making process.

Despite the careful design of our research approach, the findings are subject to some limitations that should be addressed by further research. First, the empirical data from the in-depth interviews do not allow us to make assumptions about the generalisability of our findings. Our findings refer to the use of bracelets and watches in the specific context of self-tracking. Researchers should be careful when transferring the results to other sorts of wearables or other digital devices in other use contexts. Furthermore, our sample only included actual wearable users and neglected non-adopters and discontinuers. Thus, our research solely discloses factors influencing the continued use of wearables. However, privacy risks may be regarded as more relevant by individuals who decided not to adopt wearables in the first place or who stopped using them. We encourage further research to investigate the generalisability of the findings by considering other technologies, use contexts and adoption phases. Second, our research focuses on individuals from Switzerland. A closer look at potential cultural differences may prove fruitful. Further research should focus on investigating the influence of cultural differences on the cognitive processes involved in privacy-related decision-making. Third, we focus on wearables offered by firms such as Fitbit, Jawbone, Samsung and Apple. The results illustrate the influence of customers' brand perception. We encourage scholars to investigate the relevant contextual factors of a firm that influence individuals' cognitive processes.

References

Acquisti, A., John, L. and Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. Journal of Marketing Research, 49 (2), 160-174.

Anderson, C.L. and 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.

Bazerman, M.H. and Moore, D.A. (2008). Judgment in managerial decision making. 7th ed. John Wiley & Sons, New Jersey.

Bech-Larsen, T. and Nielsen, N.A. (1999). A comparison of five elicitation techniques for elicitation of attributes of low involvement products. Journal of Economic Psychology, 20, 315-341.

Belanger, F. and Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35 (4), 1017-1041.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices. Florida.

Buchwald, A., Letner, A., Urbach, N. and von Entress-Fuerstenbeck, M. (2015). Towards explaining the use of self-tracking devices: Conceptual development of a continuance and discontinuance model. In proceedings of the Thirty Six International Conference on Information Systems (ICIS 2015), p. 1, Association for Information Systems, USA, Forth Worth.

Chen, H., Chiang, R.H.L. and Storey, V.C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36 (4), 1165-1188.

Constantiou, I.D., Lehrer, C. and Hess, T. (2014). Changing information retrieval behaviours: An empirical investigation of users' cognitive processes in the choice of location-based services. European Journal of Information Systems, 23, 513-528.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and 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. and Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. Behaviour & Information Technology, 23 (6), 413-422.

Dinev, T., McConnell, A.R. and Smith, H.J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. Information Systems Research, 26 (4), 639-655.

Fitbit (2014). Fitbit official site for activity trackers more. https://www.fitbit.com/uk. Accessed 3 January 2016.

Gao, Y., Li, H. and Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. Industrial Management & Data Systems, 115 (9), 1704-1723.

Gutman, J. (1982). A means-end chain model based on consumer categorization processes. Journal of Marketing, 46 (2), 60-72.

IDC (2015). Worldwide wearables market forecast to reach 45.7 million units shipped in 2015 and 126.1 Million Units in 2019. http://www.idc.com/getdoc.jsp?containerId=prUS25519615. Accessed 3 January 2016.

Jawbone (2014). Jawbone UP: The path to better starts here. https://jawbone.com/. Accessed 3 January 2016.

Jung, Y. (2014). What a smartphone is to me: Understanding user values in using smartphones. Information Systems Journal, 24, 299-321.

Jung, Y. and Kang, H. (2010). User goals in social virtual worlds: A means-end chain approach. Computers in Human Bevaviour, 26, 218-225.

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American Economic Review, 93 (5), 1449-1475.

Kehr, F., Kowatsch, T., Wentzel, D. and Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal, 25, 607-635.

Kehr, F., Wenztel, D. and Mayer, P. (2013). Rethinking the privacy calculus: On the role of dispositional factors and affect. Proceedings of Thirty Fifth International Conference on Information Systems (ICIS 2013), p. 1, Association for Information Systems, Italy, Milan.

Lacity, M.C. and Janson, M.A. (1994). Understanding qualitative data: A framework of text analysis methods. Journal of Management Information Systems, 11 (2), 137-155.

Li, H. and Wu, J. (2014). The war in the wearable device market: The analysis from economic perspective. In Proceeding of the 19th Pacific Asia Conference on Information Systems (PACIS 2014), p. 1, Association for Information Systems, China, Chengdu.

Maddox, T. (2016). The dark side of wearables: How they're secretly jeopardizing your security and privacy. http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/. Accessed 3 Janurary 2016.

Markus, M.L. (2015). New games, new rules, new scoreboards: The potential consequences of big data. Journal of Information Technology, 30, 58-59.

Markus, M.L. and Topi, H. (2015). Big Data, big decisions for science, society, and business. https://www.bentley.edu/files/2015/10/08/BigDataWorkshopFinalReport.pdf. Accessed 3 January 2016.

McAfee, A. and Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review, October.

Motti, V.G. and Caine, K. (2015). Users' privacy concerns about wearables. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8976, 231-244.

Mills, D. (2015). Consumers like wearable technology but worry about data security. http://www.healthline.com/health-news/consumers-concerned-about-privacy-personal-health-data-wearables-mobile-apps-072815#1. Accessed 3 January 2016.

Min, J. and Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. Journal of the Association for Information Science and Technology, 66 (4), 839-857.

Newell, S. and Marabelli, M. (2014). The crowd and sensors era: Opportunities and challenges for individuals, organizations, society, and researchers. Proceedings of Thirty Fifth International Conference on Information Systems (ICIS 2014), p. 1, Association for Information Systems, New Zealand, Auckland.

Newell, S. and Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. Journal of Strategic Information Systems, 24 (1), 3-14.

Olson, J.C. and Reynolds, T.J. (2001). The means-end approach to understanding consumer decision making. In: Reynolds, T.J., Olson, J.C. (Eds.). Understanding consumer decision making: The means-end approach to marketing and advertising strategy. Lawrence Erlbaum, Associates, Mahwah.

Reynolds, T.J., Gengler, C.E. and Howard, D.J. (1995). A means-end analysis of brand persuasion through advertising. International Journal of Research in Marketing, 12, 257-266.

Reynolds, T.J. and Gutman, J. (1988). Laddering theory, method, analysis, and interpretation. Journal of Advertising Research – February/March, 11-24.

Reynolds, T.J. and Olson, J.C. (2001). Understanding consumer decision making: The means-end approach to marketing and advertising strategy. Erlbaum, Mahwah.

Rogers, E. (1995). Diffusion of innovations. Free Press, New York.

Schäfer, T. (2013). Exploring carsharing usage motives: A hierarchical means-end chain analysis. Transportation Research Part A, 47, 69-77.

Setia, P., Venkatesh, V. and Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. MIS Quarterly, 37 (2), 565-590.

Sjöklint, M., Constantiou, I. and Trier, M. (2015). The complexities of self-tracking - an inquiry into user reactions and goal attainment. In Proceedings of the European Conference on Information Systems, p. 1, European Research Centre for Information Systems, Germany, Münster.

Slovic, P. (1995). The construction of preferences. American Psychologist, 50 (5), 364-371.

Smith, H.J., Dinev, T. and Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35 (4), 989-1015.

Statista (2016a). Welche der folgenden medien nutzen sie an einem normalen wochentag (montag bis freitag), egal wie häufig? http://de.statista.com/statistik/daten/studie/420271/umfrage/regelmaessige-nutzung-ausgewaehlter-medien-in-der-dach-region/. Accessed 3 January 2016.

Statista (2016b). Wie wahrscheinlich ist es, dass sie sich in den nächsten 12 monaten eine smartwatch kaufen? http://de.statista.com/statistik/daten/studie/422088/umfrage/marktpotenzial-der-smartwatch-in-der-schweiz-nach-alter-geschlecht-und-region/. Accessed 3 January 2016.

Sun, Y., Wanga, N., Shen X. and Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. Computers in Human Behavior, 52, 278-292.

Sutanto, J., Palme, E., Tan, C.H. and Phang, C.W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. MIS Quarterly, 37 (4), 114-1164.

Trickler, C. (2013). An overview of self-monitoring systems. In Proceedings of the Nineteenth Annual 16th Southern Association for Information Systems Conference (SAIS 2013), p. 197, Southern Association for Information Systems, USA, Georgia.

Wagner, T. (2007). Shopping motivation revised: A means-end chain analytical perspective. International Journal of Retail & Distribution Management, 35 (7), 569-582.

Wilson, D.W. and Valacich, J.S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. In Proceedings of Thirty Third International Conference on Information Systems (ICIS 2012), p. 1, Association for Information Systems USA, Orlando.

Xu, H., Teo, H.H, Tan, B.C. and Agarwal, R. (2009). The role of push–pull technology in privacy calculus: The case of location-based services. Journal of Management Information Systems, 26 (3), 135-173.

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. Journal of the Associations for Information Systems, 12 (12), 798-824.

Zhang, D., Guo, B. and Yu, Z. (2011). The emergence of social and community intelligence. Computer 44 (7), 21-28.

Zhao, L., Lu, Y. and Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. International Journal of Electronic Commerce, 16 (4), 53-90.