Abstract
With the rapid development of the Internet of Things, intelligent systems are increasingly finding their way into everyday life and into people’s homes. With the spread of these technologies, there is a growing concern about what sensitive data is collected and what it is used for. Unfortunately, the role of privacy has remained largely unexplored in the smart home (SH) usage context. This study addresses this gap in literature: to what extent users’ concerns for information privacy influence the intended SH usage. This study takes an interactional psychology perspective and links the dimensions of the privacy concerns to the intention to use SH devices. Therefore, a multi-theoretical model using Smart PLS 3.2.8 was tested. This study contributes to the literature on privacy, and SH usage by exploring how and why privacy concerns influence participants’ intended SH usage. The findings, derived from the empirical study emphasize the importance of addressing privacy concerns because they are capable of directly and indirectly influencing the intended SH usage. Finally, the results which indicate new directions for privacy and SH research are discussed and implications for research and practice are given.

Keywords Privacy concerns · Smart home technologies · Technology acceptance · Theory of planned behavior · Structural equation modelling

1 Introduction
The fusion of the physical and digital world in the Internet of Things (IoT) has significant effects on the design of residential spaces and the convenience and efficiency in daily life [1]. Intelligent appliances in the home are no longer operated separately and locally. Increasingly, domestic appliances are mutually connected via information and communication technology, resulting in the emergence of smart homes (SH). Sensors, network connections and applications build an intelligent and interactive architecture aiming at increasing efficiency of everyday tasks and improving safety of homes and the people living in them [2]. A rising importance for SH environments with the potential to become an essential installation for everyday life is proposed by other studies [3].

The diffusion of mobile networks and the growing popularity of smart devices and intelligent systems lead to rapid growth of the business segment. While the global market for SH services was estimated at $38.50 billion in 2017, it is forecasted to increase up to $125.07 billion until 2023. By that time, the global market penetration is expected to be 19.5% [4]. Despite the positive prospects for the spread of SH technologies in the future, the adoption of SH seems doubtful [5]. An important reason may be the still very fragmented market, where many SH technologies are not yet mature and standardization is not
yet in place to ensure interoperability between different manufacturers.

Nevertheless, a major obstacle to adoption is the nature of the technology that gives rise to new concerns about information privacy [6]. An editorial in the Information Systems Journal stated that “recent technological changes are generating additional privacy challenges beyond the existing landscape” [7, p. 575]. SH devices make use of various sensing technologies to provide services. These sensors collect vast amounts of data, which are processed and analyzed to provide a service to the users. This collection of personal data in combination with the increasing deployment of internet-connected devices in the home exposes residents to new privacy and security risks. According to this, privacy concerns could represent a potential barrier to the adoption of SH devices. Therefore, we aim to identify relevant privacy concerns of potential users in connection with the use of SH devices and to investigate whether these have a significant influence on the acceptance of this particular technology. While studies on user acceptance and on the behavior of potential customers are of great importance for successful acceptance and diffusion in the market, little research has been done on this topic. Rather, the majority of scientific work in the context of SH has a technological background [8]. Users’ worries resulting from these dangers and their influence on technology acceptance remained largely unconsidered. Especially the construct of privacy concerns has not yet been part of scientific research on this topic. Consequently, influences of the diffusion and adoption of SH technologies have not been adequately addressed. This study at hand seeks to get a deeper insight into the critical success factors of smart devices in households against the background of information privacy concerns. Consequently, we aim to provide deeper insight into the issue by answering the following research question:

**RQ** How do users’ concerns for information privacy influence the intention to use SH devices?

We discuss the concept of privacy concerns for the application of SH devices and instruments measuring information privacy concerns and user acceptance. Hypotheses are derived and a conceptual model is developed that links these privacy concerns to the intention to use SH devices taking into account critical influencing factors of the technology acceptance model (TAM) and the theory of planned behavior (TPB) as antecedents for to intention to use. Then, the methodology is described. After that we report the data analysis results. Discussion and implications for research and practice are presented in the sixth section, followed by identifying limitations and providing an outlook for further research.

## 2 Theoretical foundation

### 2.1 SH and related literature

Advances in ubiquitous computing have promoted the development of SH systems. This fact and the reality that technological innovations are making smart devices cheaper and more available have given a boost to the IoT trend [9]. The SH as a result of this trend unites a multitude of devices from the IoT-area in itself. SH technology is the application of IoT-technology in the residential environment [3]. There is no uniform definition for the term SH, but rather the definition is based on the respective application. According to Aldrich [10, p. 17] a SH can be defined as “[…] a residence equipped with computing and information technology which anticipates and responds to the needs of the occupants […]” By the extension “smart or intelligent”, the system (the “house” in our case), is able to give tailored assistance for the users [11]. In this study we define SH according to [12] as a residence “equipped with a high-tech network, linking sensors and domestic devices, appliances and features that can be remotely monitored, accessed or controlled, and provide services that respond to the needs of its inhabitants”. These advanced user assistance systems help inhabitants to fulfil different tasks and provide (intelligent) assistance [13]. Essentially, these SH devices provide services in three areas: security, energy management, healthcare and lifestyle support [12].

The number of application areas in the SH context, as well as the vast amount of elements working together in a SH raises users privacy concerns. Because users know about the value of their personal data, they have an increased concern for privacy invasion and data misuse. Past research about SH and the usage of their services marked the importance on the awareness of privacy concerns, sometime linked to security issues (e.g., [14, 15]). Studies explored, for example, importance of a safe usage of personal health data from the users [16]. From a more technical perspective, other researchers propose web services in order to raise SH user’s privacy [17], encryption methods for preserving SH data privacy [18] or gateway architectures enhance users’ privacy [19]. Other studies explored privacy hazards directly connected to the usage of an IoT based SH because of the networks between mobile devices of the users and SH infrastructure, like doors or windows (e.g., [2]).

### 2.2 Privacy and technology acceptance

As described before, complexity of privacy is a relevant aspect in a SH context and is also presented as
a potential barrier for SH usage [20]. Due to the rapid technological development and diversity of applications, there is a need to develop increasingly precise models for measuring information privacy concerns [21]. The most prominent models in current research literature are the Concern for Information Privacy (CFIP), the Internet Users’ Information Privacy Concerns (IUIPC) and the Mobile Users’ Information Privacy Concerns (MUIPC) model, which serve as one of two theoretical pillars for our research model.

Since the Internet offers a multitude of possibilities for collecting, evaluating and storing various user data, [22] developed the IUIPC on the basis of the CFIP proposed by [23] for the online context. The expansion of the Internet and related technologies has implications for the privacy concerns of users. The possibilities offered by the Internet allow users to control what information is stored in the databases of companies [22]. On the other hand, users can no longer perceive exactly when and by whom data is collected as in an offline context. The MUIPC was developed by [24] with the purpose to measure privacy concerns in the context of mobile applications. Like the IUIPC, the MUIPC is based on the CFIP. The model MUIPC measures the privacy concerns of mobile users based on the following three dimensions: perceived intrusion, perceived surveillance, and secondary use of personal information [24]. Following [25], mobile devices differ from other technologies because of the usage of environmental sensors, like integrated cameras. These sensors have the advantage to enhance mobile users’ tasks, but raises privacy concerns on the other hand.

The literature points to a considerable research interest in topics related to online privacy. The different measurement models were often combined with some consumer behavior models to investigate the influence of privacy concerns on the behavior of individuals (e.g., [26]). In particular, the TAM and the TPB were extensively used to examine the influence of privacy concerns on behavioral intention and were used as a second theoretical pillar in this study of SH usage and privacy concerns. The TAM was developed by [27] to explain and predict the use of information systems by individuals. The underlying assumption of the model is that the characteristics and capabilities of a technology influence the motivation to use it. This motivation, in turn, can be used to predict the use of the technology [28]. The model originally consisted of three factors: perceived usefulness (PU), perceived ease of use (PEOU) and attitude (A). The final version of the TAM by [29] the attitude factor was discarded and replaced by behavioral intention as proxy for actual use. The TAM is used both in its original form and often in combination with other models such as the TPB. Research shows that the integrated use of TAM and TPB increases the explanatory and predictive power on the intention to use information systems [30].

The TPB was developed by [31], by means of this model the constructs attitude, subjective norm and perceived behavioral control (PBC) and their influence on behavioral intention are investigated. Compared to the theory of reasoned action (TRA) [32], it has a further determinant of behavioral intention, which is PBC. This variable examines an individual’s perception of whether performing a behavior is easy or difficult based on internal and external limitations [31]. Moreover, it is the degree over which individuals have limited volitional control over their behavior [30]. The attitude represents an evaluation of an individual towards a behavior as favorable or unfavorable regarding the consequences of the behavior [30]. The social pressure to perform or not to perform a specific behavior is represented by the variable subjective norm [30].

3 Hypothesis generation and research model

The proposed research model aims to examine the way privacy concerns influence the use of SH devices. The basic premise is that the more users see their privacy endangered, the lower the intention to use SH devices. It is essential for companies to understand what factors lead individuals to consider the use of their products or what hinders individuals to use products and services. Because with this knowledge they can adapt to customer needs. To study the acceptance of complex IS that are different from conventional IT, [33] propose to include TPB to provide a more comprehensive theoretical perspective of user acceptance. This extension is supposed to provide a higher explanatory power to understand the adoption of SH devices. [34] support this hypothesis as they state that the TPB outperforms other acceptance models in the context of technology adoption decisions in the household. Figure 1 depicts our research model.

The construct of PU is defined as an individual’s belief that the use of a technology increases one’s own performance [27]. The TAM model generally identifies the PU of a technology as a mediator in the relationship between external variables such as beliefs and perceptions, and intentions [35]. Therefore, beliefs are the information an individual has about some object [31]. Thus, the privacy concerns can be interpreted as beliefs about the awareness of a SH service. This leads to the assumption that the PU might be influenced by beliefs about privacy concerns of the respective SH service [35]. Regarding this, the usage of a SH service could cause that a user perceives a high level of intrusiveness by providing personal information. If the user does not believe that the SH service is private, the
individual may be less prepared to recognize the usefulness of the service or technology [36]. According to [27], individuals with a high degree of privacy concerns are expected to have a psychological burden that negatively affects their belief in utility. Hence, it is hypothesized that the PU influences the intention to use SH devices—with the perceived privacy concerns as its precursor.

**H1** Privacy concerns are negatively associated with the perceived usefulness of SH devices.

PU originally referred to productivity, performance and effectiveness perceived using the respective technology [27]. Many studies on technology acceptance showed that the perceptions of usefulness have a direct positive influence on intentions to use a technology in the course of various environments and different influencing factors (e.g., [37]). Reasons that motivate individuals to use SH systems are support in daily tasks and routines, the creation of security, increased energy efficiency or entertainment. In general, the systems can be seen as support for enhancing effectiveness and efficiency. Therefore, we propose the following hypothesis:

**H2** Perceived usefulness is positively associated with the intention to use SH devices.

The TPB explains behavioral intention as the most important determinant of individuals’ behavior. It involves situations in which one does not have complete control over one’s own behavior and uses the construct of PBC for this purpose. The influence of privacy concerns on the dimensions of PBC has not yet been the subject to scientific research. PBC is defined as an individual’s behavior over which people have limited volitional control [31]. In particular, PBC represents internal and external limitations when performing certain activities [5]. Therefore, it is supposed that privacy concerns have an impact on the internal limitations a potential user encounters while deciding whether to adopt SH technology.

**H3** Privacy concerns are negatively associated with the perceived behavioral control.

Several empirical studies have found a relationship between PBC and intention (e.g., [5]). [38] found that PBC was positively related to the behavioral intention in terms of IT usage. Furthermore, research showed that PBC has a positive influence on the use of mobile data services [38]. [39] applied the TPB on smart meter adoption and found evidence for a positive relationship between PBC and intention to use. In this study, PBC refers to the perception of a potential user about the difficulty and barriers in adopting SH devices. As mentioned by [40], it can be assumed that higher users’ beliefs about their ability to interact with SH devices and the absence of barriers to use this technology, leads to a greater control over the use of SH devices. Thus, we propose the following hypothesis:

**H4** Perceived behavioral control is positively associated with the intention to use SH devices.

In early stages of diffusion of technologies, people lack information to decide whether or not to adapt them. As
a consequence, the adoption decision of a potential user may be influenced by others’ opinions within his/her social system [41]. This social element of the decision on technology acceptance is mapped in the TPB via the construct “subjective norm” [32]. Subjective norm refers to a person’s assessment on how people important to him/her relate to the question of whether he/she should carry out the behavior in question [32]. Since people tend to surround themselves with people who share similar views, it is assumed that with a higher level of concerns about information privacy of a potential user, people around them are more likely to reject the acceptance of SH devices. Consequently, we propose the following hypothesis:

H5 Privacy concerns are negatively associated with subjective norms.

The more an individual perceives that their significant individuals support the behavior in question, the greater the motivation to meet their expectations. Acting according to the expectations of how others expect one to behave is known as the perceived prevalence effect [42]. Consequently, it can be presumed that the attitudes of affiliated people towards SH devices have an influence on the individual’s intention to use them. Therefore, we propose the following hypothesis:

H6 Subjective norms are positively associated with the intention to use SH devices.

A common definition for information privacy is “one’s ability to control information about oneself” [21]. With the advancement of digital technologies, it becomes more difficult to guarantee this ability. Especially in the context of SH, in which a vast amount of data is needed to perform adequately to users’ expectations, there is a high potential for violation of privacy. Thus, SH services are perceived to be risky, which in turn creates information privacy concerns. In this context, privacy concerns represent an individual’s generalized concerns about how organizations collect, store, and use personal information. Numerous studies have handled the construct of privacy concerns as an antecedent to different behavior related aspects, e.g., the willingness to disclose personal information and intention to transact. The negative effect of privacy concerns on the intention to use has been empirically proven in a large number of empirical studies and a variety of topics, e.g., e-commerce [43] and health wearable devices [44]. If users get worried not to be able to control information about themselves, they will ensure that the risk of invasion of privacy is minimized. With regard to SH devices it could lead to individuals avoiding the use of SH devices. Therefore, the following hypothesis is proposed:

H7 Privacy concerns have a negative impact on the intention to use SH devices.

4 Research methods

4.1 Research design and data collection

Given the research goals, we chose to use an anonymous self-reported survey for data collection. Participation was voluntary and the participants were guaranteed anonymity. Furthermore, we used multivariate analysis methods to test the underlying model statistically, which is proposed by other researchers as a well-accepted approach [45]. As mentioned by [45], a substantial volume of IS research has used studies that involve self-reported behaviors, in different contexts (e.g., [46]). Furthermore, non-probabilistic sampling was used for data collection. This type of sampling is used when it is difficult to find a sample based on pure chance [47]. In this case it is used due to lack of information about the population, in order to select a representative sample. The survey questionnaire was distributed via social media platforms, e.g., Facebook, Xing, and LinkedIn in order to recruit participants through announcements. No monetary or comparable incentive was given to answer the survey. The posting provided a cover letter, which stated the objective of the study and also included the link to the survey questionnaire as well as the explanation of the data handling procedure. The time needed to complete the questionnaire was indicated as 5–8 min. As the group of potential SH users is not limited by obvious reasons due to the diversity of the technology, we have not excluded any groups from the sample. Therefore we included both, current users and people who reject SH in the survey. A total of 236 responses were collected. Out of these 236 respondents, 49 participants (21%) did not finish the survey and thus, the results could not be used and the data was removed from the data set. Consequently, \(n = 187\) results (79%) of the questionnaires could be used for our analysis. The gender distribution of the sample was 100 males and 79 females, and 8 participants did not provide any information. Age, Income, Education, and branch of industry details for the sample are reported in Table 1.

In the first part of the questionnaire, participants were asked to respond to the privacy items according to their subjective perceptions in the context of using SH devices. Therefore, the 3 dimensions of the MUIPC, namely, perceived surveillance, perceived intrusion, and secondary use of information, 1 dimension of IUIPC, namely, awareness of privacy practices, 2 dimensions of the TAM, namely, PU intention to use, and 1 dimension of the TPB, namely, subjective norms were measured using a 5-point
rating scale, which ranged from 1 “strongly disagree” to 5 “strongly agree”. Online Appendix S1 provides the full details of the items and questions.

Because the data were self-reported, we used several approaches to prevent common method bias [a.k.a., common method variance (CMV)] ex ante in the research design stage (e.g., counterbalancing the order of the questions, presenting the survey items in a random manner, and adapting the measurement items for the independent and dependent constructs from different previously validated studies) and ex post after the research has been conducted. Given our care in survey design and based on our analysis, CMV in our model is not likely (compare Online Appendix C).

4.2 Operationalization of variables and measurement

For our survey instrument, we adapted items from existing research literature for all latent constructs wherever possible. Before we started with the survey, we conducted a comprehensive preliminary analysis. We adapted items from most closely related scale and changed the wording to fit into the context of SH. In a first step, we employed a panel of four experts (two professors and two doctoral students) to evaluate the questions. To ensure that the questions (indicators) reflected the intent of the study, we provided the panel with the indicators for the purpose intended. Their comments on the questions (e.g. on the clarity/phrasing, the ordering, and the appropriateness of the indicators) were then compiled and evaluated. This process to increase content validity led to refinement of the items, including dropping a few indicators and rephrasing [minor grammatical changes were made for the scales from the TPB and the TAM (Table A1)] and therefore also increase the clarity and conciseness of the survey questions.

After examining the relationship between each construct and each associated indicator in our research model, we found that the overall constructs to be reflective because of the covariation among the indicators, the direction of the causality, the interchangeability of the indicators as well as the nomological net of the constructs, which should not vary [48]. According to [24], the structure of the MUIPC is represented more concise as a hierarchical component model than as a first-order model. Following these arguments, we conceptualize MUIPC as a second-order (hierarchical component model) because it is substantively meaningful, theoretically sound, operationally convenient, and empirically justified. “This higher-order abstraction is justified because if all items are bundled together, the explanation of the resultant construct is incomplete (…) and the contributions of various content domains to the final scale score will not be known (…)” [52]. Overall, the approach chosen here reduces the complexity of the model and leads to more parsimony, which makes it easier to grasp [49]. By enabling the collection of complex concepts in comparatively simple abstractions, multidimensional higher-order constructs, such as second-order constructs, provide opportunities for advancing research [50] and increase the realism of empirical models [51].
5 Data analysis and results

We applied partial least squares structural equation modeling (PLS-SEM) to analyze our empirical data. As mentioned by [52] the use of PLS-SEM has increased exponentially in a variety of disciplines. Depending on the objective of the respective researchers, PLS path modeling can be used either for explanation or prediction purposes [56]. Our analysis focuses on explanatory/confirmatory modeling. We have therefore used the proposed PLS approach, which offers a broad flexibility and scope for theory and practice [53]. In contrast to maximum likelihood (ML)-based covariance-based SEM approaches, the evaluation of the structural and measurement model in PLS-SEM is based on a number of nonparametric evaluation criteria [49, 52] and PLS-SEM is more suitable for unestablished models or preliminary model building [66]. The use of PLS-SEM has several advantages, e.g., when sample sizes are small, with less normalized data, or when complex models with many items and relationships are estimated [49]. Furthermore, it permits simultaneous testing of the measurement model and the estimation of the structural model [24] and provides a broad scope and flexibility for practice and theory [53]. Measurement validation and model testing were conducted using a two-step approach with the SmartPLS/-Version 3.2.8 software [54]. The two-step approach involves the structural model and a separate assessment of the measurement models [49]. To analyze the reflective–reflective hierarchical latent construct “privacy concerns”, we applied the repeated indicator approach. The advantage of this approach is that it considers both the higher and lower-order components as well as the entire nomological network. Instead of estimating all the dimensions individually, this approach allows estimating all constructs simultaneously [55]. Before testing the hypotheses, we evaluated the validity and reliability of the construct measures. As reliability is a necessary condition for validity, this aspect was examined first. To ensure indicator reliability, we examined the loadings of each indicator relative to their respective underlying construct (compare Table B.1. and B.2.). In our study, we found that all the outer loadings of the reflective constructs are significant (min. T-value 13.742–max. T-value 112.726) and well above the threshold value of 0.70 (Table 2).

Table 2 Results of the measurement assessment

| Construct                       | Construct indicator | Convergent validity | Internal consistency reliability | Discriminant validity |
|---------------------------------|---------------------|---------------------|---------------------------------|----------------------|
|                                 |                     | Loadings | t-statistics | Indicator reliability (>0.50) | AVE (>0.50) | Composite reliability (>0.70) | Cronbach’s alpha (>0.60) | HTMT (confidence interval does not include 1) |
| Secondary use of personal info (SUoP) | SUoPI_1             | 0.935 | 72.311 | 0.874 | 0.859 | 0.948 | 0.918 | Yes |
|                                 | SUoPI_2             | 0.927 | 52.748 | 0.859 |                |
|                                 | SUoPI_3             | 0.919 | 54.596 | 0.845 |                |
| Perceived surveillance (PS)     | PS_2                | 0.917 | 98.467 | 0.841 | 0.753 | 0.859 | 0.682 | Yes |
|                                 | PS_3                | 0.816 | 16.935 | 0.666 |                |
| Perceived intrusion (PI)        | PI_1                | 0.879 | 50.081 | 0.773 | 0.780 | 0.914 | 0.859 | Yes |
|                                 | PI_2                | 0.885 | 49.795 | 0.783 |                |
|                                 | PI_3                | 0.885 | 48.385 | 0.783 |                |
| Awareness of privacy practices (AoPP) | AoPP_1            | 0.792 | 14.976 | 0.627 | 0.629 | 0.835 | 0.705 | Yes |
|                                 | AoPP_2             | 0.851 | 24.775 | 0.658 |                |
|                                 | AoPP_3             | 0.732 | 13.742 | 0.534 |                |
| Perceived usefulness (PU)       | PU_1                | 0.809 | 30.411 | 0.654 | 0.797 | 0.940 | 0.914 | Yes |
|                                 | PU_2                | 0.915 | 52.698 | 0.837 |                |
|                                 | PU_3                | 0.917 | 58.011 | 0.840 |                |
|                                 | PU_4                | 0.925 | 64.958 | 0.856 |                |
| Perceived behavioral control (PBC) | PBC_1              | 0.930 | 73.796 | 0.865 | 0.816 | 0.898 | 0.778 | Yes |
|                                 | PBC_2              | 0.875 | 25.888 | 0.766 |                |
| Subjective norms (SN)           | SN_1                | 0.937 | 71.637 | 0.878 | 0.873 | 0.932 | 0.855 | Yes |
|                                 | SN_2                | 0.932 | 63.479 | 0.869 |                |
| Intention to use (ItU)           | ItU_2               | 0.944 | 88.727 | 0.891 | 0.899 | 0.947 | 0.888 | Yes |
|                                 | ItU_4               | 0.953 | 112.726 | 0.908 |                |
The item AoPP.3 has the smallest indicator reliability, with a value of 0.53 (0.732²), while the indicator ItU.4 has the highest indicator reliability, with a value of 0.91 (0.953²). We assessed the reflective measurement models with regard to their validity and internal consistency reliability. First, we considered the composite reliability as a means of assessing the internal consistency reliability (ICR). According to [56], the reliability of each construct should be sufficiently high, with values of 0.70 or more. In our case, the values of all the reflective constructs are above the threshold value (Table 2). Furthermore, we assessed convergent validity using the following criteria: (1) significant factor loadings at \( p < 0.01 \) (see Table 2) and (2) average variance extracted (AVE) values above 0.50. The AVE values for all the reflective constructs are well above the required minimum level of 0.50. Thus, the measures of the reflective constructs have high levels of convergent validity (Table 2). Next, we checked for discriminant validity because if discriminant validity is not established, “constructs have an influence on the variation of more than just the observed variables to which they are theoretically related” and, thus, “researchers cannot be certain results confirming hypothesized structural paths are real or whether they are a result of statistical discrepancies” [57]. In our study, discriminant validity is determined on the basis of the heterotrait-monotrait ratio of correlations (HTMT) [56]. The HTMT should be less than one to clearly discriminate between two or more factors [56]. The values for all the constructs in our model except the second-order constructs range from 0.102 to 0.829. Thus, the HTMT show evidence of discriminant validity [56] and we conclude that discriminant validity has been established. Regarding second-order constructs, discriminant validity is not necessarily a requirement because all the lower constructs are assumed to belong to one overarching concept.

The PLS-SEM path coefficient estimates from the two-stage approach and their significance. This analysis produced estimates of both the explained variance and path coefficients, which are shown in Fig. 2. As shown by the PLS results, all seven hypotheses (H1–H7) were found to be significant. The intention to use SH devices (\( R^2 = 0.532 \)) is predicted by perceived usefulness, perceived behavioral control, subjective norms, and privacy concerns.

To further assess the quality and robustness of our results, we checked to ensure the effect sizes were strong and had predictive relevance. The effect size \( f^2 \) is, in addition to the values of the path coefficients another measure of the substantial effect of exogenous latent variables on the latent endogenous variable and is calculated according to [58], to check for practical significance. Table D.1 summarizes this analysis and indicates that the supported relationships range from small to large effect sizes. Considering the predictive relevance, the present results of the blindfolding consistently show values in the range 0.016 to 0.595 (see Table D.2.). Thus it is concluded that predictive relevance is given for all endogenous constructs.

**Fig. 2** Overview of the findings: partial least squares results for the structural model

**Note:** * \( p < 0.05 \), ** \( p < 0.01 \), *** \( p < 0.001 \)
6 Discussion

6.1 Implications and recommendations for research and practice

Our research aims to shed light on the phenomenon how privacy concerns, as reflected by its dimension of secondary use of personal information, perceived surveillance, perceived intrusion, and awareness of privacy practices, is linked to the intention to use SH devices. Privacy is one of the six different risk types in the context of technology-based innovations, in addition to functional, financial, temporal, psychological, content and social risks [59] and is viewed as a significant challenge for organizations in the context of SH usage and in particular in the area of service strategies. SH assistance as a specific capability of intelligent systems co-create value by the customers and providers via connected systems and machine intelligence [60]. As mentioned by [61], in addition to the service offered by the technology itself, the interaction between provider and customer is necessary. Therefore, we address a substantial research investigation of privacy aspects in IoT, which is mentioned by [6] and [13] and whose relevance is particularly mentioned in the smart service context, e.g., by [61].

Our research contributes to theory by identifying relevant constructs of information privacy, which are important for the acceptance of such user assistance systems. The evaluation of results shows that the developed research model is a meaningful instrument for the investigation influence of user privacy concerns on behavioral intention to use SH systems. The empirical results have proven a good explanatory power for the proposed research model. IUIPC, MUIPC, TAM, and TPB are suitable models as underlying theoretical pillars to measure privacy concerns in a SH-specific context. Our research expands the academic knowledge about MUIPC by testing the MUIPC in a SH-specific context, following the suggestion for further empirical tests of the MUIPC by [24]. Dealing adequately with privacy concerns, among other factors that are already known, is essential for the adoption and usage of SH services. To best of our knowledge, such an empirically grounded and theoretically informed understanding has been absent from the existing research and practice discourses. In our study we were able to confirm a negative influence of privacy concerns on the intention of use. Since SH services are characterized by the interaction of providers and customers to deliver value, our findings are significant. This cooperation in creating values can lead to a continuously adjustment according to the customers individual changing needs [60]. In order to support customers with SH services and thus also realize new business models, it is indispensable to understand and take into account the antecedents of the intention of use, especially the obstacles such as privacy concerns.

On the other hand, this study provides useful managerial implications for decision-making of SH device manufacturers. We elaborated the influence of different variables (e.g., privacy concerns, PU, PBC, and SN) on the decision to use SH technology. Having empirically proven the relevance of these factors, they can now be targeted by the industry to increase adoption rates. The realization, that privacy concerns have a negative direct influence on the decision to use intelligent systems in the home is of great importance to industry. This allows resources to be focused on addressing the key factors of decision making directly, namely PU, PBC and SN. Furthermore, practitioners can use our study as a starting point for further discussions about the design and the features of successful and well-accepted SH devices in order to better meet customers’ requirements. To the extent that the privacy concerns is an important factor influencing the behavioral intention to use SH systems, it is also important for service provider that these privacy concerns reduces the perceived usefulness of these systems and users’ perceived behavioral control. It follows that additional incentives around perceived benefits (e.g., more functions or customized features) must be accompanied by a limited collection of sensitive information in order to reduce the perceived risk of disclosure of information by the user in order to mitigate users’ privacy concerns.

Finally, we provide implications for SH privacy from a regulatory perspective. Several regulatory compliances and government regulations have been established to address the growing threats to privacy and security. For instance, the European Union has implemented the General Data Protection Regulation (GDPR) requiring measures to protect citizens within the EU [62]. From the practical perspective (i.e., considering government regulations), SH provider should react to users’ privacy concerns to comply with government regulations such as the GDPR to avoid any legal complications through the use of SH devices and the associated personal data. Future research should investigate whether regulatory initiatives, such as GDPR, also create greater trust (e.g., through the unified transparency of data protection for SH solutions) among users in the protection of their personal data and whether these initiatives reduce concerns about the use of SH devices. Nevertheless, even if the government regulations have been established to address the growing threats to privacy and security government regulators and privacy advocate should not tar privacy concerns in user assistant services such as SH services with a broad brush. While the basic protection is provided by the GDPR, these government...
regulations are not suited for ensuring that each user of intelligent systems (e.g., SH systems) is able to choose the level or privacy that he or she desires. With the rapid advancement of intelligent systems and the challenge to support individuals with adequate assistance functionalities (e.g., SH services), such a “one-size-fits-all” approach to assure privacy is unable to accurately or quickly meet the interest of a broad group of users or each individual. By contrast, a dynamic approach that assures control over the technological functionalities and personal data in the hands of SH users seems more attractive and will positively influence the willingness to use these intelligent systems and the corresponding assistants like SH assistants. Furthermore, both decreased risk and increased user control can be managed by individual regulations and policies, and they both affect the perceived privacy.

SH services providers must develop improved devices with user-friendly interfaces to prevent privacy concerns of the users. We argue that government regulations and rules such as the GDPR are relevant, but a technology-based solution to control personal information while using SH would be more flexible to customers changing needs.

6.2 Limitations and future research directions

Although our study opens possibilities for future research, it is subject to the following limitations. Firstly, the model is restricted to the chosen theoretical founded antecedents of the behavioral intention to use SH devices. Further research should test other influencing factors like, e.g., technology readiness. Secondly, another limitation concerns cultural differences. Privacy is especially interesting for cross-cultural investigations, because of, e.g., different legal environments [63]. In their empirical work on cross-cultural differences in risk perception, [64] have found a significant influence of culture on the perception of risk. Consequently, the customers’ acceptance of SH services might be affected by culture resulting in a limited transferability of the findings to other cultures and nationalities. We argue for an extension of this study across different cultural settings. Another limitation lies in the complex nature of examinations of SH device acceptance. The objective of this paper was to investigate the influence of privacy concerns on the acceptance of SH technology as a holistic approach. Differences between distinct components of SH devices with varying functions and risks have not been investigated. [65] showed a strong impact on acceptance of SH medical technologies. Therefore, results of this study have to be considered as a general approach to the topic of SH devices. In order to examine differences between different technologies and application areas of SH devices in more detail, it is of interest to consider them separately.

7 Conclusions

We assessed the influence of privacy concerns on the acceptance of SH devices. We proposed a model based on MUIPC, IUIPC, TBP and TAM to better represent critical factors influencing the intention to use SH devices. Secondary use of information, perceived surveillance, perceived intrusion and awareness of privacy practices were identified as essential elements for representing information privacy concerns. New technological options as SH applications can have numerous advantages but also challenges like privacy concerns. It is crucial for academics and practitioners to understand both. Our study provides a first step in this process.

Acknowledgements Open Access funding provided by Projekt DEAL.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest. Furthermore, all procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards. Informed consent was obtained from all individual participants involved in the study.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Hsu C-L, Lin JC-C (2016) An empirical examination of consumer adoption of internet of things services: network externals and concern for information privacy perspectives. Comput Hum Behav 62:516–527
2. Geneiatakis D, Kounelis I, Neisse R, Nai-Fovino I, Steri G, Baldini G (2017) Security and privacy issues for an IoT based smart home. In: Proceedings of the 40th international convention on information and communication technology, electronics and microelectronics
3. Kim Y, Park Y, Choi J (2017) A study on the adoption of IoT smart home service: using value-based adoption model. Total Qual Manag Bus Excell 28(9–10):1149–1165
4. Statista (2018) Smart home-weltweit|Statista marktprognose. https://de.statista.com/outlook/279/100/smart-home-weltweit. Accessed 12 Oct 2019

5. Yang H, Lee H, Zo H (2017) User acceptance of smart home services: an extension of the theory of planned behavior. Ind Manag Data Syst 117(1):68–89

6. Lowry PB, Dinev T, Willison R (2017) Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. Eur J Inf Syst 26(6):546–563

7. Bélanger F, Xu H (2015) The role of information systems research in shaping the future of information privacy. Inf Syst J 25(6):573–578

8. Reinsch C, Kofler M, Iglesias F, Kastner W (2011) ThinkHome energy efficiency in future smart homes. EURASIP J Embed Syst 1:1–18

9. Bugeja J, Jacobsson A, Davidsson P (2018) Internet of things A to Z: technologies and applications. Wiley, New York

10. Aldrich FK (2003) Smart homes: past, present and future. In: Harper R (ed) Inside smart homes. Springer, London, pp 17–39

11. Morana S, Friemel C, Gnewuch U, Maedche A, Pfeiffer J (2017) Interaktion mit smarten Systemen: Aktueller Stand und zukünftige Entwicklungen im Bereich der Nutzersicherheit. Wirtschaftsinformatik and Manag 9(5):42–51

12. Balta-Ozkan N, Davidson R, Bicket M, Whitmarsh L (2013) Social barriers to the adoption of smart homes. Energy Policy 63:363–374

13. Maedche A, Morana S, Schacht S, Werth D, Kruemel J (2016) Advanced user assistance systems. Bus Inf Syst Eng 58(5):367–370

14. Dorri A, Kanhere S S, Jurkád R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of the IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)

15. Plachkinova M P, Vo A, Alluhaidn A (2016) Emerging trends in smart home security, privacy, and digital forensics. In: Proceedings of the 22nd Americas conference on information systems

16. Kolksowska E, Kajtazi M (2015) Privacy dimensions in design of smart home system for elderly people. In: Proceedings of the 10th AIS SIGSEC workshop on information security and privacy

17. Belanger F, Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. Manag Inf Syst Q 35(4):1017–1041

18. Malhotra NK, Kim SS, Agarwal J (2004) Internet users’ information privacy concerns (IUIPC): the construct, the scale, and a causal model. Inf Syst Res 15(4):336–355

19. Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: measuring individuals’ concerns about organizational practices. Manag Inf Syst Q 20(2):167–196

20. Xu H, Gupta S, Rosson MB, Carroll JM (2012a) Measuring mobile users’ concerns for information privacy. In: Proceedings of the 33rd international conference on information systems

21. Enck W (2011) Defending users against smartphone apps: techniques and future directions. In: Jajodia S, Mazumdar C (eds) Information systems security. Springer, Berlin, pp 49–70

22. Korzaan ML, Boswell KT (2008) The influence of personality traits and information privacy concerns on behavioral intentions. J Comput Inf Syst 48(4):15–24

23. Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. Manag Inf Syst Q 13(3):319–340

24. Ahn M, Kang J, Hustedt G (2015) A model of sustainable household technology acceptance: sustainable household technology acceptance model. Int J Consum Stud 40:83–91

25. Venkatesh V, Davis FD (1996) A model of the antecedents of perceived ease of use: development and test. Decis Sci 27(3):451–481

26. Fortes N, Rita P (2016) Privacy concerns and online purchasing behaviour: towards an integrated model. Eur Res Manag Bus Econ 22(3):167–176

27. Azieni I (1991) The theory of planned behavior. Organ Behav Hum Decis Process 50(2):179–211

28. Fishbein M, Azieni I (1975) Belief, attitude, intention and behaviour: an introduction to theory and research. Addison-Wesley Pub. Co., Boston

29. Safeena R, Date H, Hundewale N, Kammani A (2013) Combination of TAM and TPB in internet banking adoption. Int J Comput Theory Eng 5(1):146–150

30. Brown SA, Venkatesh V, Hoehle H (2015) Technology adoption decisions in the household: a seven-model comparison. J Assoc Inf Sci Technol 66(9):1933–1949

31. Zweig D, Webster J (2002) Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. J Organ Behav 23(5):605–633

32. Junglas IA, Johnson NA, Spitzmüller C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur J Inf Syst 17(4):387–402

33. Hojatii SN, Khodakarami M (2016) Evaluation of factors affecting the adoption of smart buildings using the technology acceptance model. Int J Adv Netw Appl 7(6):2936–2943

34. Taylor S, Todd PA (1995) Understanding information technology usage: a test of competing models. Inf Manag 26(6):546–563

35. Zweig D, Webster J (2002) Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. J Organ Behav 23(5):605–633

36. Junglas IA, Johnson NA, Spitzmüller C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur J Inf Syst 17(4):387–402

37. Hojati SN, Khodakarami M (2016) Evaluation of factors affecting the adoption of smart buildings using the technology acceptance model. Int J Adv Netw Appl 7(6):2936–2943

38. Taylor S, Todd PA (1995) Understanding information technology usage: a test of competing models. Inf Sys Res 6(2):144–176

39. Kim B (2010) An empirical investigation of mobile data service continuance: incorporating the theory of planned behavior into the expectation-confirmation model. Expert Syst Appl 37(10):7033–7039

40. Wunderlich P, Veit D, Sarker, S (2012) Examination of the determinants of smart meter adoption: an user perspective. In: Proceedings of the 33rd international conference on information systems

41. Venkatesh V (2000) Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. Inf Syst Res 11(4):342–365

42. Hu PJ-H, Clark THK, Ma WW (2003) Examining technology acceptance by school teachers: a longitudinal study. Inf Manag 41(2):227–241

43. Simpson PM, Banerjee D, Simpson CL (1994) Softlifting: a model of motivating factors. J Bus Ethics 13(6):431–438

44. Chellappa RK, Sin RG (2005) Personalization versus privacy: an empirical examination of the online consumer’s dilemma. Inf Technol Manag 6(2):181–202
45. Li H, Wu J, Gao Y, Shi Y (2016) Examining individuals’ adoption of healthcare wearable devices: an empirical study from privacy calculus perspective. Int J Med Inf 88(1):8–17
46. Lowry PB, Zhang J, Wang C, Siponen M (2016) Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. Inf Syst Res 27(4):962–986
47. Venkatesh V, Thong JY, Xu X (2012) Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. Manag Inf Syst Q 36(1):157–178
48. Denscombe M, Ebrary I (2010) The good research guide for small-scale social research projects, 4th edn. England McGraw-Hill, Maidenhead
49. Petter S, Straub D, Rai A (2007) Specifying formative constructs in information systems research. Manag Inf Syst Q 31(4):623–656
50. Hair JF, Hult GTM, Ringle CM, Sarstedt M (2017) A primer on partial least squares structural equation modeling (PLS-SEM). Thousand Oaks, California
51. Polites GL, Roberts N, Thatcher J (2012) Conceptualizing models using multidimensional constructs: a review and guidelines for their use. Eur J Inf Syst 21(1):22–48
52. Edwards JR (2001) Multidimensional constructs in organizational behavior research: an integrative analytical framework. Organ Res Methods 4(2):144–192
53. Guhr N, Lebek B, Breitner MH (2019) The impact of leadership on employees’ intended information security behaviour: an examination of the full-range leadership theory. Inf Syst J 29:340–362
54. Richter NF, Cepeda G, Roldán JL, Ringle CM (2016) European management research using partial least squares structural equation modeling (PLS-SEM). Eur Manag J 34(6):589–597
55. Ringle CM, Wende S, Becker JM (2015) SmartPLS 3. www.smartpls.com. Accessed 12 July 2019
56. Becker JM, Klein K, Wetzel M (2012) Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models. Long Range Plan 45(6):359–394
57. Henseler J, Ringle CM, Sarstedt M (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. J Acad Market Sci 43(1):115–135
58. Farrell AM (2010) Insufficient discriminant validity: a comment on Bove, Pervan, Beatty, and Shiu (2009). J Bus Res 63(3):324–327
59. Cohen J (1988) Statistical power analysis for the behavioral sciences. Lawrence Erlbaum Associates, Hillsdale
60. Paluch S, Wunderlich NV (2016) Contrasting risk perceptions of technology-based service innovations in inter-organizational settings. J Bus Res 69(7):2424–2431
61. Gavrilova T, Kokouлина L (2015) Smart services classification framework. In: Proceedings of the federated conference on computer science and information systems
62. Dreyer S, Olivotti D, Lebek B, Breitner MH (2019) Focusing the customer through smart service: a literature review. Electr Markets 29:55–78
63. Nadeau M (2018) General data protection regulation (GDPR): what you need to know to stay compliant. https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html. Accessed 12 July 2019
64. Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. Manag Inf Syst Q 35(4):989–1016
65. Bontempo RN, Bottom WP, Weber EU (1997) Cross-cultural differences in risk perception: a model-based approach. Risk Anal 17(4):479–488
66. Himmel S, Ziefle M (2016) Smart home medical technologies: users’ requirements for conditional acceptance. i-Com 15(1):39–50

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.