Research Center
Finance & Information Management

Fraunhofer
FIT

Project Group
Business & Information
Systems Engineering

Discussion Paper

Will I or will I not? Explaining the willingness to disclose personal self-tracking data to a health insurance company

by

Matthias von Entreß-Fürsteneck, Arne Buchwald[1], Nils Urbach

September 2018

To be presented at: 52nd Hawaii International Conference on System Sciences (HICSS), January 2019

[1] EBS Business School

WI-820

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: Wittelsbacherring 10, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

Will I or will I not? Explaining the willingness to disclose personal self-tracking data to a health insurance company

Matthias von Entreß-Fürsteneck
University of Bayreuth
Project Group Business & Information Systems
Engineering of Fraunhofer FIT
matthias.entress-fuersteneck@uni-bayreuth.de

Arne Buchwald
EBS Business School
Center for Digital Transformation at the Strascheg Institute for Innovation, Transformation, & Entrepreneurship
arne.buchwald@ebs.edu

Nils Urbach
University of Bayreuth
Project Group Business & Information Systems
Engineering of Fraunhofer FIT
nils.urbach@uni-bayreuth.de

Abstract

Users of digital self-tracking devices increasingly benefit from multiple services related to their self-tracking data. Vice versa, new digital as well as "offline" service providers, such as health insurance companies, depend on the users' willingness to disclose personal data to be able to offer new services. Whereas previous research mostly investigated the willingness to disclose data in the context of social media, e-commerce and smartphone apps, the aim of our research is to analyze the influence of the privacy calculus of personal risks and benefits on the willingness to disclose highly personal and confidential self-tracking data to health insurance companies. To do so, we develop a conceptual model based on the privacy calculus concept and validate it with a sample of 103 respondents in a scenario-based experiment using structural equation modeling. Our results reveal that privacy risks always have a negative impact on the willingness to disclose personal data, while positive effects of privacy benefits are partly depending on the data sensitivity.

1. Introduction

With rising demand for personal services, e.g. in the areas of healthcare, education, and entertainment [3], the processing of personal data becomes more and more a critical factor of business success. While digital service providers, such as social media and e-commerce platforms, have typically already heavily invested in the personalization of their services to customers, "offline" services, such as physicians or health insurance companies, are mostly still in their infancy in terms of providing personalized services. For these "offline" services, personal self-tracking data is one type of data that could lead to service improvements.

In general, self-tracking (also known as life-logging, quantified-self, personal analytics, and personal informatics) is the current trend to collect data about specific features of life through mobile and wearable digital devices [37]. Self-tracking devices are placed in the category of wearable electronics and/or multi-sensor platforms in the field of the Internet of Things [53]. These devices can take the shape of smartwatches, wristband sensors, wearable sensor patches, artificial reality-augmented glasses, brain computer interfaces, or wearable body metric textiles [53]. They enable the individual to capture data about daily activities, exercises, vital parameters, disease symptoms, or nutrition, among others [20]. Due to the development of new technologies and decreasing sensor sizes, self-tracking becomes not only increasingly convenient [20, 38], but also enables users to capture more and more aspects of their life. Major players in the consumer electronic market, such as Apple, Google, as well as specialized producers like fitbit, launched their own self-tracking devices (e.g., Apple Watch, Android Wear, Fitbit Charge) and start to build up software and hardware ecosystems around their devices with open APIs, enabling new players (e.g. runtastic, nike+), but also typical "offline" service providers, such as physicians and health insurance companies, to offer services based on the collected data. Considering the expectation that the shipment of solely wearable self-tracking devices will grow from 102 million units in 2016 to more than 224 million units in 2020 [30], we expect the service ecosystem around such devices to grow as well. However, without the customers' agreement to share their personal self-tracking data, the service providers cannot (fully) deliver their services. This fact becomes even more critical given the launch of the General Data Protection Regulation (GDPR) of the European Union in May 2018. Thus, the willingness of the customer to disclose personal data gathered through a self-tracking device is essential for the success of the service provider.

The privacy research stream has an ongoing history of studies, which are dedicated to explaining the willingness to disclose personal data. Research regarding information disclosure in the personal context primarily analyzes sharing information within the domain of social media or to some extent within the e-commerce and smartphone app area [7, 8, 15, 21, 28]. There is evidence for users unconsciously accepting terms and conditions about their privacy disclosure [4, 32]. Thus, users are not always aware of the extent of private information disclosure [52]. However, we propose that there is a difference regarding to what extent users are aware and sensitive of sharing personal data in the case of self-tracking, since the “commodity” they provide allows service providers to derive direct conclusions to one’s physical or health condition and is thus more confidential. To our knowledge, little research has been carried out in the area of full awareness about information disclosure, where people are completely informed about the type of data, anonymity level, or purpose of information. Because of the higher risks and the valuable benefits involved in comparison to other personal information, such as shopping behavior or social media usage, it is likely that peoples’ disclosing behavior differs from other personal information contexts. We therefore aim to analyze the influence of the calculus of personal risks and benefits (privacy calculus) on the willingness to disclose highly personal self-tracking data. Further, we will focus on health insurance companies as the third-party exchange partner since this type of “offline” service provider already started to test the usage of self-tracking devices [e.g. 49], thus providing an interesting near-future scenario:

RQ: How does the calculus of personal risks and benefits influence the willingness of an individual to disclose highly personal and confidential self-tracking data to a health insurance company?

To do so, we develop and empirically validate a research model that is based on the comprehensive APCO Macro Model (Antecedents, Privacy Concerns, Outcomes) of Smith et al. [50] but then focus on the link between the privacy calculus and the behavioral reactions. In addition, we contribute to the specific context of self-tracking by adapting the characteristics of the privacy calculus accordingly and also consider the sensitivity of the self-tracking data, the perceived activity status and the perceived health status of the users.

We organize this article as follows: Section 2 outlines the theoretical foundations of our study by introducing established and related theories in the field of privacy and information disclosure. In Section 3, we describe the research context as well as the development of our constructs and hypotheses which we finally synthesize into a conceptual model. In Section 4, we describe the research method, followed by the presentation of the analysis and results in Section 5. Section 6 is dedicated to the discussion of our results, while we conclude with the limitations, the future research process and our main contributions in Section 7.

2. Theoretical foundations

With the establishment of laws to protect private data [50], privacy was considered to be a human right and people became able to decide to what extent information about themselves should be disclosed. Self-disclosure describes the action of uncovering personal information, such as locations or activities [46]. There, according to communication privacy management theory (CPM), people face a conflict between privacy and disclosure while determining whether to reveal private data and information or not [44]. Even though people report high concerns regarding their privacy, they voluntarily submit personal information at numerous events. This observation is known as the privacy paradox [40] and is rooted in the fact that people view privacy less as a right but rather as a commodity [5, 12, 18, 50]. Within this view, it is possible to assign privacy an economic value, which is the basis for cost-benefit analysis and trade-offs [5, 12, 50]. Consumers, which are asked for providing private information to receive a product or service, perform cost-benefit analyses to evaluate the consequences they would encounter in return for the disclosed information, and they respond accordingly. Such consequences are the perceived benefits as well as risks. Exemplary benefits are a better service through personalization or financial rewards. However, any information exchange entails considerable uncertainty or is subject to opportunistic behaviors of the receiver. For instance, the receiver of the private data may utilize them for different purposes than declared. Therefore, the following consequences of the information disclosure may be too complex to anticipate beforehand and contain a personal risk. Results by Keith et al. [31] suggest these perceived risks to be more important for explaining information disclosure compared to perceived benefits. This process of comparing benefits and risks is understood as privacy calculus, with drivers and inhibitors effecting the decision process at the same time regarding whether to disclose information or not [11, 13]. Since concepts, such as benefits and risks from information disclosure, differ from situation to situation, it is vital to analyze information disclosure context-specific in order to understand the person's information sharing behavior [11, 50]. In this respect, the disclosure of self-tracking associated data is of medical and behavioral nature, which can be considered one of the most private data possible.

3. Conceptual development

After having outlined previous research in the privacy area, we will now proceed to explain the research context as well as the different constructs and hypotheses we will draw upon for explaining an individual's willingness to disclose personal self-tracking data to a health insurance company.

3.1 Research context

As indicated earlier and described by Smith et al. [50], it is "impossible to develop a one size-fits-all conceptualization of general privacy" (p. 1002). Hence, we subsequently describe the specific research context of private information disclosure we consider in our model. We draw upon the privacy calculus concept [11, 13] which in turn is grounded in the calculus of behavior theory [10, 33]. On this basis, we focus on the context of individual usage of self-tracking devices (such as smartwatches, wristbands, patches, clip-on devices, wireless weight scales or blood pressure monitors) [36, 53] through which personal data is collected, processed, and analyzed.

Further, depending on the service, self-tracking data can be shared in different ways referring to the aggregation level, e.g. the variety, the volume and the velocity. Within our study, we framed the context for participants in our scenario-based experiment that the personal data could be assigned to themselves, is shared instantly without any aggregation and includes all collected data.

Concerning the third-party exchange partners (usually service providers), we expect significant different results for our research model depending on which exchange partner is considered. Nowadays, users of self-tracking devices can share data with service providers which enable them to connect to their social group, e.g. family and friends, social media or special online platforms such as fitness-tracking platforms (e.g. runtastic, nike+). Prospectively, it can be assumed that soon, it will be possible to share data with a larger group of exchange partners which offer common services such as physicians, health insurance companies, pharmacies, research institutes or sport and fitness clubs. We assume that users will evaluate the risks and benefits for each service provider separately and calculate the privacy calculus accordingly. Since health insurance companies already started to test the usage of self-tracking devices within their services [e.g. 49], we see this service provider as the most interesting concerning our research subject. Hence, within our research paper, we set the context to this type of third-party exchange partner.

Finally, previous research suggests that the type of data matters in individuals' data sharing decisions, such as financial versus purchase preferences [39], demographic versus lifestyle [45] and the sensitivity of health information records [1] which is why we propose that the type of data is also a relevant factor in the self-tracking context. Within our research study, we refer to the type of data as data sensitivity and define it as one's consideration of the type of personal self-tracking data within the privacy calculus. It addresses that self-tracking users do not only share information, such as contact information or usage patterns (e.g. website usage), but also sensitive personal data that is directly linked to their activity or health condition. Yet, even though activity and health data belong to the group of sensitive data types, we argue that there are still increments present. We therefore distinguish between weak sensitive personal data, such as activity data (e.g. walking distance, steps, calories burned or the sleep rhythm), and strong sensitive personal data, such as vital and body data (e.g. heart rate, blood pressure, stress level, weight, body fat, muscle mass or the body mass index). While weak sensitive personal data allows to derive general assumptions about one's well-being or fitness, strong sensitive personal data, in contrast, enables to draw conclusions about the health status or possible diseases and is thus more sensitive. We assume that users of self-tracking devices take this fact into account when they calculate the risks and benefits of information disclosure. Hence, we set two different research contexts for the participants in our scenario-based experiment, distinguishing between weak and strong sensitive data, to analyze the influence of the calculus of personal risks and benefits on the willingness to disclose personal self-tracking data to a health insurance company in each context.

3.2 Constructs and hypotheses

We investigate the relationships between characteristics of the privacy calculus and the behavioral reactions of self-tracking users instead of intentions because past research indicates that behaviors do not match actual intentions due to the interference of the privacy paradox [40, 50]. Behavioral reactions can become visible as one's willingness to disclose information [50]. We therefore focus on the **willingness to disclose personal self-tracking data** (WtD) as the dependent variable and define it as the will of a self-tracking user to disclose personal self-tracking data to a health insurance company. Our independent variables encompass the characteristics of the privacy calculus, i.e., privacy risks and privacy benefits proposed by Smith et al. [50]. As we aim at explaining the effects of different privacy benefits, we further distinguish between multiple types of privacy benefits, namely financial rewards [e.g. 25, 29, 58], personalization benefits [6, 56], and social adjustment benefits [35]. With our focus on the formal interaction between self-tracking users and health insurance companies, we include financial rewards and personalization benefits, which we adapt to service improvement benefits to fit to the context of self-tracking into our model. We further omit social adjustment benefits, since this construct refers to the fulfillment of the need for affiliation [35], thus on informal relations between users which are not reflected in our investigated type of interaction.

Privacy risks (PR) are defined as "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" [50]. The manifestation of the risk is the result of a calculation of the likelihood of negative consequences and the perceived severity of those consequences [43]. Several studies verified the negative effect of perceived risk on intentions or willingness to disclose information [e.g. 14, 42, 59]. Following them, we assume, that privacy risks are also a key negative determinant of the willingness to disclose information in the self-tracking context, since users share highly personal activity and health data. In the case of a loss of control over these personal data, the severity of consequences can be serious and influences one's social and financial status sustainably. For example, a health insurance company could increase fees of a customer if it gets access to self-tracking data that is not in favor of its user. Hence, we posit:

H1: Privacy risks have a negative effect on the willingness to disclose personal self-tracking data to a health insurance company.

Service improvement benefits (SIB) through service personalization refer to Chellappa and Sin [6] who define 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). Previous research showed that personalization benefits support the customer's willingness to disclose their personal and preference information [56].

While personalization is rooted in the context of commerce, we adapt it to the context of self-tracking by redefining it as the ability to tailor common services to the needs of self-tracking users based upon their self-tracking data and rename the variable to service improvement benefits. We argue, when self-tracking data is shared with certain service providers, they are able to customize their services to the advantage of the user. For example, customers who share their data with a health insurance company could in return receive individual services that address certain issues analyzed from the self-tracking data such as suggestions for sport or fitness activities, faster clearance of special treatments or suggestion for physician consultations. Hence, we posit:

H2: Service improvement benefits have a positive effect on the willingness to disclose personal self-tracking data to a health insurance company.

Financial rewards (FR) can have various forms, such as discounts, vouchers or free gifts [29]. Several studies confirmed that financial rewards have a positive impact on the motivation to disclose information [e.g. 25, 29, 58]. We assume that in the context of self-tracking, financial rewards are also a relevant benefit. For example, financial rewards could be granted by health insurance companies to customers for providing their self-tracking data to demonstrate health-promoting behavior. We therefore also include the variable in our model, define it as the granting of monetary rewards, discounts, vouchers or free gifts to self-tracking users based upon their self-tracking data, and posit:

H3: Financial rewards have a positive effect on the willingness to disclose personal self-tracking data to a health insurance company.

In addition to the adapted constructs of the privacy calculus, we incorporate two moderating variables in our model, which relate to the perceived activity status and the perceived health status of the users. Previous research has shown that patients with a perceived poor health status are more sensitive about their health data than others [2, 54]. We adapt this construct to the context of self-tracking and define the **perceived activity status (PAS) and perceived health status (PHS)** as one's consideration of the actual status of the activity and health condition within the privacy calculus, respectively. We argue that self-tracking users who have a decent activity level or are in general healthy and thus do not have critical data, do not expect negative consequences when disclosing their self-tracking activity or health data. In contrast, users who are less active or healthy and therefore have by tendency more critical data, assume higher risks of negative consequences by third parties and thus take this fact into consideration when they evaluate the risks of information disclosure. Hence, we posit:

H4a/b: The perceived activity status / health status has a negative moderating effect on the relation between privacy risks and the willingness to disclose personal self-tracking data to a health insurance company.

4. Research method

4.1 Design and operationalization

To realize our goal to compare two contexts in terms of data sensitivity, we chose an experimental design and collected data using an online-based tool. We build on the factorial survey approach [17] which allows us to create and compare two hypothetical settings in which we ask the participants at first to evaluate their privacy calculus and the willingness to share personal self-tracking data to a health insurance company under the assumption that weak sensitive data (activity data such as steps or distance walked, sleep duration or quality or general activity level) would be shared. In a second setting, we asked the same participants to evaluate their privacy calculus and the willingness to share personal self-tracking data to a health insurance company under the assumption that strong sensitive data (health data such as heart rate or rhythm, blood pressure or weight) would be shared. We decided not to refer the context to a specific real-world health insurance company or established benefits program but to enable the participants in our experiment to consider their privacy calculus and willingness to disclose to their own health insurance company to increase the validity of their responses.

For the operationalization of our measurement model, we build on established and validated measures wherever possible as well as self-developed items. We further adapted all items to the self-tracking context as well as to the specific context of weak and strong data sensitivity in the respective research model (Table 1). Each of the item statements was measured with a seven-point Likert scale [34] between (1=I do not at all agree; 7=I do fully agree). All constructs are measured reflectively. Ultimately, we analyzed our sample data using structural equation modeling [51, 55].

Table 1: Construct operationalization

Construct	Item operationalization for the weak / strong sensitive data context	Adapted from
Willingness to disclose personal self-tracking data	I would be willing to share my personal self-tracking activity-data / health-data with my health insurance company.	Self-developed based on [6, 14]
	I would be open to an analysis of my personal self-tracking activity data / health-data by my health insurance company.	
	I would allow my health insurance company to save my personal self-tracking activity-data / health-data.	
Privacy risks	It would be risky to give my personal self-tracking activity-data / health-data to my health insurance company.	Adapted from [57]
	There would be high potential for privacy loss associated with giving my personal self-tracking activity-data / health-data my health insurance company.	
	My personal self-tracking activity-data / health-data could be inappropriately used by my health insurance company.	
	Providing my health insurance company with my personal self-tracking activity-data / health-data would involve many unexpected problems.	
Service improvement benefits	I would value if my health insurance company improves the service reliability and accuracy through the usage of my personal self-tracking activity-data / health-data.	Self-developed based on [9, 41]
	I would value if my health insurance company improves the response time through the usage of my personal self-tracking activity-data / health-data.	
	I would value if my health insurance company improves the individualized attention towards me through the usage of my personal self-tracking activity-data / health-data.	
	I would value if my health insurance company improves the service flexibility and personalization through the usage of my personal self-tracking activity-data / health-data.	
Financial rewards	I would value if my health insurance company offers me financial rewards in exchange for my personal self-tracking activity-data / health-data.	Adapted from [29]
	I would value if my health insurance company offers me financial discounts in exchange for my personal self-tracking activity-data / health-data.	
	I would value if my health insurance	

	company offers me vouchers or gifts in exchange for my personal self-tracking activity-data / health-data.	
Perceived activity status / health status	I perceive my physical activity / health condition to be positive.	Self-devel-oped based on [2]
	I perceive my physical activity / health condition to be above average.	
	I perceive my physical activity / health condition to represent a good constitution.	
	I perceive my physical activity / health condition would be positively evaluated by others.	

4.2 Data collection

We collected data by distributing our research instrument to active as well as non-active users of self-tracking devices, since the hypothetical experimental setting allows anyone to participate. To gather our data from respondents, we circulated the invitation message to participate in our experiment in online social networks (e.g. Facebook wall postings and Facebook groups), online business networks (e.g., Xing), the e-learning system of the authors' university, among others. We decided in favor of openly circulating our invitation to allow for a snowball effect. As we circulated the invitation for participation anonymously, we cannot determine a response rate.

5. Analysis and results

Overall, we received 125 responses during May and June 2018. After excluding incomplete (22) responses, we analyzed the remaining 103 responses. Out of these remaining responses 52% are male and have an average age of 28. Furthermore, 70% have a university degree and 96% are European citizens. 61% do currently own and use a self-tracking device. There are no missing values for the key variables in our model since the answers were mandatory.

For the analysis of our measurement and structural model, we used SmartPLS 3.2. [48]. We chose PLS-SEM as an established approach in the IS research discipline, also due to our relatively small sample size [19, 22, 23, 47]. We checked the measurement model of each context for internal consistency, convergent validity, and discriminant validity. We analyzed Cronbach's Alpha (CA) and the Composite Reliability (CR) to test the internal consistency of our measurement instrument. All values exceed the threshold of 0.8, showing a high degree of internal consistency. The Average Variance Extracted (AVE) is greater than the critical threshold of 0.5 for all constructs (Table 2 and 3). Furthermore, we analyzed the indicator reliability. The outer loadings of all measurement items exceed the threshold of 0.708 [24].

Table 2. Assessment of the measurement model for weak data sensitivity (activity data)

	CA	CR	AVE
PAS	0.862	0.906	0.706
FR	0.891	0.932	0.821
PR	0.855	0.902	0.679
SIB	0.922	0.945	0.810
WtD	0.938	0.961	0.890

Table 3. Assessment of the measurement model for strong data sensitivity (health data)

	CA	CR	AVE
PHS	0.918	0.939	0.793
FR	0.926	0.953	0.871
PR	0.878	0.916	0.732
SIB	0.948	0.963	0.866
WtD	0.920	0.950	0.863

To assess discriminant validity, we applied the Fornell-Larcker criterion [16]. The square root of each construct's AVE is greater than its highest correlation with any other construct (Table 4 and 5). In addition to the traditional discriminant validity check, we applied the Heterotrait-monotrait (HTMT) approach [26]. All values are below 0.85 which is why we conclude that discriminant validity has been established [22].

Table 4. Fornell-Larcker criterion of the measurement model for weak data sensitivity

	PAS	FR	PR	SIB	WtD
PAS	0.840				
FR	0.147	0.906			
PR	-0.238	-0.532	0.835		
SIB	0.093	0.654	-0.494	0.900	
WtD	0.228	0.690	-0.681	0.646	0.944

Table 5. Fornell-Larcker criterion of the measurement model for strong data sensitivity

	PHS	FR	PR	SIB	WtD
PHS	0.890				
FR	0.139	0.934			
PR	-0.236	-0.456	0.856		
SIB	0.119	0.737	-0.367	0.931	
WtD	0.213	0.663	-0.654	0.634	0.929

Further, we assessed the measurement invariance between the two models following the MICOM procedure [27]. We consider configural invariance to be present after a qualitative assessment. In addition, compositional invariance and equality of composite mean values and variances was positively tested using the permutation algorithm in SmartPLS with 5,000 subsamples.

Finally, we assessed the structural model of each scenario with partial least squares (PLS) structural equation modeling (SEM) (path weighting scheme, stop criterion 10^{-7}). To assess the significance levels, we applied bootstrapping with 5,000 sub-samples (no sign changes). The results for each model are provided in Table 6, encompassing standardized path coefficients, significance levels, and R^2 value. Relating to the weak data sensitivity context (activity data), the direct influence of privacy risks (β=-0.339***) and financial rewards (β=0.334**) could be confirmed, while in the strong data sensitivity context (health data) privacy risks (β=-0.424***), service improvement benefits (β=0.276***) and financial rewards (β=0.254**) have a significant impact. In contrast, we neither found a significant moderating effect of perceived activity status nor perceived health status on the relationship between privacy risks and the willingness to disclose personal self-tracking data to a health insurance company.

Table 6. Final results

Hypothesis	**Weak data sensitivity context (activity data)**		**Strong data sensitivity context (health data)**	
	Beta coefficients	**P-values**	**Beta coefficients**	**P-values**
H1: Privacy risks → Willingness to disclose personal self-tracking data	**-0.339**	**0.000*** **	**-0.424**	**0.000*** **
H2: Service improvement benefits → Willingness to disclose personal self-tracking data	0.230	0.078ns	**0.276**	**0.001*** **
H3: Financial rewards → Willingness to disclose personal self-tracking data	**0.334**	**0.010** **	**0.254**	**0.009** **
H4a: Moderating effect of perceived activity status between privacy risks and the willingness to disclose personal self-tracking data	-0.148	0.279ns	-	-
H4b: Moderating effect of perceived health status between privacy risks and the willingness to disclose personal self-tracking data	-	-	0.104	0.339ns
R²	0.666		0.646	
* significant at p ≤ .050; ** significant at p ≤ .010; *** significant at p ≤ .001; ns: not significant				

6. Discussion

In general, while previous studies focused on the often unconscious willingness to disclose data within the domain of social media, e-commerce and smartphone apps, our findings show the applicability of the privacy calculus part of the APCO Macro Model of Smith et al. [50] to the underexplored context of disclosing consciously highly personal and confidential self-tracking data. Concerning our adaptations of the model to the new context, the consideration of the perceived activity status and the perceived health status show no influence on the proposed relations, while the consideration of two different contexts concerning the data sensitivity yield different results. Subsequently, we will discuss the results in more detail and derive practical implications.

For the negative side of the privacy calculus – privacy risks –, the results are in line with previous research on privacy risks in the context of e-ommerce [e.g. 14, 42, 59], which showed a negative relationship between perceived privacy risks and the willingness to disclose. While users are already concerned about data privacy of “ordinary” data, such as contact or billing information, they are consequently also concerned about the privacy of highly sensitive self-tracking data. In this regard, the distinction between weak and strong sensitive data types seem to be negligible for users. For health insurance companies, these results show that perceived privacy risks of their customers have to be considered, if they want them to share their personal activity or health data. This could, for example, be accomplished by measures, such as high transparency about the data usage or an external certification of the privacy standards.

For the positive side of the privacy calculus, our results reveal that in both contexts financial rewards are a strong positive indicator for the willingness to disclose personal self-tracking data. The results re-confirm former research projects in different contexts [e.g. 25, 29, 58] and thus show that this is also true for activity and health data in the self-tracking domain. Health insurance companies could exploit this positive relationship, for example by controlling the customers effort to improve his or her activity or health condition through the disclosed self-tracking data, and offer financial rewards accordingly.

Further, considering the influence of service improvement benefits on the willingness to disclose personal data, the results vary between the two different data sensitivity contexts. Within the context of strong data sensitivity, service improvement benefits have a significant influence on the willingness to disclose personal data, thus being in accordance with former research in a commerce context [56]. In turn, in the context of weak data sensitivity, the relationship is not significant. These results suggest that customers attribute different advantages of service improvement benefits to the type of data. In this regard, customers might not be able to imagine how their activity data could lead to individual and valuable service improvement benefits by a health insurance company (e.g. suggestions for sport or fitness activities). In contrast, customers might attribute service improvements benefits to the disclosure of health data that offer them benefits that support the treatment of health issues (e.g. faster clearance of special treatments, suggestion for physician consultations). As a practical implication, health insurance companies could either focus their service improvement benefits solely on measurements that are related to the health data of their customers or make every effort to emphasize to the customers how also the disclosure of activity data could lead to valuable service improvements.

Finally, our results do not confirm the hypothesized moderating effect of perceived activity status / perceived health status on the relationship between privacy risks and the willingness to disclose personal self-tracking data to a health insurance company and thus are contradicting pervious findings in a health-care context [2, 54]. As shown before, privacy risks have in both contexts a significant negative effect on the willingness to disclose data. Since neither the perceived activity status nor perceived health status mitigate this relationship for users who do have a favorable activity or health condition, the results suggest that the privacy risks are determined independently of one's actual condition. For health insurance companies, these results are favorable since they suggest that customers with an unfavorable activity or health condition do not assess privacy risks differently than those with a good condition. Hence, if the health insurance companies manage the perceived privacy risks well, they are able to reach all customers independent of their perceived activity status or health status.

7. Conclusion

Since privacy research with a focus on highly personal activity or health data has received little attention so far, we directed our research on the field of highly sensitive data of self-tracking. Therefore, we set out to deductively build up a conceptual model with which we aimed to determine the influence of the calculus of personal risks and benefits on the willingness of an individual to disclose personal self-tracking data a health insurance company.

To answer our research question, we build on the privacy calculus part of the APCO model of Smith et al. [50], added the context specific moderator variables perceived activity status / perceived health status and used the factorial survey approach to build two conceptual models, which allowed us to create hypothetical settings and compare the results for weak and strong data sensitivity. Our results reveal that privacy risks always have a negative impact on the willingness to disclose personal data, while positive effects of privacy benefits are partly depending on the data sensitivity. Further, the perceived activity status and perceived health status of a user has no effect on the relationship between privacy risks and the willingness to disclose personal self-tracking data. Our research results advance the theoretical understanding in the field of information privacy and provide practical implications for practitioners in the field of self-tracking privacy decisions. Especially for health insurance companies, our research reveals a deeper understanding which factors concerning the disclosure of self-tracking data are important for their customers. Hence, they will be able to adapt their services accordingly.

Besides our promising results, we acknowledge the following limitations and suggest future research. At first, our results are based on two hypothetical contexts which we presented to the sample group. While the results for real case situations might differ, we suggest a review of our results as soon as the disclosure of personal self-tracking data to health insurance companies is a common practice. Further, with our research models, we only analyzed how the influence of the calculus of personal risks and benefits on the willingness to disclose personal data differs depending on the data sensitivity. Yet, the analysis if the willingness to disclose is significantly different between the two contexts remains for future research. Lastly, former research identified several other possible determinants on the willingness to disclose personal data, most prominently privacy concerns, which comprises elements such as privacy experience, demographic differences or culture. Succeeding research may then narrow down the focus on these specific aspects.

8. References

[1] Anderson, C.L. and R. Agarwal, "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information", Information Systems Research, 22(3), 2011, pp. 469–490.

[2] Bansal, G., F.“M.” Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", Decision Support Systems, 49(2), 2010, pp. 138–150.

[3] Barrett, M., E. Davidson, J. Prabhu, and S.L. Vargo, "Service innovation in the digital age: Key contributions and future directions", MIS Quarterly, 39(1), 2015, pp. 135–154.

[4] Buck, C., C. Horbel, C.C. Germelmann, and T. Eymann, "The Unconscious App Consumer: Discovering and Comparing the Information-seeking Patterns among Mobile Application Consumers", Proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv, 2014.

[5] Campbell, J.E. and M. Carlson, "Panopticon.com: Online Surveillance and the Commodification of Privacy", Journal of Broadcasting & Electronic Media, 46(4), 2002, pp. 586–606.

[6] Chellappa, R.K. and R.G. Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer’s Dilemma", Information Technology and Management, 6(2-3), 2005, pp. 181–202.

[7] Chen, R., "Living a private life in public social networks: An exploration of member self-disclosure", Decision Support Systems, 55(3), 2013, pp. 661–668.

[8] Contena, B., Y. Loscalzo, and S. Taddei, "Surfing on Social Network Sites", Computers in Human Behavior, 49, 2015, pp. 30–37.

[9] Cronin, J.J. and S.A. Taylor, "Measuring Service Quality: A Reexamination and Extension", Journal of Marketing, 56(3), 1992, p. 55.

[10] Culnan, M.J. and P.K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", Organization Science, 10(1), 1999, pp. 104–115.

[11] Culnan, M.J. and R.J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations", Journal of Social Issues, 59(2), 2003, pp. 323–342.

[12] Davies, S.G., "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity", Technology and Privacy: The New Landscape, 1997, pp. 143–165.

[13] Dinev, T., M. Bellotto, P. Hart, V. Russo, I. Serra, and C. Colautti, "Internet Users' Privacy Concerns and Beliefs About Government Surveillance", in Handbook of Research on Information Management and the Global Landscape, M.G. Hunter and F.B. Tan, Editors. 2009. IGI Global.

[14] Dinev, T. and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions", Information Systems Research, 17(1), 2006, pp. 61–80.

[15] Forest, A.L. and J.V. Wood, "When social networking is not working: individuals with low self-esteem recognize but do not reap the benefits of self-disclosure on Facebook", Psychological science, 23(3), 2012, pp. 295–302.

[16] Fornell and Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", Journal of Marketing Research, 18(1), 1981, pp. 39–50.

[17] Frings, C., "Das Messinstrument faktorieller Survey", in Soziales Vertrauen: Eine Integration der soziologischen und der ökonomischen Vertrauenstheorie, C. Frings, Editor. 2010. VS Verlag für Sozialwissenschaften: Wiesbaden.

[18] Garfinkel, S., "Database nation: The death of privacy in the 21st century, 1st edn., O'Reilly, Beijing u.a., 2001.

[19] Gefen, D., E.E. Rigdon, and D. Straub, "An Update and Extension to SEM Guidelines for Administrative and Social Science Research", MIS Quarterly, 35(2), 2011, pp. 3–14.

[20] Gimpel, H., M. Nissen, and R. Goerlitz, "Quantifying the Quantified Self: A Study on the Motivations of Patients to Track Their Own Health", Proceedings of the Thirty Fourth International Conference on Information Systems, Milan, 2013.

[21] Green, T., T. Wilhelmsen, E. Wilmots, B. Dodd, and S. Quinn, "Social anxiety, attributes of online communication and self-disclosure across private and public Facebook communication", Computers in Human Behavior, 58, 2016, pp. 206–213.

[22] Hair, J., C.L. Hollingsworth, A.B. Randolph, and A.Y.L. Chong, "An updated and expanded assessment of PLS-SEM in information systems research", Industrial Management & Data Systems, 117(3), 2017, pp. 442–458.

[23] Hair, J.F., C.M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a Silver Bullet", The Journal of Marketing Theory and Practice, 19(2), 2011, pp. 139–152.

[24] Hair, J.H., JR., G.T.M. Hult, C.M. Ringle, and M. Sarstedt, "A Primer on Partial Least Squares Structural Equation Modeling PLS-SEM, Sage Pubn Inc, Thousand Oaks, 2014.

[25] Hann, I.-H., K.-L. Hui, S.-Y. Lee, and I. Png, "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach", Journal of Management Information Systems, 24(2), 2007, pp. 13–42.

[26] Henseler, J., C. Ringle, and M. Sarstedt, "A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling", Journal of the Academy of Marketing Science, 43(1), 2015, pp. 115–135.

[27] Henseler, J., C.M. Ringle, and M. Sarstedt, "Testing measurement invariance of composites using partial least squares", International Marketing Review, 33(3), 2016, pp. 405–431.

[28] Huang, H.-Y., "Examining the beneficial effects of individual's self-disclosure on the social network site", Computers in Human Behavior, 57, 2016, pp. 122–132.

[29] Hui, K.-L., B.C.Y. Tan, and C.-Y. Goh, "Online Information Disclosure: Motivators and Measurements", ACM Transactions on Internet Technology, 6(4), 2006, pp. 415–441.

[30] IDC, "Worldwide Smartwatch Market Will See Modest Growth in 2016 Before Swelling to 50 Million Units in 2020", 2016.

[31] Keith, M.J., S.C. Thompson, J. Hale, P.B. Lowry, and C. Greer, "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior", International Journal of Human-Computer Studies, 71(12), 2013, pp. 1163–1173.

[32] Kim, H.-S., "What drives you to check in on Facebook?: Motivations, privacy concerns, and mobile phone involvement for location-based information sharing", Computers in Human Behavior, 54, 2016, pp. 397–406.

[33] Laufer, R.S. and M. Wolfe, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory", Journal of Social Issues, 33(3), 1977, pp. 22–42.

[34] Likert, R., "A Technique for the Measurement of Attitudes, Columbia Univ, New York, 1932.

[35] Lu, Y., B. Tan, and K.L. Hui, "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits", Proceedings of the Twenty-Fifth International Conference on Information Systems, Washington DC, USA, 2004.

[36] Lupton, D., "Understanding the Human Machine", IEEE Technology and Society Magazine(Winter), 2013, pp. 25–30.

[37] Lupton, D., "Self-tracking Cultures: Towards a Sociology of Personal Informatics", Proceedings of the Australian Conference on Human-Computer Interaction (HCI), Sydney, 2014.

[38] Lupton, D., "Self-tracking Modes: Reflexive Self-Monitoring and Data Practices", Proceedings of the Imminent Citizenships: Personhood and Identity Politics in the Informatic workshop, Canberra, 2014.

[39] Malhotra, N.K., S.S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", Information Systems Research, 15(4), 2004, pp. 336–355.

[40] Norberg, P.A., D.R. HORNE, and D.A. HORNE, "The privacy paradox: Personal information disclosure intentions versus behaviors", Journal of consumer affairs: official publication of the American Council on Consumer Interests, 41(1), 2007, pp. 100–126.

[41] Parasuraman, A., V.A. Zeithaml, and L.L. Berry, "SERVQUAL: Multiple-Item Scale for Measuring Consumer Perceptions of Service Quality", Journal of Retailing, 64(1), 1988, pp. 12–40.

[42] Pavlou, P. and D. Gefen, "Building Effective Online Marketplaces with Institution-Based Trust", Proceedings of the Twenty-Third International Conference on Information Systems, Barcelona, 2002.

[43] Peter, J.P. and L.X. Tarpey, "A Comparative Analysis of Three Consumer Decision Strategies", Journal of Consumer Research, 2(1), 1975, pp. 29–37.

[44] Petronio, S., "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples", Communication Theory, 1(4), 1991, pp. 311–335.

[45] Phelps, J., G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information", Journal of Public Policy & Marketing, 19(1), 2000, pp. 27–41.

[46] Posey, C., P.B. Lowry, T.L. Roberts, and T.S. Ellis, "Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities", European Journal of Information Systems, 19(2), 2010, pp. 181–195.

[47] Ringle, C.M., M. Sarstedt, and D. Straub, "A Critical Look at the Use of PLS-SEM in MIS Quarterly", MIS Quarterly, 36(1), 2012, pp. 3–14.

[48] Ringle, C.M., S. Wende, and J.-M. Becker, "SmartPLS, SmartPLS GmbH, Bönningstedt, 2015.

[49] https://www.cebit.de/en/news-trends/news/self-tracking-generates-billions-177, accessed 9-3-2018.

[50] Smith, H.J., T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 35(4), 2011, pp. 989–1015.

[51] Straub, D.W., "Validating Instruments in MIS Research", MIS Quarterly, 13(2), 1989, pp. 147–169.

[52] Stutzman, F., R. Gross, and A. Acquisti, "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", Journal of Privacy and Confidentiality, 4(2), 2013, pp. 7–41.

[53] Swan, M., "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0", Journal of Sensor and Actuator Networks(1), 2012, pp. 217–253.

[54] Tisnado, D.M., J.L. Adams, H. Liu, C.L. Damberg, F.A. Hu, W.-P. Chen, D.M. Carlisle, C.M. Mangione, and K.L. Kahn, "Does the concordance between medical records and patient self-report vary with patient

characteristics?", Health Services and Outcomes Research Methodology, 6(3-4), 2006, pp. 157–175.

[55] Urbach, N. and F. Ahlemann, "Structural Equation Modeling in Information Systems Research Using Partial Least Squares", Journal of Information Technology Theory and Application, 11(2), 2010, pp. 5–40.

[56] White, T.B., "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework", Journal of Consumer Psychology, 14(1/2), 2004, pp. 41–51.

[57] Xu, H., T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances", Journal of the Association for Information Systems, 12(12), 2011.

[58] Xu, H., H.-H. Teo, B.C.Y. Tan, and R. Agarwal, "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", Journal of Management Information Systems, 26(3), 2009, pp. 135–174.

[59] Zimmer, J.C., R.E. Arsal, M. Al-Marzouq, and V. Grover, "Investigating online information disclosure: Effects of information relevance, trust and risk", Information & Management, 47(2), 2010, pp. 115–123.