Tracking Fitness or Sickness - Combining Technology Acceptance and Privacy Research to Investigate the Actual Adoption of Fitness Trackers

Riccardo Reith
University of Bayreuth
riccardo.reith@uni-bayreuth.de

Christoph Buck
Queensland University of Technology
christoph.buck@qut.edu.au

Bettina Lis
University of Bayreuth
bettina.lis@uni-bayreuth.de

Torsten Eymann
University of Bayreuth
torsten.eymann@uni-bayreuth.de

Abstract

Personal data is often collected, processed and utilized without the knowledge of the information system's user. With regard to the enormous value of personalized data for companies as well as consumers' tendency to unreflectively disclose their data, privacy concerns have been an essential topic for researchers since the mid-1990s. However, established research models of wearable IS-technologies are inadequate to comprehensively investigate the issue of privacy and its effects on acceptance variables. Therefore, the following study aims to empirically validate a research model which considers privacy concerns as a central construct in predicting the actual usage of fitness trackers. The results of our investigation underline the vital role of privacy concerns for the acceptance of fitness trackers and imply that the current providers' advertising is insufficient in meeting the consumers' needs.

1. Introduction

Latest scandals of Facebook and Google have shattered the consumer's trust in using IS, particularly showing doubt in an appropriate and reasonable usage and storage of personal data. In contrast to most economic exchanges, individuals are usually not able to estimate the quality and performance characteristics of the IS they use. Nevertheless, research reveals that individuals are concerned about their privacy and that they are cautious regarding the collection and use of their personal data [13].

Fitness Trackers (FTs) are an IS which gathers highly sensitive and therefore extremely valuable personalized body data, such as heart frequency and activity level. These self-tracking devices can be worn on the body, interact with multi-sensor platforms on the Internet of Things and collect data about daily activities, exercise and vital body data [21]. The user profiles, which are developed out of the data can be particularly interesting for health insurance companies, who already incentivize by granting subsidies or even mandate the use of FTs. Previous research has focused mainly on the technological aspects and only few studies have addressed the problem of privacy issues [e.g. 17]. Therefore, Kalantari [28] explicitly encouraged further research to gain a deeper understanding of adoption antecedents such as privacy concerns in the field of wearable technology. Additionally, the scope of current research has been limited to the investigation of intention to use rather than actual adoption. Consequently, our study endeavors to close these research gaps.

To widen the scope of current research, this study addresses the call for a unified research model and merges the APCO (Antecedents - Privacy - Concerns - Outcomes) model [48] with an enhanced Technology Acceptance Model (TAM) [10], thereby combining the two prevailing research models of their respective domains. Herein, we seek to validate the consumers' privacy concerns as a second-order construct, which is supported by established literature regarding privacy [e.g. 34, 50]. Furthermore, we derive novel theoretical contributions regarding the relationship between privacy concerns and subjective norms in the domain of FTs. As our knowledge of FTs is largely based on the evaluation of the consumer's intention to use such devices, this study aims to evaluate the underlying rationale of building attitudes, which lead to intention and finally to the actual usage of wearable technology. To develop useful practical implications, we analyzed the contents of the websites of five FT providers in Germany and compared, if the communicated aspects of their marketing strategy are consistent with the recommendations gained from the results of our investigation. Our findings offer vital options of improvement for current marketing concepts, which for the

URI: https://hdl.handle.net/10125/64176
978-0-9981331-3-3

most part do not appropriately consider privacy aspects in their communication strategy.

2. Relevant Work

2.1 Fitness Trackers and Technology Acceptance

Researchers in the field of FTs regularly referred to established acceptance models such as the TAM, the Unified Theory of Acceptance and Use of Technology (UTAUT) proposed by Venkatesh et al. [61] as well as various extensions of these models. The TAM and UTAUT have been shown to achieve satisfactory predictive power when evaluating the benefits of FT devices [e.g. 27, 63]. A few studies considered a combination of established acceptance models such as TAM and UTAUT in the domain of IS [59, 64]. Due to the special context of FTs, researchers investigated the impact of social factors, as the usage of novel technologies can help individuals improve their image and differentiate them from other members of their peer group [6]. Gao et al. [17] as well as Wu et al. [63] were able to confirm the importance of social influence on the acceptance of wearable fitness devices. Furthermore, past studies have integrated barriers against using wearable technologies, such as lack of trust [23], performance risks [68] as well as security and privacy concerns [e.g. 36] into their research models. Privacy issues are of particular importance, as their impact on the intention to use is twofold: For one thing, they directly affect the consumer's intention to use a given technology [13, 48], and for another, they have a negative impact on the mediating factor of trust [23], which consequently dampens the intention to use. Due to the special characteristics of FTs, an integration of privacy constructs into traditional acceptance models is crucial, as this essential barrier is not well understood in the field of wearable technology [28].

2.2 Privacy research

As this study investigates the acceptance of FTs, it focuses on the dimension of information privacy and refers to information that is individually identifiable or describes the private informational spheres of an individual [48]. According to economic theory and the notion of privacy as a tradeable asset [49], users do not disclose their data unless they expect it to yield personal benefits. In literature, this cost-benefit analysis is described as the privacy calculus [e.g. 12]. According to the privacy calculus, "individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes" [51]. Therefore, users are supposed to undertake an anticipatory, rational weighing of risks as well as benefits and make fully informed decisions when being confronted to disclose personal information [9, 34].

A central aspect to numerous empirical research studies on privacy is the construct of privacy concerns [e.g. 30]. Therefore, almost all empirical privacy studies in social sciences are based on privacy concerns as a privacy-related proxy to measure information privacy [3, 48]. As privacy concerns emerged as the central measurement in privacy research, the three most important macro-models in privacy research set them as their central construct for the explanation of privacy behavior [3, 32, 48]. As both domains, research of technology acceptance and privacy research, call for a corresponding extension of their existing research models for the investigation of FTs [13, 28], this paper provides a novel approach by merging TAM and APCO. In the next chapter, we review both models.

3. Theoretical Framework and Model Development

3.1 An enhanced Technology Acceptance Model

The TAM theorizes that the effects of external variables such as system characteristics and development processes on the intention to use are mediated by the two variables "perceived ease of use" and "perceived usefulness" (PU) [10, 60]. Both factors relate to the individual's attitude towards using a technological system (AT). Furthermore, the factors affect the behavioral intention (IU), which then impacts the actual use [40]. In the field of health information and wearable technology, which includes FTs, the TAM provides the basis for most studies [18, 28] as a multitude of researchers have drawn upon the model for their investigation on the adoption of wearable devices [e.g. 17, 29].

Venkatesh and Davis [60] enhanced the original TAM to the so-called TAM 2 by integrating the variable "subjective norm" (SN). This integration is supported by theory of reasoned action (TRA) [14]. Consequently, we integrated the variable "subjective norm", which plays a vital role in the context of wearable technology [e.g. 17, 28]. However, there is not only a social desire when an individual is evaluating whether to adopt FTs. Personal health information is an extremely sensitive subject for the vast majority of the population. The influence of privacy concerns (PC) on a consumer's adoption of this technology appears highly relevant, as most FT services lack privacy

policies and those that do are not transparent [53]. Although these concerns have been researched extensively for IS [3, 32, 48] and have been shown to be associated with technology acceptance [2, 57], their connection to the TAM has not been investigated as thoroughly.

3.2 The APCO Model

Regarding the three overarching macro models in privacy research, the most popular work has been done by Smith et al. [48]. The so-called APCO model is divided into three main categories: Antecedents (A), Privacy Concerns (PC) and Outcomes (O). Smith et al. [48] also identified privacy concerns as the main construct in privacy research and these concerns are examined in the literature as both a dependent and independent variable.

One variable which has been proposed as an outcome of privacy concerns is trust. Various Studies indicate the significance of trust especially in the presence of uncertainty, for instance, regarding the usage of personal data [e.g. 41, 47]. A lower level of privacy concerns goes in line with increased trust and impacts the outcome of privacy decisions [35, 67]. Consequently, including the trust in operator (TO) variable into our TAM-based model is necessary and consistent with various research in the field of privacy [e.g. 13, 48] as well with acceptance research of health information technology [e.g. 4].

Another construct, which is affected by privacy concerns is the privacy calculus [48]. Herein, individuals deliberate on the risks involved and the potential benefits received when deciding to disclose personal information [12]. The privacy calculus is therefore an individual trade-off between privacy-related risks and benefits. Both constructs, the privacy calculus and trust are proposed to affect privacy behavior according to the APCO [48].

3.3 Merging TAM and APCO

With the combination of the TAM 2 [10, 60] and the APCO model [48], our research contributes to the rising debate on privacy issues regarding the use of self-tracking devices. We applied the construct of privacy concerns as a core antecedent to form the privacy calculus in our research model. According to APCO, it is reasonable to assume that privacy concerns reflect individual privacy risks, herein forming one part of the privacy calculus [12]. For the benefit-aspect of the privacy calculus, we used the TAM variable perceived usefulness. Both constructs are proposed to affect the individual's attitude towards using FT devices, thereby specifying the privacy calculus of the APCO model through the assessment of attitude in the TAM. The individual's attitude, which reflects an evaluation of privacy risks and benefits, affects the intention to use according to the TAM. This is also consistent with the APCO model, indicating that the privacy calculus impacts behavioral reactions, such as the disclose of personal information. As the usage of FTs is inevitably correlated with the disclosure of personal information for most devices, it is a sensible approach to replace the behavioral reactions of APCO through intention to use of TAM in the context of FTs.

Through the combination of the APCO model and the TAM 2, we identified new path structures, which were not proposed in each of the original models. First, the original TAM 2 did not include trust, which is an essential element according to the APCO framework. Second, the APCO did not include subjective norm, which is proposed as an important factor in TAM 2. This begs the question, how both constructs can be integrated into a coherent research model, which will be discussed in the following chapter.

Consequently, our study follows the call for research from Kalantari [28] and sheds new light on the existing literature by delving deeper into privacy concerns as a vital adoption antecedent. Additionally, we

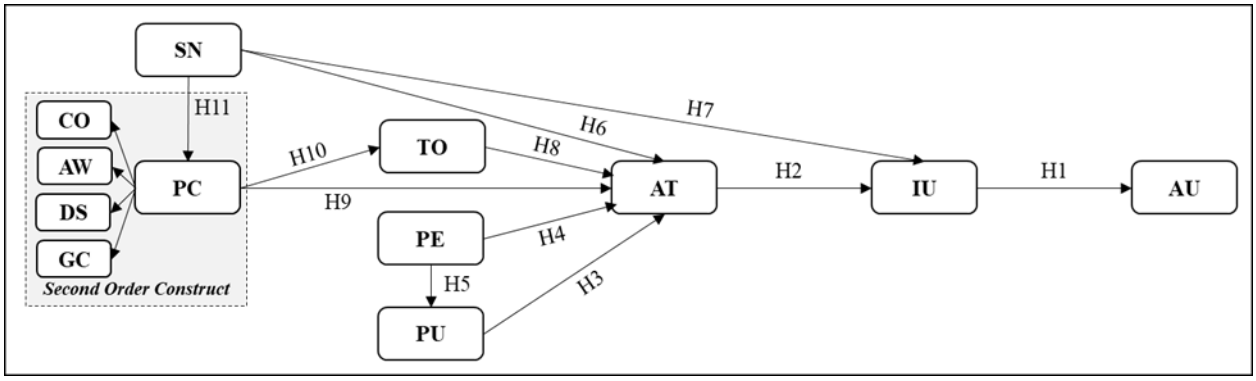

Figure 1. Proposed research model

gain a comprehensive understanding of the relationship between privacy concerns, subjective norms and the behavioral reaction, which Kalantari [28] also identified as a research gap. The construct privacy concerns is established appropriately as a second-order latent construct and consists of collection (CO), awareness (AW), data sensitivity (DS) and global information privacy concerns (GC). Our suggested framework can be seen in Figure 1.

4. Hypotheses

Regarding the hypotheses, we focused on the connections between APCO and TAM, as the hypotheses of TAM and APCO are well established by previous investigations. According to TAM [10], we propose:

H1: The behavioral intention to use FTs positively affects the actual usage of FTs.

H2: The attitude toward using FTs positively affects the behavioral intention to use FTs.

H3: Perceived usefulness has a positive influence on the attitude towards FTs.

H4: Perceived ease of use positively affects the attitude towards FTs.

H5: Perceived ease of use positively affects perceived usefulness.

As mentioned above, Venkatesh and Davis [60] suggested the integration of subjective norm into the TAM 2. The TAM 2 bases its hypotheses on the TRA [14] and the subsequent theory of planned behavior (TPB) [1], which propose that subjective norms have a direct influence on intention to use. Herein, subjective norms refer to perceived rules of conduct that are built through compliance, internalization and identification mechanisms and shared by a reference group [1, 14, 60]. The rationale for a direct correlation between subjective norm and intention to use can be explained by perceived social pressure (compliance) or affiliation motivation (identification). Within the context of FTs, people may feel a social pressure to be physically fit and consequently use FTs regardless of their attitude towards such devices. Regarding the identification mechanism, people may intend to use a FT device just to feel more integrated into their social environment, even if they are not keen toward the usage or its consequences themselves [60]. Previous studies confirmed the positive impact of social influence on the intention to adopt FTs [17].

Whereas the proposed direct effect of subjective norm on intention in TRA and TPB is based on compliance and identification, the internalization mechanism indicates an indirect relationship between subjective norm and intention to use through attitude. Here, internalization is described as an "influence to accept information from another as evidence about reality" [11]. That means, that individuals incorporate their referent's belief structure into their own belief structures [60]. The social expectation that one should intend on using a technology can enhance someone's view of the technology's value [46]. In the context of FTs, individuals would likely internalize the advice of important sporty friends and shape their attitude about FTs accordingly. Regarding these arguments, we hypothesize:

H6: Subjective norm positively affects the attitude towards FTs.

H7: Subjective norm positively affects the intention to use FTs.

The use of FTs requires consumers to share vulnerable body data with the provider of the FT or the connected service. Herein, consumers generally assume that a trusted service provider will act in a socially responsible manner and not take advantage of their vulnerabilities [19] such as the abuse of personal data. Consequently, consumers with a high level of trust are less likely to assume that service providers will take advantage of their data and therefore evaluate the attitude towards FTs more positively. Regarding the exchange of personal data, Shin [47] was able to confirm a positive correlation between trust and attitude towards using social network sites. In the context of fitness apps, Beldad and Hegner [4] already confirmed a positive relationship between trust in the app developer and perceived usefulness, which is correlated to an individual's attitude according to the TAM. Thus, we propose the following hypothesis:

H8: Perceived trust positively affects the attitude towards FTs.

Users of FTs have to disclose sensitive personal data [25]. As monitoring of personal information is ubiquitous, the concerns about information privacy are growing. Current research states that privacy concerns have a direct impact on privacy behavior [48]. Additionally, privacy concerns affect privacy-related risks, which directly impact privacy behavior [48]. Consequently, privacy concerns reflect the risk-related part of the privacy calculus, which is measured as attitude towards FTs, assessing an evaluative predisposition to the behavior as a function of its determinant personal consequences [14]. Therefore, high privacy concerns result in a tentative appraisal regarding FTs and in a more negative attitude towards FTs. Consequently, we hypothesize:

H9: Privacy concerns negatively affect the attitude towards FTs.

The relationship between privacy concerns and trust has been extensively investigated and is proposed in the APCO model [48]. Consequently, we hypothesize:

H10: Privacy concerns negatively affect trust.

Kalantari [28] claims that further research in the domain of FTs should be conducted in order to identify how privacy concerns are mediated by social norms. However, previous findings indicate that subjective norms will influence individual beliefs such as privacy concerns. Privacy concerns, as an individual's evaluation about the potential for a loss associated with personal information [42], are likely to be an issue which will be discussed with important others. The variable subjective norm refers to the opinion of significant others about, for instance, the usage of FTs. According to the Social Identity Theory [54], people tend to classify themselves as in-group members. Individuals compare themselves to the in-group [54, 62], which herein exerts influence on the individual's belief structure. Consequently, if the social system is likely to recommend FTs, individuals are likely to adopt the positive beliefs of important others and lower their privacy concerns regarding FTs. This rationale is consistent with the self-categorization theory of Turner [58], proposing that people use the reference group's opinion to create a picture of reality, which is consistent with their social identity. This implies that the social opinion leads to an adjustment of individual belief structures until these beliefs are consistent with the corresponding group norms. In the context of FTs, individuals would link their privacy concerns to the recommendation of others and adjust their privacy issues towards these devices accordingly. Consequently, we hypothesize:

H11: Privacy concerns negatively affect subjective norm.

5. Operationalization and Data Collection

All constructs in this paper have been adapted from previously validated studies. We adjusted the original TAM variables "perceived ease of use", "perceived usefulness", "attitude towards using" and "intention to use" [10, 29, 61] for the context of FTs. Regarding the extension of the TAM, we used items of Gefen et al. [20] to assess "trust" and the items of Venkatesh and Davis [60] to evaluate "subjective norm". To examine privacy concerns in an appropriate manner, we based our model on the Internet users' information privacy concerns (IUIPC) of Malhotra et al. [34]. Although this construct has not been used extensively in previous research [3], it has been shown to be more profound at explaining variance than the often used "concern for information privacy" (CFIP) [34]. According to Malhotra et al. [34], privacy concerns are established as a second-order construct entailing "collection", "control", and "awareness". Herein, collection "captures the central theme of equitable information exchange based on the agreed social contract" [34]. The variable "control" "represents the freedom to voice an opinion or exit" and the factor "awareness" "indicates understanding about established conditions and actual practices" [34]. Malhotra et al. [34] additionally used the factor "global information privacy concerns" which we adjusted for FTs and included in the second-order construct "privacy concerns". Furthermore, we considered the high sensitivity of the collected physical fitness data and therefore integrated the variable "data sensitivity," which we adapted from Mohamed and Ahmad [37]. For actual usage, we applied a binary interval of Bhattacherjee [5].

To collect data we used an online survey, which took place from February 22nd to March 12th, 2018, in Germany. We used convenience sampling on social media to reach participants and systematic sampling by posting our questionnaire on social media groups for sports students to particularly reach adopters of FTs. In total, 773 subjects participated in our study and due to our control questions, a total of 582 questionnaires could be evaluated. 50.5 percent of the 17- to 65-year-old participants were female and 49.5 percent were male. We noted that predominantly younger people participated in the corresponding survey, with an M age = 29.9. Our sample shows a high educational level with more than 50 percent of the subjects having attained a university degree. Regarding the usage of FTs, 46.7 percent of our sample currently use FTs and 53.3 percent do not use FT devices.

6. Results

6.1 Measurement model

To confirm the reliability and validity of our scales, we tested Cronbach's alpha, composite reliability, convergent validity as well as discriminant validity. An exploratory factor analysis confirmed the assumed one-dimensionality of our variables. All constructs exceed the recommended threshold value of 0.70 [38] for Cronbach's alpha. Convergent validity was assessed on the basis of factor loadings, composite reliability and average variance extracted. Factor loadings should be over 0.5, composite reliabilities over 0.8 and the minimum for the average variance extracted is 0.5. All the criteria for convergent validity were met. However, we had to delete the first item of subjective norm due to its low loading (.590) to reach the recommended level of 0.8 for composite reliability. Regarding discriminant validity, it is equal to the approach Fornell and Larcker [15] to illustrate discriminant validity by showing that the square roots of the AVEs are greater than the corresponding off-diagonal inter-construct correlations [24]. This criteria was met for our data. Hu and Bentler [26] suggest combining

the Tucker-Lewis Index (TLI), the Incremental Fit Index (IFI), the Comparative Fit Index (CFI) as well as the Standardized Root Mean Square Residual (SRMR) to validate the model. The TLI = .947, IFI = .954, CFI = .954 and the SRMR = .061 indicates a good measurement model fit. Due to the use of a single method (online survey), we tested for common method bias. Herein, we integrated a common latent factor to capture the common variance among all observed variables [43]. The comparison of the standardized regression weights from the model without the latent factor did not show significant differences to the model with the integrated latent factor, indicating that common method bias was not a great concern.

6.2 Structural model and hypothesis test

The same model fit indices were used to validate the structural model and showed a satisfactory level. We also controlled for age and gender. The TLI = .929, IFI = .938, CFI = .937 and the SRMR = .086, which indicates a good model fit, except for the SRMR. However, the SRMR is near to the strict recommended threshold of Hu and Bentler [26] and can be considered acceptable.

The analysis of the structural equation model revealed that nearly all proposed hypotheses were significant, except the effects of EOU, rejecting H4. The summary of our evaluation can be seen in Table 1.

Table 1. Summary of the hypothesis test.

Variable	B	SE B	C .R.	β	P
H1: IU → AU	.183	.008	22.978	.691	<.001***
H2: ATT → IU	1.292	.058	22.289	.793	<.001***
H3: PU → ATT	.280	.028	9.888	.388	<.001***
H4: PEU → ATT	.044	.041	1.067	.039	n.s.
H5: PEU → PU	.165	.072	2.276	.107	<.05**
H6: SN → ATT	.253	.036	7.037	.286	<.001***
H7: SN → IU	.152	.043	3.561	.105	<.001***
H8: TO → ATT	.171	.043	4.028	.158	<.001***
H9: PC → ATT	-.417	.058	-7.147	-.351	<.001***
H10: PC → TO	-.363	.057	-6.313	-.331	<.001***
H11: SN → PC	-.219	.068	-3.207	-.166	<.001***

Note: B = unstandardized coefficient, SE B = standard error B, C.R = critical ratio, β = standardized coefficient, p = p-value (* p < .1;** p < .05; *** p < .001; n.s. = not significant).

7. Discussion

7.1 Theoretical implications

Following the call for research to combine privacy with behavioral reaction by integrating the TAM into the APCO was validated as a promising approach, as shown by the result of the satisfactory fit of our model. Consequently, this study has several major contributions to theory. The integration of privacy concerns into an acceptance model for wearable devices widens the scope of current research, as this essential barrier has not yet been considered by most investigations [e.g. 7, 8, 29]. Gao et al. [17] investigated the impact of privacy-related barriers on the intention to adopt healthcare wearable devices. However, they did not establish privacy concerns as a second-order construct, which limits the contribution of their outcomes. Validating this construct in a suitable manner is vital and established literature regarding privacy explicitly emphasized the need to validate this construct as a second-order factor [e.g. 34, 50, 66]. We based our construct on the second-order factor IUIPC of Malhotra et al. [34], as this factor has been shown to explain more variance of a person's willingness to transact than the CFIP and is being underutilized by current investigations [3]. The IUIPC construct was adapted due to the special context of FTs and could be evaluated as a second-order latent construct consisting of the first-order factors "collection", "awareness", "global information privacy concerns" and "data sensitivity".

Second, the influence of subjective norm is particularly interesting in the context of FTs considering the growing social pressure and fitness trend on social media. The effect of subjective norm on intention to use

is partially mediated through the consumer's attitude. The direct impact on attitude can be explained by an underlying internalization mechanism. Consequently, a person internalizes the advice of other persons within their social system and integrates this advice to shape an individual attitude. This effect was illustrated to a high level within our sport-affine sample, as French and Raven [16] emphasize a strong social influence for persons with special knowledge or proficiency in a particular domain. The underlying rationale for a direct relationship between subjective norm and the intention to use FTs is likely to be a result of an identification or compliance mechanism. Consequently, persons will intend to use FTs due to social pressure or to establish or maintain a social relationship to another individual, without building a positive attitude towards such devices.

Furthermore, we were able to shed new light on the relationship between privacy concerns and subjective norm in the context of FTs. Kalantari [28] encourages researchers to close this research gap and explain how privacy concerns are mediated by social norms. We identified that subjective norms have a negative influence on privacy concerns, confirming that individuals adjust their belief structure regarding privacy as a result of their reference group's opinion. This result underlines the vital role of subjective norms in the domain of FT devices. Additionally, the establishment of subjective norm as an antecedent of privacy concerns enriches the scarce literature on the left-hand side of the APCO model, viewing privacy concerns as a dependent variable [48].

Third, we contribute to the long-running debate of perceived usefulness being mediated by attitude rather than showing a directly influencing intention to use. A direct relationship between usefulness and intention was proposed by Davis [10] in the original TAM, where people performed a behavior in order to increase their job performance. In such organizational settings, people may perform a behavior just to increase their job performance regardless of whether their attitude towards the behavior is positive or negative. However, as the usage of FTs is voluntary, we followed the assumption of Fishbein and Ajzen [14] that individual beliefs affect behavior only via an indirect influence on attitude.

Surprisingly, the TAM's variable perceived ease of use did not show a direct significant effect on the attitude towards FTs. An explanation for this somewhat astounding result is given by Venkatesh et al. [61], who identified that perceived ease of use will only show a significant influence on attitude in the initial stage of technology adoption. Regarding the wide adoption of FTs within our sample as well as the high level of sport involvement, these devices cannot be considered novel anymore. We also assume that the age of our sample might be a rationale for the missing effect of ease of use on attitude. As we analyzed predominantly Digital Natives and therefore a younger and affine group for new technologies [39, 44], ease of use might not be very relevant to this target group. Additionally, other research regarding wearable technology was not able to confirm significant effects of ease of use on attitude either [e.g. 7, 8].

However, and contrary to other research [e.g. 7, 8, 29], we investigated actual behavior instead of only referring to the consumer's intention to use FTs. Although previous studies in IS identified intention to be a powerful predictor of actual behavior [e.g. 55], some researchers [e.g. 52] have expressed concerns about the predictive ability of intention. Our results confirm that intention is a powerful predictor of actual adoption. Furthermore, an investigation of actual behavior benefits practitioners and enables us to develop appropriate recommendations.

7.2 Practical implications

In order to develop target-oriented recommendations, we analyzed the contents of the websites and advertising of the five most established FTs in Germany. Herein, we searched for information regarding the collection and usage of data captured by providers of FTs, namely "Fitbit", "Garmin", "Samsung", "Polar" and "TomTom". Our analysis did not identify advertising or communicated content concerning privacy or data security issues for four of the five providers. As a result, a user of such devices might become skeptical regarding the usage and storage of their data, which aggravates their privacy concerns. Privacy issues do not only negatively affect the attitude towards using but do also show a significant negative influence on important predictors of attitude such as trust. Consequently, we strongly recommend the providers of FTs to establish a compelling marketing message to alleviate the privacy concerns among their current users and potential customers. Privacy issues can be dampened by establishing a data protection declaration and an appropriate privacy policy within the company [65]. Xu et al. [65] identified structural assurances through privacy policy as being a crucial factor to reduce privacy risks. Fitbit as the only provider included the issue of privacy concerns into their website and communicated the security as well as a data protection declaration, illustrating a promising approach and a competitive advantage towards the other providers. In this context, Culnan and Armstrong [9] identified that consumers are more willing to continue their interactions with a company when fair information and data practices are

applied and communicated. Another approach to reduce privacy concerns is the establishment of functional cyber security systems, as privacy issues and cyber security are related [33]. Systems ensuring data security should be certified by independent organizations [33] to increase transparency and therefore the user's trust.

In line with the related studies of Chuah et al. [8] and Choi and Kim [7], we could not identify ease of use to significantly predict the attitude towards FTs. By analyzing the contents of the five named FT providers, we noticed that TomTom highlights their FTs to be easy and intuitive to use as well as their compatibility with other smart devices. Instead of the device's intuitive use, we recommend a promotion of other aspects such as data security or subjective norm. Both subjective norm and perceived usefulness show strong effects on the attitude towards FTs. Furthermore, we were able to demonstrate that subjective norm positively influences the intention to use FTs and helps to lower individual privacy concerns. Consequently, people might tend to value and be persuaded by social ties, such as family and friends [22]. In order alleviate privacy concerns and change attitudes provoking electronic word-of mouth appears to be a powerful instrument [e.g. 31]. Therefore, providers of FTs should provide a platform which allows all users to share, compare and discuss recorded data, if they wish to do so. Furthermore, an integration into popular social media platforms should be implemented. The Runtastic fitness application for smartphones is a good example for sharing recorded fitness data on Facebook [56]. By analyzing the websites of the providers of FTs, we identified that all providers strongly emphasize the usefulness of their devices, which is in line with the results of our investigation.

7.3 Limitations and further research

We are aware that this research may have some limitations, which offer opportunities for further research. Our sample focused on the group of Digital Natives. As this customer group is assumed to be less careful in disclosing their personal data [45], the results of our study show slight bias compared to the entire German population. Additionally, culture is an antecedent of privacy concerns according to the APCO model [48]. Cultural aspects can moderate the effects of our model. Consequently, future research should apply our model in different cultural contexts to confirm its validity. Furthermore, not all FT devices are connected to a cloud and some versions can work without the collection of sensitive data. As we did not control for this, the results of our study might be biased, as our surveyees might not connect the actual adoption to the disclosure of sensitive personal data.

8. References

[1] Ajzen, I., "The theory of planned behavior", Organizational Behavior and Human Decision Processes, 50(2), 1991, pp. 179–211.

[2] Bailey, A.A., I. Pentina, A.S. Mishra, M. Ben, and M. Slim, "Mobile payments adoption by US consumers: An extended TAM", International Journal of Retail & Distribution Management, 45(6), 2017, pp. 626–640.

[3] Bélanger, F. and R.E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", MIS Quarterly, 34(4), 2011, pp. 1017–1041.

[4] Beldad, A.D. and S.M. Hegner, "Expanding the Technology Acceptance Model with the Inclusion of Trust, Social Influence, and Health Valuation to Determine the Predictors of German Users' Willingness to Continue using a Fitness App: A Structural Equation Modeling Approach", International Journal of Human–Computer Interaction, 34(9), 2017, pp. 882–893.

[5] Bhattacherjee, A., "Managerial Influences on Intraorganizational Information Technology Use: A Principal-Agent Model", Decision Sciences, 29(1), 1998, pp. 139–162.

[6] Buenaflor, C. and H.C. Kim, "Six Human Factors to Acceptability of Wearable Computers", International Journal of Multimedia and Ubiquitous Engineering, 8(3), 2013, pp. 103–114.

[7] Choi, J. and S. Kim, "Is the smartwatch an IT product or a fashion product? A study on factors affecting the intention to use smartwatches", Computers in Human Behavior, 63, 2016, pp. 777–786.

[8] Chuah, S.H.W., P.A. Rauschnabel, N. Krey, B. Nguyen, T. Ramayah, and S. Lade, "Wearable technologies: The role of usefulness and visibility in smartwatch adoption", Computers in Human Behavior, 65, 2016, pp. 276–284.

[9] 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.

[10] Davis, F.D., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", MIS Quarterly, 13(3), 1989, pp. 319–339.

[11] Deutsch, M. and H.B. Gerard, "A study of normative and informational social influences upon individual judgment", The Journal of Abnormal and Social Psychology, 51(3), 1955, pp. 629–636.

[12] Dinev, T. and P. Hart, "An extended privacy calculus model for e-commerce transactions", Information Systems Research, 17(1), 2006, pp. 61–80.

[13] Dinev, T., A.R. McConnell, and H.J. Smith, "Research Commentary - Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box", Information Systems Research, 26(4), 2015, pp. 639–655.

[14] Fishbein, M. and I. Ajzen, Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison-Wesley, Reading, MA, 1975.

[15] Fornell, C. and D.F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", Journal of Marketing Research, 18(1), 1981, p. 39.

[16] French, J.R.P. and B.H. Raven, "The bases of social power", in Studies in social power, D. Cartwright, Editor. 1959. Institute for Social Research: Ann Arbor, MI.

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

[18] Garavand, A., M. Mohseni, H. Asadi, M. Etemadi, M. Moradi-Joo, and A. Moosavi, "Factors influencing the adoption of health information technologies: A systematic review", Electronic physician, 8(8), 2016, pp. 2713–2718.

[19] Gefen, D., "E-commerce: The role of familiarity and trust", Omega, 28(6), 2000, pp. 725–737.

[20] Gefen, D., E. Karahanna, and D.W. Straub, "Trust and TAM in online shopping: An integrated model", MIS Quarterly, 27(1), 2003, pp. 51–90.

[21] Gimpel, H., M. Niessen, and R. Goerlitz, "Quantifying the Quantified Self: A Study on the Motivations of Patients to Track Their Own Health", in Proceedings of the 34th International Conference on Information Systems. 2013, December. AIS: Milan, IT.

[22] Gotlieb, J.B. and D. Sarel, "The Influence of Type of Advertisement, Price, and Source Credibility on Perceived Quality", Journal of the Academy of Marketing Science, 20(3), 1992, pp. 253–260.

[23] Gu, Z., J. Wei, and F. Xu, "An Empirical Study on Factors Influencing Consumers' Initial Trust in Wearable Commerce", Journal of Computer Information Systems, 56(1), 2016, pp. 79–85.

[24] Henseler, J., C.M. 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.

[25] Higgins, J.P., "Smartphone Applications for Patients' Health and Fitness", The American journal of medicine, 129(1), 2016, pp. 11–19.

[26] Hu, L.T. and P.M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", Structural Equation Modeling: A Multidisciplinary Journal, 6(1), 1999, pp. 1–55.

[27] Jang, Y.K., Determinants of Users’ Intention to Adopt Mobile Fitness Applications: An Extended Technology Acceptance Model Approach: Unpublished PhD theses, Albuquerque, NM, 2014.

[28] Kalantari, M., "Consumers' adoption of wearable technologies: Literature review, synthesis, and future research agenda", International Journal of Technology Marketing, 12(3), 2017, pp. 274–307.

[29] Kim, K.J. and D.H. Shin, "An acceptance model for smart watches: implications for the adoption of future wearable technology", Internet Research, 25(4), 2015, pp. 527–541.

[30] Kokolakis, S., "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, 64, 2017, pp. 122–134.

[31] Lee, M., S. Rodgers, and M. Kim, "Effects of Valence and Extremity of eWOM on Attitude toward the Brand and Website", Journal of Current Issues and Research in Advertising, 31(2), 2009, pp. 1–11.

[32] Li, Y., "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework", Communications of the Association for Information Systems, 28, 2011, pp. 453–496.

[33] Liu, J., Y. Xiao, S. Li, W. Liang, and P. Chen, "Cybersecurity and Privacy Issues in Smart Grids", IEEE Communications Surveys & Tutorials, 14(4), 2012, pp. 981–997.

[34] 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.

[35] Metzger, M.J., "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce", Journal of Computer-Mediated Communication, 9(4), 2006, pp. 1–29.

[36] Mills, A.J., R.T. Watson, L. Pitt, and J. Kietzmann, "Wearing safe: Physical and informational security in the age of the wearable device", Business Horizons, 59(6), 2016, pp. 615–622.

[37] Mohamed, N. and I. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia", Computers in Human Behavior, 28(6), 2012, pp. 2366–2375.

[38] Nunnally, J.C., Psychometric theory, McGraw Hill, New York, NY, 1978.

[39] Palfrey, J.G. and U. Gasser, Born digital: understanding the first generation of digital natives, Basic Books, New York, NY, 2008.

[40] Park, S.Y., "An Analysis of the Technology Acceptance Model in Understanding University Students' Behavioral Intention to Use e-Learning", Educational Technology & Society, 12(3), 2009, pp. 150–162.

[41] Pavlou, P.A., "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology

Acceptance Model", International Journal of Electronic Commerce, 7(3), 2003, pp. 101–134.

[42] Pavlou, P.A., "State of the information privacy literature: Where are we now and where should we go?", MIS Quarterly, 35(4), 2011, pp. 977–988.

[43] Podsakoff, P.M., S.B. MacKenzie, J.Y. Lee, and N.P. Podsakoff, "Common method biases in behavioral research: A critical Rev of the literature and recommended remedies", Journal of Applied Psychology, 88(5), 2003, pp. 879–903.

[44] Prensky, M., "Digital Natives, Digital Immigrants Part 1", On the Horizon, 9(5), 2001, pp. 1–6.

[45] Reppel, A.E. and I. Szmigin, "Consumer-managed profiling: A contemporary interpretation of privacy in buyer-seller interactions", Journal of Marketing Management, 26(3-4), 2010, pp. 321–342.

[46] Salancik, G.R. and J. Pfeffer, "A Social Information Processing Approach to Job Attitudes and Task Design", Administrative Science Quarterly, 23(2), 1978, p. 224.

[47] Shin, D.-H., "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption", Interacting with Computers, 22(5), 2010, pp. 428–438.

[48] Smith, H.J., T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review", MIS Quarterly, 35(4), 2011, pp. 989–1016.

[49] Spiekermann, S., A. Acquisti, R. Böhme, and K.-L. Hui, "The challenges of personal data markets and privacy", Electronic Markets, 25(2), 2015a, pp. 161–167.

[50] Stewart, K.A. and A.H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument", Information Systems Research, 13(1), 2002, pp. 36–49.

[51] Stone, E.F. and D.L. Stone, "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms", Personnel and Human Resources Management, 8(3), 1990, pp. 349–411.

[52] Straub, D., M. Limayem, and E. Karahanna-Evaristo, "Measuring System Usage: Implications for IS Theory Testing", Management Science, 41(8), 1995, pp. 1328–1342.

[53] Sunyaev, A., T. Dehling, P.L. Taylor, and K.D. Mandl, "Availability and quality of mobile health app privacy policies", Journal of the American Medical Informatics Association: JAMIA, 22(1), 2015, 28-33.

[54] Tajfel, H. and J.C. Turner, "The social identity theory of intergroup behavior", in Psychology of intergroup relations, 2, S. Worchel and W.G. Austin, Editors. 1985. Nelson Hall: Chicago, IL.

[55] Taylor, S. and P. Todd, "Assessing IT Usage: The Role of Prior Experience", MIS Quarterly, 19(4), 1995, p. 561.

[56] https://help.runtastic.com/hc/de/articles/200484971-Teilen-von-Aktivit%C3%A4ten, accessed 8-16-2018.

[57] Thiesse, F., "RFID, privacy and the perception of risk: A strategic framework", The Journal of Strategic Information Systems, 16(2), 2007, pp. 214–232.

[58] Turner, J.C., Rediscovering the social group: A self-categorization theory, 1st edn., 1988.

[59] van Heek, J., A.K. Schaar, B. Trevisan, P. Bosowski, and M. Ziefle, "User requirements for wearable smart textiles: does the usage context matter (medical vs. sports)", in Proceedings of the 8th International Conference on Pervasive Computing Technologies for Healthcare. 2014, May. ICST: Oldenburg, GER.

[60] Venkatesh, V. and F.D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies", Management Science, 46(2), 2000, pp. 186–204.

[61] Venkatesh, V., M.G. Morris, G.B. Davis, and F.D. Davis, "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly, 27(3), 2003, pp. 425–478.

[62] Wood, W., "Attitude change: persuasion and social influence", Annual review of psychology, 51, 2000, pp. 539–570.

[63] Wu, L., J.Y. Li, and C.Y. Fu, "The adoption of mobile healthcare by hospital's professionals: An integrative perspective", Decision Support Systems, 51(3), 2011, pp. 587–596.

[64] Wu, L.H., L.C. Wu, and S.C. Chang, "Exploring consumers' intention to accept smartwatch", Computers in Human Behavior, 64, 2016, pp. 383–392.

[65] Xu, H., T. Dinev, H.J. Smith, and P. Hart, "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View", in Proceedings of the 29th International Conference on Information Systems. 2008, December. AIS: Paris, FR.

[66] Xu, H., S. Gupta, M. Rosson, and J. Carroll, "Measuring Mobile Users' Concerns for Information Privacy", in Proceedings of the 33rd International Conference on Information Systems. 2012, December. AIS: Orlando, FL.

[67] Xu, H., H.-H. Teo, and B.C.Y. Tan, "Predicting the adoption of location-based services: the role of trust and perceived privacy risk", in Proceedings of the 26th International Conference on Information Systems. 2005, December. AIS: Las Vegas, NV.

[68] Yang, H., J. Yu, H. Zo, and M. Choi, "User acceptance of wearable devices: An extended perspective of perceived value", Telematics and Informatics, 33(2), 2016, pp. 256–269.