Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

I Spy with my Little Sensor Eye - Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology.

Evgenia Princi
University of Duisburg-Essen
evgenia.princi@uni-due.de

Nicole C. Krämer
University of Duisburg-Essen
nicole.kraemer@uni-due.de

Abstract

The increasing number of smart objects in private households leads to a profound invasion of privacy. Based on privacy calculus theory, we assume that many users accept tracking in exchange for full functioning and convenience. However, privacy calculus has not yet been tested in an area where privacy protection is a binary decision: to either use a product or not. Therefore, we examined the effect of convenience and tracking on the intention to use a smart device in a 2 x 2 between-subjects online experiment (N = 209). While convenience is a major factor for the willingness to deploy smart technology, users do not seem to care whether these devices track their personal data or not.

1. Introduction

Today, smart technology is an inherent part of our everyday life. It is estimated that within a few years 100 billion smart devices will use the infrastructure of the Internet [1]. Data-tracking plays a key role regarding the efficiency of smart technology especially in contexts such as user-authentication and provision of personalized content [2,3].

Considering the high sensitivity level of personal information that can be accessed by smart devices, especially in private households, the omnipresent tracking is a controversial issue regarding data security and privacy [4,5]. Scandals on gadgets secretly spying on their owners and sale of user data are daily fare intensifying users' privacy concerns [6,7].

Nevertheless, the number of smart devices in private households is increasing [8] indicating that people weigh worries about their privacy against anticipated benefits of smart technology utilization. This is addressed by the *privacy calculus theory* [9] describing the trade-off between perceived risks and benefits of providing personal information. One of the major benefits of the deployment of smart technology in private households is its convenience. Therefore, intelligent technology is able to offer personalized services [10] to meet individual needs of users and provide them with the greatest possible comfort [11]. Furthermore, convenience is a relevant factor for users' acceptance of new technologies [12].

In order to provide convenience to consumers full functioning of smart devices has to be ensured. Smart technology can thereby simplify everyday tasks by saving users' time and effort with functions such as automated operating or usage of experience in order to improve performance. Collecting user data is a key element to the effectiveness of smart technology [13]. Concerning this matter, people differ in their attitudes towards tracking [7]. Youn [14] found that individuals experiencing more privacy concerns have a more negative attitude towards tracking.

However, the unobtrusive and inscrutable mode of operation makes it difficult for users to assess the entire spectrum of possible impacts. In many cases, there is no possibility for individuals to monitor the collection of their data leading to a lack of information about tracking practices [3]. Along with extended technical possibilities of smart technology, new research questions arise: how do users perceive being tracked and how do tracking methods affect users' attitude and especially behavioral intention towards deploying smart technology? Which explicit benefits can exceed the privacy risks? In this regard, there has been little scientific discussion on these topics.

This study aims to revisit the privacy calculus in order to investigate its applicability within the framework of the usage of smart technology. The vast gathering of data on the one hand and the lack of information leading to inestimable consequences for users on the other hand call into question, whether the traditional approach of the trade-off is adequate. For this purpose, in this paper we present an empirical study which focuses on the intention to use a smart device depending on its tracking capability and the provided convenience taking privacy concerns and the attitude towards tracking into consideration.

2. Theoretical framework

2.1. Consequences of tracking on user information disclosure

In the last few years, tracking of user-data has become more and more common. In general, tracking can be understood as an analytic procedure with a user-centric view where personal and

URI: https://hdl.handle.net/10125/63910
978-0-9981331-3-3

behavioral data are collected and aggregated to a detailed, person-specific profile [3,15]. A number of studies revealed that user behavior can be traced back even across multiple devices and that different websites pass on user information to third parties [7,15–17].

The Internet of Things (IoT) enables transboundary tracking beyond the virtual environment. Specifically, IoT-devices represent electronic gadgets usually equipped with multiple sensors (e.g. camera, motion sensors etc.), which are connected using various networks, and can to some extent operate autonomously [13,18]. In contrast to social network sites (SNS), information about users can be tracked even when they do not actively indicate or share data. This makes it almost impossible for people to identify tracking practices or to estimate how many of their data are tracked.

As for IoT, for the most part of smart technology tracking is fundamental in order to provide full functioning [13]. Thus, a smooth user experience and individually tailored services require many user data which might lead to people being worried about their privacy [4,5]. This is addressed by the *personalization-privacy-paradox* [19,20] stating that people in general profit from personalized services responding to their individual needs [21]. At the same time, personalized information and individually tailored services make users aware of how much of their personal data have been collected and analyzed [20] leading to privacy concerns.

Generally, privacy can be classified into four dimensions [22]. *Informational privacy* defines the individual's right to control the release of information about the self. *Social privacy* encompasses regulation and restriction of social relationships and interactions. *Psychological privacy* relates to one's thoughts and feelings. *Physical privacy* describes the accessibility of individual's physical space including surveillance and physical contact [22]. While research has tended to focus on informational privacy [2,23–25], IoT-tracking additionally applies to all four dimensions of privacy. Social privacy is compromised when IoT devices register interactions of users. This is the case when for example a smart monitoring system captures a conversation of employees at the workplace. Mood-detecting sensors are able to determine individual's emotions towards brands, which refers to psychological privacy. Finally, physical privacy is involved when IoT devices monitor user location, physiological factors or daily habits potentially exceeding the overall privacy violation. Furthermore, the inconspicuousness of tracking comprises a lack of transparency which makes it difficult for the user to react against the collection of his or her data.

Previous research reveals that people show reactance tendencies towards products and services requiring too much personal information [7,21]. This can be traced back to the universal and cross-cultural need for privacy [26,27]. Consequently, when the need for privacy is challenged by methods of data collection users could be expected to evade smart technology in order to preserve their privacy. Considering this fact, we proceed on the assumption that if individuals are pointed out to the advanced tracking functions of a smart device (e.g., motion tracking) their willingness to use it will decline. This leads to the first hypothesis:

Hypothesis 1 (*H1*)*:* Participants' intention to use a smart device will be lower if the device has tracking capability.

2.2. Privacy calculus and the benefit of convenience

For a number of studies, *privacy calculus theory* [9] is the basis of research [2,28]. Specifically, this theory refers to a weighing of risks and benefits individuals expect when providing personal information [24,28–30]. Wenninger, Widjaja, Buxmann, & Gerlach [31] have shown that users, despite existing privacy concerns, are willing to disclose private information for the free use of certain online services such as the social networks XING or LinkedIn. Similar results were reported by Krasnova, Spiekermann, Koroleva and Hildebrand [32]. In their study, the authors examined the role of the cost-benefit analysis for the disclosure of personal data on SNS and noted that users shared more personal information when expecting benefits (e.g., maintaining relationships). The perceived risks at the same time decreased information disclosure.

There have already been attempts at extending the privacy calculus theory traditionally assuming rational decision making with privacy as a tradable good. Kehr and colleagues [24] revealed that the assessment of risks and benefits is bounded by situational context, limited cognitive resources and heuristic thinking. However, in the context of tracking we argue that privacy calculus theory has again to be reconceptualized with regard to the specific field of smart technology deployment. Whereas SNS-users for example can vary the amount of disclosed information gradually calculating the level of risk, specific characteristics of data-tracking by smart devices call into question whether or not a calculation can take place. Weighing risks against benefits seems dispensable, if the risks cannot be reduced or if users do not know about them. As smart devices collect data without users actively disclosing it or being aware of the tracking the only decision left to the individual is to either use a smart device or not. For this reason, in this paper we suggest a new perspective for the privacy calculus as a binary decision.

Regarding the benefits of deploying smart technology, convenience by a number of studies is referred to as a crucial factor [33–35]. Brown [36] differentiates five convenience dimensions which in particular are time (i.e., device can be used at a time that is convenient for the user), place (i.e., device can be used in a place that is convenient for the user),

acquisition (i.e., the purchase of the device is convenient for the user), use (i.e., the handling of the device is convenient for the user) and execution (i.e., the usage of the device saves physical effort). Furthermore, in addition to innovation and efficiency, convenience is a distinctive feature of smart devices compared to their non-intelligent predecessors [5,18,37]. Examples for smart, convenience providing technology are smart phones managing our daily habits, intelligent loudspeakers ordering new detergents on command or smart robotic vacuum cleaners saving effort and time. Zheng and colleagues [8] confirm convenience as the driving force behind the usage of smart devices. To be more precise, the authors state that "user interests and values are ultimately what dictate privacy expectations, practices and norms" (p. 3) and that users prioritize perceived benefits, such as convenience and connectedness over privacy concerns. The authors justify their findings by claiming that people value certain benefits offered by smart devices more than having control over their data [7]. Moreover, in their study Yoon and Kim [12] postulate that perceived convenience is also related to individuals' acceptance and use of new technology. From this we derive our second hypothesis:

Hypothesis 2 (*H2*)*:* Participants' intention to use a smart device will be higher when the device promises convenience.

Considering the convenience of smart technology as a benefit within the privacy calculus, the privacy threat can be opposed as a risk. People want to deploy technology which provides convenience [12]. At the same time, the personalization-privacy-paradox [19,20] refers to the fact that the vast collection of data, which is necessary in order to provide convenience in the form of customized services and personalized information, is arousing skepticism and worries on behalf of users about their private information [7].

Consequently, those smart devices, which do not track and therefore minimize the risk for privacy will be perceived as the ideal choice when at the same time they will provide convenience. From this, we assume an interaction effect between the tracking capability and the convenience of a smart device leading to the following hypothesis:

Hypothesis 3 (*H3*)*:* Participants' intention to use a smart device will be highest when the device is convenient and has no tracking capability.

2.3. The impact of tracking on privacy

In the course of the digital age, privacy research changed perspectives due to the mass storage of user data and the partially unrestricted accessibility of private information potentially resulting in a large-scale invasion for privacy [38]. On that front the need for privacy [26,27] is particularly threatened by smart technology gathering, sharing and forwarding user data [17,39]. Due to various sensors smart devices are able to collect identifying information, analyze users' interactions with others and even track biological data as for instance blood-pressure or heart-rate (tracked with biosensors implemented in certain wearable devices) violating informational, social, psychological and physical dimensions of privacy [22].

An increasing number of studies investigated various constructs in relation to privacy. Regarding demographical variables, it has been suggested that women were more concerned about their privacy [40] whereas results on the perceptions of privacy concerns between older and younger users are contradictory [41].

In their study, Aguirre and colleagues [21] demonstrated that personalized content leads to customer discomfort making users realize that private information was collected without their consent. Correspondingly, tracking even with the purpose of providing customer-tailored services, in line with the personalization-privacy-paradox [19,20], can be perceived as privacy-intrusive leading to negative emotions [21] such as privacy concerns. Previous studies have shown that the capability of users to be always aware of their data being tracked is limited by distraction, cognitive capacity or lack of information [3,16,42]. However, when users assume to be an object of data collection without the possibility to control what data is being recorded and without having access to explicit information regarding the tracking they start worrying about their privacy [7]. As a consequence, privacy concerns might be pivotal for the willingness to use a smart device that is capable of tracking personal data on varying degree. From that derives our fourth hypothesis:

Hypothesis 4 (*H4*)*:* The effect of tracking capability on the intention to use a smart device will be moderated by privacy concerns.

2.4. Attitude towards tracking and users' intention to deploy smart technology

Prior research has shown that individuals differ in their attitudes towards tracking [7]. When people are ensured of confidentiality regarding the handling of personal data their attitude towards data collection is enhanced [43]. However, this concept seems to be constrained by something Sutanto and colleagues [20] call the *information limit* describing the amount of information gathering a user is willing to accept. Thus, it can be expected that when the information limit is reached, user's attitude towards tracking will decline. Due to the impenetrable practice of data-tracking people are worried about what personal information is being gathered by whom, where it is stored and how it is processed. We assume that distrust towards smart technology results in a negative attitude towards tracking reducing individual's intention to use a smart device. This leads to our last hypothesis:

Hypothesis 5 (*H5*): The effect of tracking capability on the intention to use a smart device will be moderated by the attitude towards tracking.

3. Method

First, a pretest with $N = 23$ participants aged 21 to 56 ($M = 26.74$, $SD = 7.09$) was conducted asking people to evaluate the convenience of smart devices from different categories and to indicate to what extent they would be worried about their privacy when using such a device (see Figure 1). Therefore, we generated three items asking participants for the convenience of the presented devices (e.g., "The following device makes my life easier") and another four items investigating privacy concerns regarding the different devices (e.g., "The following device is able to collect sensitive data about me") on a 5-point Likert-scale (from 1 = *I do not agree at all* to 5 = *I totally agree*). The pretest was conducted online. People were contacted via Email and different Facebook groups in order to ask them for participation. Participants were given no incentives. Based on the convenience dimensions formulated by Brown [36] and the results of the pretest smart household appliances (instead of smart phones, intelligent speakers and smart driver assistants) were chosen as possessing the optimal trade-off between perceived convenience and perceived privacy risks.

As a smart household device, a robotic vacuum cleaner compared to intelligent objects from other categories in the private environment causes less mistrust in users and, at the same time, ranked among household appliances was rated highly convenient. Smart vacuum cleaners work autonomously and can be operated via Internet. The user can define the best suitable time for the vacuum cleaner to start its work (time dimension) operating the device from anywhere without his/her attendance (place dimension). Due to the Internet connection of smart devices they can be centrally controlled (use dimension) and perform their work without physical effort on behalf of the user (execution dimension). Hence, we assume that a robotic vacuum cleaner corresponds to Brown's [36] requirements of convenience and therefore selected it to be implemented in the vignettes shown to participants in the main study.

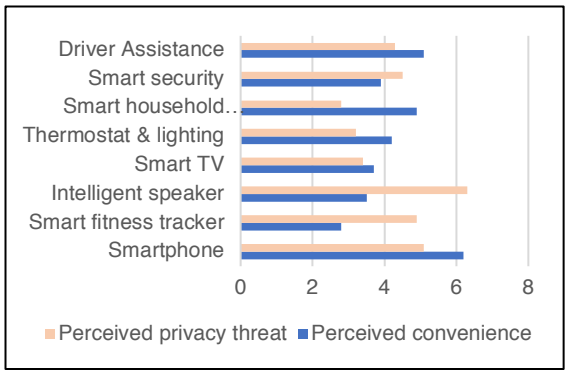

Figure 1. Perceived convenience and privacy threat of categories of smart devices in private households.

3.1. Sample and design

The study was conducted online. A total of 263 participants took part in the survey. In a first step, we filtered out participants who showed problematic response patterns (e.g., no variance in scales with reverse-coded items) and unreasonable reading times which we tested to be less than ten seconds per vignette resulting in an overall sample size of 209 individuals. The sample included 52 males and 157 females with an age range of 18 to 59 ($M = 27.49$, $SD = 6.95$). We employed a 2 x 2 between-subjects design manipulating the convenience and the amount of tracking of the smart device as shown in Table 1. Each of the four conditions included a different vignette describing a convenient/ inconvenient smart robotic vacuum cleaner with either intense or without any tracking capability. In order to present realistic versions of a smart vacuum cleaner the different features as well as their description were based on information from manufacturer websites (e.g., www.irobot.com) or on information usually provided by product packaging.

Table 1. Features of the presented versions of the robotic vacuum cleaner

Feature	*Convenient*	*Inconvenient*	*Intense tracking*	*No tracking*
Procedure	Efficient cleaning scheme	Chaos principle		
Change of movement direction	Automatically	After collision with other objects		
Charge	Autonomously	Plug in		
Technical service	Automatically	Manually		
Updates	Automatically	Manually		
Mapping				
App			Yes	No
Connectivity to other devices			Yes	No
Access on the way			Yes	No
Data analysis			Yes	No
Control			Voice, App	Touch
Registration			Yes	No
Dual-camera			Yes	No
Motion-detection			Yes	No

Table 2. Conditional effects of tracking on intention to use smart technology (moderated by privacy concerns)

Privacy concerns	*b*	SE_b	*95% CI*		*t*	*p*
One *SD* below mean	-.52	.23	-.972	-.07	-2.28	.024*
At the mean	-.15	.16	-.469	.169	-.93	.354
One *SD* above mean	.22	.23	-.231	.673	.96	.336

Note. $*p < .05$

Thus, tracking functions were named without particularizing what sensors are implemented, where collected data are stored or how they are processed.

3.1. Measures

The behavioral intention to use smart devices (*M* = 3.50, *SD* = 1.17) was assessed by the measurement from Moon and Kim [44] on a 5-point Likert-scale (from 1 = *I do not agree at all* to 5 = *I totally agree*) and consisted of three items (e.g., "I will enjoy using the smart robotic vacuum cleaner") plus an additional self-generated item asking whether participants could imagine using the presented robotic vacuum cleaner with α = .91. The measurements for perceived convenience (*M* = 3.90, *SD* = .94) on a 5-point Likert-scale (from 1 = *I do not agree at all* to 5 = *I totally agree*) were adapted from Yoon and Kim's study [12] which also established their reliability and validity. One example item is: "Using the smart robotic vacuum cleaner gives me convenience in performing my work". Internal consistency was excellent (α = 93). The primary function of the additional convenience scale was to serve as a manipulation check for the convenience in the conditions.

In order to assess participants' attitude towards tracking (*M* = 2.56, *SD* = .63) ten items were generated (e.g., "It makes sense to collect also non-anonymized data in order to provide full functionality of smart devices" or "User tracking should be forbidden categorically") on a 5-point Likert-scale (from 1 = *I do not agree at all* to 5 = *I totally agree*). The inventory was reduced due to a confirmatory analysis leading to a 4-item scale with α = .79, an average percentage of variation explained among items (AVE) of .52 and McDonald's omega of ω = .81.

Privacy concerns (*M* = 4.35, *SD* =.41) were assessed on a 5-point Likert-scale (from 1 = *I do not agree at all* to 5 = *I totally agree*) via 11 items (e.g., "I'm concerned that companies are collecting too much personal information about me") developed by Smith, Milberg and Burke [45]. Additionally, Malhotra, Kim and Agarwal's [46] three items for awareness of privacy practices (e.g., "It is very important to me that I am aware and knowledgeable about how my personal information will be used") and another three items for global information privacy concerns (e.g., "I am concerned about threats to my personal privacy today") were added to the scale (α = .86).

4. Results

All statistical analyses were computed using the statistics software *IBM SPSS Statistics 24*. In order to check for differences among the experimental conditions we computed a two-way analysis of variance (ANOVA). *H1* assumed that participants' intention to use a smart device will be lower if the device has tracking capability.

No significant differences could be found for participants' intention to use the smart device in the tracking and the non-tracking condition ($F(1, 205)$ = .81, p = .37, η^2 = .004). The intention to use the robotic vacuum cleaner did not depend on its capability to track user data. Therefore, *H1* has to be rejected.

Table 3. Conditional effects of tracking on intention to use smart technology (moderated by the attitude towards tracking)

Attitude towards tracking	*b*	SE_b	*95% CI*		*t*	*p*
One *SD* below mean	.19	.22	-.248	.632	.86	.39
At the mean	-.13	.16	-.435	.182	-.81	.42
One *SD* above mean	-.45	.22	-.883	-.007	-2.00	.046*

Note. $*p < .05$

Table 4. Bivariate correlations between convenience, attitude towards tracking, privacy concerns and the intention to use the smart device

	M (SD)	1.	2.	3.
1. Convenience	3.90 (.94)	-		
2. Attitude towards tracking	2.87 (.90)	.22**	-	
3. Privacy Concerns	4.35 (.41)	.03	-.48**	-
4. Intention to use	3.50 (1.17)	.69**	.26**	-.02

Note. $**p < .01$

With regard to *H2* our assumption that convenience increases the intention to use a smart device was confirmed because participants' willingness to deploy the device was significantly higher in the convenient condition than in the less convenient condition ($F(1, 205) = 6.84$, $p = .01$, $\eta^2 = .032$).

When the smart robotic vacuum cleaner was perceived as convenient participants had greater interest in using it. An additional regression analysis of the effect of perceived convenience on the intention to use the smart vacuum cleaner was highly significant ($b = .69$, $t(207) = 13.6$, $p < .001$) explaining 47% of the variance ($R^2 = .47$, $F(1, 207) = 184.85$, $p < .001$).

H3 suggested an interaction between convenience and tracking. The data does not support this assumption ($F(1, 205) = 1.94$, $p = .165$, $\eta^2 = .009$). The effect of convenience on the intention to use a smart device did not depend on its tracking capability.

Referring to *H4*, we have hypothesized a moderating effect of privacy concerns on the relationship between the amount of tracking and the intention to use a smart device. A moderation analysis was conducted using the PROCESS macro for SPSS [47]. Based on the findings of the moderated regression analysis *H4* can be accepted ($F(1, 205) = 5.24$, $p = .023$, $R^2 = .02$). The results indicate that the effect of tracking on the intention to use the robotic vacuum cleaner depended on users' privacy concerns. The interaction was probed by testing the conditional effects of privacy concerns (simple slopes) one standard deviation below the mean, at the mean, and one standard deviation above the mean. As shown in Table 2, the relationship between tracking and intention to use smart technology was significant when privacy concerns were one standard deviation below the mean ($p = .024$) but not when privacy concerns were at the mean ($p = .354$) or one standard deviation above the mean ($p = .336$).

Participants with lower privacy concerns had a higher intention to use the robotic vacuum cleaner with intensive tracking whereas participants with higher privacy concerns had a higher intention to use the smart device without tracking.

However, it should be noticed that the smallest value on the 5-point Likert privacy concerns scale was 3.12. Accordingly, the Johnson-Neyman significance zone ranged from 3.12 to 4.11.

Lastly, we tested the moderation effect of tracking attitude on the relationship between the amount of tracking and the intention to use a smart device (*H5*). As the items for the attitude towards tracking were generated for this study, we calculated a correlation between privacy concerns and attitude towards tracking. We found a significant relationship ($r = -.48$, $p < .01$) additionally validating the attitude towards tracking scale. Bivariate correlations between all constructs can be seen in Table 4. As with the prior moderator, the overall model was significant ($F(3, 205) = 6.46$, $p < .001$, $R^2 = .09$), revealing that the willingness to use a smart device depends on the effect of the attitude towards tracking on the relationship between the amount of tracking and the intention to use the device.

Simple slopes analysis showed that the relationship between tracking and the intention to use smart technology was significant when the tracking attitude was one standard deviation above the mean ($p = .046$) but not when privacy concerns were at the mean ($p = .42$) and one standard deviation below the mean ($p = .39$). The Johnson-Neyman significance zone ranged from 3.7 to 5. There is an interaction showing that the more positive people's attitude towards tracking is, the more likely they will accept tracking and be willing to use a smart device with a high amount of tracking. At the same time, participants with a more negative attitude towards tracking had a lower intention to use a device with high amount of tracking and a higher intention to use the device without tracking. Table 5 shows the proposed hypotheses with corresponding results.

5. Discussion

In this paper we examined the influence of data tracking on users' behavioral intention towards deploying smart technology capable of tracking. We further investigated the effect of convenience pledged by IoT technology.

Table 5. Overview of the proposed hypotheses

		Significance level	Result
H1	Participants' intention to use a smart device will be lower if the device has tracking capability.	.37	Rejected
H2	Participants' intention to use a smart device will be higher when the device promises convenience.	.01	Accepted
H3	Participants' intention to use a smart device will be highest when the device is convenient and has no tracking capability.	.165	Rejected
H4	The effect of tracking capability on the intention to use a smart device will be moderated by privacy concerns	.023	Accepted
H5	The effect of tracking capability on the intention to use a smart device will be moderated by the attitude towards tracking.	<.001	Accepted

Therefore, we conducted an online study where participants were presented different scenarios of a specific IoT device varying in its data tracking ability and convenience. Our findings show that people do not seem to care whether they are being tracked or not.
Even when provided with information regarding the ability of an IoT device to collect personal information there was no effect on the intention to use the respective device. This means that when purchasing smart household appliances individuals decide upon device deployment regardless of its potential privacy threat. One possible reason might be that subtle information about tracking capability of smart devices is not sufficient in order to raise the awareness of how many private data would be tracked and what consequences people could expect. In other words, people deploy smart technology knowing what functions and services they can get from it but even if informed that tracking takes place, they do not necessarily realize how many of their data are tracked in order to provide these functions. In our design, the description of the tracking features was short but was informed by real-world practices as provided by product packaging or manufacturer websites. In terms of ecologic validity, the vignettes therefore matched what we nowadays find in product descriptions.

In addition to the lack of information, Okazaki, Li and Hirose [48] argue that negative experiences of privacy violation lead to a stronger perception of risks which is why an underestimation of risks resulting from tracking could be attributed to participants' lack of negative experiences.

Another explanation might be that smart technology is in wide use and people do not always have a possibility to avoid being tracked eventually leading to a silent acceptance. The frequent exposure to collection of private data, as a consequence, could result in habituation decreasing users' attention towards risks [49].

Similarly, resignation might be causing indifference regarding the tracking ability of IoT devices. When people know that their data are ubiquitously collected online and by technology they deploy while at the same time they only have limited possibilities to protect their data they give up on it. In this context, Wirth and colleagues [50] showed that resignation has a positive effect on the perception of benefits and a negative effect on the perception of risks. Consequently, people who gave up on the protection of their data might deploy IoT devices with intense tracking capability regardless the potential privacy threat.

While the ability of the IoT device to collect personal data did not play a role in participants' intention to use it, according to our expectations, convenience was a crucial factor. Here, our findings demonstrate the importance of convenience of smart technology for its application in private households. This supports previous findings from Zheng and colleagues [8] who identified convenience as the driving factor in the usage of smart devices and substantiates the striving of manufacturers to create smart technology in a most comfortable way [11]. In their analysis, Yoon and Kim [12] revealed that convenience highly correlated with perceived usefulness of a smart device and that both factors are related to technology acceptance. Our work confirms these findings as convenience seems to be even more relevant for users than privacy.

Further, our findings show that when people perceive an IoT device as convenient they have a more positive attitude towards the collection of data. A positive attitude towards tracking, in turn, correlates with a higher intention to use the device. Thus, our results offer vital evidence for the attitude towards tracking to be a key determinant for the intention to use smart technology. When participants had a negative attitude towards tracking their willingness to use a smart device decreased with the intensity of its tracking capability. This corroborates the information limit [20] stating that gathering too much personal information can cause negative emotions. People who feel negative about tracking have more worries about their privacy and therefore, perceive higher risks when using smart technology. However, the more positive users' attitude is towards tracking, the higher is their intention to use a smart device with intense tracking capability. This could be due to users' demand for full functioning and personalized services which in turn require data. This means that users expect more benefits from devices that track their information. This result is worrying in the sense that users might disclose even more data when IoT devices are equipped with convenient features as a smooth user experience is preferred over privacy protection [51].

Regarding users' privacy concerns, this work has shown that worrying about one's privacy plays a central role in terms of deployment of smart technology. The results reveal that the more privacy concerns users experience, the lower is their intention to use a smart device with intense tracking capability. In this context, previous findings in the literature stated that the perceived violation of privacy can lead to negative emotions [21] and cause effects of reactance [7]. Considering the fact that smart technology is able to collect information as well as physical data, all dimensions of privacy [22] as well as the need for privacy [26,27] are compromised by tracking methods.

Taking privacy calculus into consideration, users weigh benefits they expect from an IoT device against the risks resulting from the collection of personal data in order to use this technology. In previous studies people decided to gradually change the amount of disclosed information as a result of this trade-off [32] or adjusted privacy settings [7]. This work showed that despite of the missing possibility to adjust privacy settings of a smart device people still performed the calculus between the perceived risks and benefits. The benefit of convenience significantly determined the intention to use a smart device. However, when people do not have the chance to gradually change the amount of disclosed information but still would like to use the services of the technology they rather decide to condone the data collection. Still, people´s prior attitudes in terms of existing privacy concerns reduced the intention to deploy the technology. Thus, our study confirms that privacy calculus can be adopted within the framework of the usage of smart technology and thereby extends this theory. However, users no longer take the decision what data to disclose. Smart devices and applications autonomously gather, forward and process private information without indicating it to the user, making privacy calculus in the context of smart technology deployment a binary decision: to either use a smart device or not. While users of SNS can vary the amount of information for every posting they want to disclose, users of smart appliances automatically provide all data the device is capable of tracking with the first use.

5.1. Implications

Our findings reveal the importance of providing users of smart technology with sufficient information in order to ensure awareness and self-determined decision-making. Only if people are informed about the existence and the mode of operation of tracking methods, they can estimate the potential risks. This is relevant for both data protection authorities and politics. In contrast to active disclosure of personal information, when deploying smart devices data are gathered automatically and unobtrusively in the background without any possibility for the consumer to see what information has been tracked, where it is stored and how it is processed. By means of directives, it could be achieved that manufacturers provide more detailed information about smart devices in a clear and easily accessible way. An example would be an information box on the product packaging allowing users to get an idea about what information could be accessed by a certain device before purchasing it. Further implications for research are that privacy calculus is a reliable basis for the investigation of smart technology in the context of data tracking and that more factors, such as resignation, should be taken into consideration when it comes to the risk-benefit trade-off of smart technology usage. It is, however, important to note that due to the heterogeneity of smart devices no general assumption can be made regarding privacy concerns or perceived convenience of different devices.

Implications for practice are that developers particularly need to emphasize convenience of IoT-devices in order for users to adopt and buy smart technology but at the same time to strengthen users' privacy by providing IoT-devices with privacy-protecting measures such as the possibility to change privacy settings or integrate privacy-by-design in the technology development process. This approach might contribute to higher trust and commitment of consumers demonstrating that their data are being handled responsibly.

As participants, contrary to our expectations, did not care whether they were being tracked or not, future studies might investigate the underlying processes. Also, the context of the deployment of IoT-devices (private environment or work) might give informative insights regarding the perception of privacy risks and anticipated benefits. Above all, further research needs to investigate the effect of data tracking under real circumstances in order to verify first results given by vignette studies.

5.2. Limitations

There are some limitations that should be noted concerning the methodology of this work. First, participants were asked to imagine themselves into a hypothetical situation which, by design, is limited in what it can cover. However, scenarios are important in terms of providing general understanding of the effect of IoT-tracking and allowing comparisons between different conditions. In order to present vignettes which are as realistic as possible, participants were presented detailed descriptions of the smart device including existing features of the vacuum robot. Due to the heterogeneity of IoT technology and the different characteristics of each device the general investigation of IoT devices from different categories (e.g., smart home, driving assistants etc.) seems problematic. For this reason, we focused on one particular device in our study and provided participants with different descriptions of a robotic vacuum cleaner from the category of household appliances. Further attention should be paid to the fact that no causal conclusion can be drawn, due to the cross-sectional character of the method. Another important note regarding this study is that convenience and tracking were varied independently of one another, which does not reflect reality because convenience of smart devices usually comes along with tracking and vice versa. Thus, our results do not provide insight into

what degree of convenience is required to fade out the tracking. Future studies could examine the graduation of both factors within the framework of the privacy calculus.

6. Conclusion

In this paper we have conducted an empirical study revisiting privacy calculus as a basis for the usage of smart technology. While the importance of convenience of smart technology was confirmed, contrary to our expectations there was no significant impact of data-tracking on the intention to use smart household appliances. However, when people were concerned about their privacy their intention to use an IoT device with intense tracking capability decreased. Further, we demonstrated that individuals differ in their attitude towards tracking and their willingness to use a smart tracking household device depended on their attitude towards data collection. Our results demonstrate that privacy calculus can be applied within the framework of smart technology as a binary decision resulting from the risk-benefit trade-off.

7. References

[1] C. Perera, S. Member, A. Zaslavsky, P. Christen, D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", IEE communications surveys & tutorials, IEE, pp. 414-454, 2014.

[2] T. Dinev, V. Albano, H. Xu, A. D'Atri, P. Hart, "Individuals' Attitudes towards Electronic Health Records: A Privacy Calculus Perspective", Advances in healthcare informatics and analytics, Springer, pp. 19–50, 2016.

[3] T. Ermakova, B. Fabian, B. Bender, K. Klimek, "Web Tracking-A Literature Review on the State of Research", Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, pp. 4732–4741, 2–6 January 2018.

[4] S. Trepte, P.K. Masur, "Privatheitsbedürfnisse verschiedener Kommunikationstypen on- und offline: Ergebnisse einer repräsentativen Studie zum Umgang mit persönlichen Inhalten", Media Perspektiven, pp. 250-257, 2015.

[5] B.D. Weinberg, G.R. Milne, Y.G. Andonova, F.M. Hajjat, "Internet of Things: Convenience vs. Privacy and Secrecy", Business Horizons, 2015, pp. 615-624.

[6] G. Hernandez, O. Arias, D. Buentello, Y. Jin, "Smart Nest Thermostat: A Smart Spy in Your Home", Black Hat USA, pp. 1-8, 2014.

[7] P.E. Ketelaar, M. van Balen, "The Smartphone as Your Follower: The Role of Smartphone Literacy in the Relation between Privacy Concerns, Attitude and Behaviour towards Phone-Embedded Tracking", Computers in Human Behavior, pp. 174–182, 2018.

[8] S. Zheng, M. Chetty, N. Feamster, "User Perceptions of Privacy in Smart Homes", Proceedings of the ACM on Human-Computer Interaction, pp. 200, 2018.

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

[10] J. Nolin, N. Olson, "The Internet of Things and Convenience", Internet Research, pp. 360–376, 2016.

[11] P. Gentsch, "Künstliche Intelligenz Für Sales, Marketing Und Service: Mit AI und Bots zu einem Algorithmic Business–Konzepte, Technologien und Best Practices", Springer Fachmedien Wiesbaden, Wiesbaden, 2018.

[12] C. Yoon, S. Kim, "Convenience and TAM in a Ubiquitous Computing Environment: The Case of Wireless LAN", Electronic Commerce Research and Applications, pp. 102–112, 2007.

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

[14] S. Youn, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents", Journal of Consumer Affairs, pp. 389-418, 2009.

[15] S. Zimmeck, S.M. Bellovin, T. Jebara, J.S. Li, H. Kim, "A Privacy Analysis of Cross-Device Tracking", 26th USENIX Security Symposium, Vancouver, BC, Canada, pp. 1391-1408, 16-18 August 2017.

[16] D. Arp, E. Quiring, C. Wressnegger, K. Rieck, "Privacy Threats through Ultrasonic Side Channels on Mobile Devices", IEEE European Symposium, pp. 35-47, 2017.

[17] J. Brookman, P. Rouge, A. Alva, C. Yeung, "Cross-Device Tracking: Measurement and Disclosures", Proceedings on Privacy Enhancing Technologies, pp. 133–148, 2017.

[18] F. Mattern, C. Floerkemeier, "From the Internet of Computers to the Internet of Things", From active data management to event-based systems and more, Springer Verlag, Berlin, Heidelberg, pp 242–259, 2010.

[19] N.F. Awad, M.S. Krishnan, "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization", MIS quarterly, pp. 13-28, 2006.

[20] J. Sutanto, E. Palme, C.H. Tan, C.W. Phang, "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users", MIS Quarterly, pp. 1141–1164, 2013.

[21] E. Aguirre, D. Mahr, D. Grewal, K. de Ruyter, M. Wetzels, "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness", Journal of Retailing, pp. 34–49, 2015.

[22] J.K. Burgoon, "Privacy and Communication", Annals of the International Communication Association, pp. 206–249, 1982.

[23] A. Acquisti, "Nudging Privacy: The Behavioral Economics of Personal Information", IEE security & privacy, pp. 82–85, 2009.

[24] F. Kehr, T. Kowatsch, D. Wentzel, E. Fleisch, "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus", Information Systems Journal, pp. 607–635, 2015.

[25] T. Dienlin, S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors", European Journal of Social Psychology, pp. 285–297, 2015.

[26] I. Altman, "Privacy Regulation: Culturally Universal or Culturally Specific", Journal of Social Issues, pp. 66–84, 1977.

[27] N.J. Marshall, "Dimensions of Privacy Preferences", Multivariate Behavioral Research, pp. 255–271, 1974.

[28] T. Dinev, P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions", Information system research, pp. 61–80, 2006.

[29] R.K. Chellappa, R.G. Sin, "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma", Information Technology and Management, pp. 181-202, 2005.

[30] H. Xu, X.R. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing, Decision support systems, pp. 42-52, 2011.

[31] H. Wenninger, T. Widjaja, P. Buxmann, J. Gerlach, "Der Preis Des Kostenlosen", Wirtschaftsinformatik & Managment, pp. 12–19, 2012.

[32] H. Krasnova, S . Spiekermann, K. Koroleva, T. Hildebrand, "Online Social Networks: Why we Disclose", Journal of Information Technology, pp. 109–125, 2010.

[33] R.B. Kvavik, "Convenience, Communications, and Control: How Students Use Technology", Educating the net generation, pp. 83–102, 2005.

[34] C. Phelan, C. Lampe, P. Resnick, "It's Creepy, But It Doesn't Bother Me", Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM Press: New York, New York, USA, pp 5240–5251, 2016.

[35] S. Spiekermann, J. Grossklags, B. Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior", Proceedings of the 3rd Annual ACM Conference on Electronic Commerce, Tampa, FL, USA, New York: ACM, , pp. 38–47, 14–17 October.

[36] L.G. Brown, "Convenience in services marketing", Journal of Services Marketing, pp. 191–214, 1990.

[37] T. Hargreaves, C. Wilson, R. Hauxwell-Baldwin, "Learning to Live in a Smart Home", Building Research and Information, pp. 127–139, 2018.

[38] P. Grimm, H. Krah, " Ende Der Privatheit. Eine Sicht der Medien- und Kommunikations-wissenschaft", Forschung und Lehre, 2014.

[39] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective", IEEE Internet Things Journal, pp. 349–359, 2014.

[40] K.B. Sheehan, "An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors", Journal of Interactive Marketing, pp. 24–38, 1999.

[41] E.-M. Zeissig, C. Lidynia, L. Vervier, A. Gadeib, M. Ziefle, "Online Privacy Perceptions of Older Adults", International Conference on Human Aspects of IT for the Aged Population, Springer, pp. 181–200, 2017.

[42] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, C. Diaz, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 674–689, 2014.

[43] C.H. Lee, D.A. Cranage, "Personalisation–Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites.", Tourismus Managment, pp. 987–994, 2011.

[44] J.W. Moon, Y.G. Kim, "Extending the TAM for a World-Wide-Web Context", Information and Manament, pp. 217–230, 2001.

[45] H.J. Smith, S.J. Milberg, S.J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", MIS quarterly, pp. 167–196, 1996.

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

[47] A.F. Hayes, "Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach", Guilford Press: New York, NY, US, 2013.

[48] S. Okazaki, H. Li, M. Hirose, "Consumer Privacy Concerns and Preference for Degree of Regulatory Control", Journal of Advertising, pp. 63–77, 2009.

[49] V. Venkatesh, J.Y. Thong, X. Xu, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology", MIS quarterly, pp. 157-178, 2012.

[50] J. Wirth, C. Maier, S. Laumer, "The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis.", ECIS 2018 Proceedings, 2018.

[51] S. Athey, C. Catalini, C.Tucker, "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk", National Bureau of Economic Research, 2017.