The Role of Trust and Perceived Risk in the Relationship between Privacy and Security Values, and Emotions towards Smart Home Devices

Alina Papke

Behavioural Management and Social Sciences, University of Twente
Conflict, Risk and Safety Psychology

June 30, 2022

Word Count: 7.779

1st Supervisor: Nicole Huijts
2nd Supervisor: Peter de Vries

Abstract

As using smart home devices has become increasingly popular despite coming with several risks concerning user privacy and security, this paper investigates the influence of personal security and privacy values on emotions towards smart home devices considering the role of trust and perceived risk. To do this, an online experiment was conducted, first having participants indicate their values, then asking them to imagine a situation in which an Amazon Echo smart speaker was just installed in their home, after which they reported their emotions regarding the respective situation along with their assessment of perceived risk and trust. It was found that privacy but not security values influence emotions towards smart home devices and that this relationship is moderated by trust but not perceived risk. However, perceived risk was found to have a strong correlation with emotions towards smart home devices. These findings highlight the importance of considering the privacy values of users when first of designing smart devices, and in a second instance, policing them in a way that is protecting consumers' privacy and security.

Introduction

Smart home devices are of ever-growing importance in today's globalised world. In fact, the number of digital voice assistants, a vital component of smart home technology, is projected to grow from 3.25 billion digital voice assistants being used in devices globally in 2019, to 8.4 billion in 2024, a number surpassing that of the world's population by that time (Laricchia, 2022). These voice assistants are not only a common feature of many smart phones, but also smart speakers and other smart devices used around the home.

Whilst it is obvious that smart home devices have numerous benefits, there are also some risks attached (Wilson, Hargreaves, & Hauxwell-Baldwin, 2017). Li et al. (2021), among others, identified privacy concerns as one such risk relating to security in the smart home context. Security concerns of smart homes include the fear to leave a digital trace that can be detected from outsiders who might then use them to gain an advantage that is harmful to the user (Cook, 2012). Yet, even though security is among the values that can motivate decisions and although security as well as privacy have been identified as specifically impacting adoption decisions of smart devices, these devices keep being adopted (Emami-Naeini et al., 2019; Schwartz, & Boehnke, 2004). As such, it seems worthwhile to investigate this phenomenon more closely to gain a deeper understanding.

Following this train of thought, a factor that seems to play a role here is emotions. Particularly, emotions have been found to be a vital component in user experience concerning technologies (Agarwal & Meyer, 2009), as well as in the acceptance of said technologies (Beaudry & Pinsonneault, 2010). On a similar notion, Desmet and Roeser (2015) make a case for the importance of considering the relationship between personal values and the positive and negative emotions that are evoked through them when using a technology, as they argue that technologies are value-laden, meaning that technologies are in line with or opposing certain values. Depending on the extent of the overlap with personal values this produces certain emotions in response to the technology (Desmet & Roeser, 2015). Therefore, when looking at the usage behaviour of smart home devices, emotions in response to them should also be studied especially with special attention paid to personal values.

Moreover, it has been found that values can impact emotions towards technologies (Contzen et al. 2021). Particularly, they showed that emotions towards technological innovations are influenced by people's core values as prompted by the particular characteristics of the innovation and the degree to which they align. However, this has not yet been tested for smart home devices which increasingly have a place in people's lives. Furthermore, this study is interested in the personal values of security and privacy which

have not been investigated in this context yet. Therefore, in this study emotions towards smart home devices are going to be investigated as influenced by the abovementioned values.

To be precise, the Schwartz value scale, a circumplex model of competing values (Schwartz, & Boehnke, 2004), is going to be employed to find out if personal security values influence positive and negative emotions towards domestic smart devices. However, in this study a newly devised scale of privacy is also going to be added to the security value of the scale to establish whether it can additionally contribute to explaining these emotions as this model does not yet hold it.

Moreover, the study aims to identify whether trust as well as perceived risk can moderate the abovementioned relationship. In fact, numerous authors have found these factors to be important to understand in the context of technology adoption and usage as they are influential especially in relation to privacy concerns (Daubert et al., 2015; Gerber, et al., 2018; Jaspers & Pearson, 2022). However, there seems to be a lack of research in this particular context. Hence, this study aims to close this gap. Therefore, the underlying question that this study aims to answer is: “What is the relationship between personal values and emotions toward smart home devices, and how do perceived risk and trust in the service provider influence this relationship?”.

Smart Home Devices

The particular technology that is going to be investigated are smart home devices, due to their increasing relevance in day-to-day life. A particularly comprehensive clarification of what is understood as being smart home devices is provided by Weaver et al. (2020). To be precise, a smart home device is any kind of technology that utilizes the internet of things to automate certain features in a home. To clarify, the internet of things (IoT) connects physical objects, in this case smart devices, to each other and to clouds and cloud data, using the internet and other communication networks (I.e. Bluetooth, etc.) to a degree that minimises human involvement in this process and maximises automation (Al-Fuqaha et al., 2015; Bhattarai & Wang, 2018). This feature is essential for smart devices as it allows them to perform tasks automatedly.

Moreover, smart home devices use “embedded sensors and the internet to collect and communicate data with each other and their users, seamlessly integrating the physical and digital worlds inside the home” (Zheng et al., 2018, p.1). Examples include energy-tracking switches, app or voice-controlled lights, shades, and speakers, as well as smart or video

doorbells (Zheng et al., 2018). Again, this communication between devices is enabled by IoT which essentially makes these devices smart.

This degree of automation provides a certain convenience by enhancing a home and solving problems, however in gathering and handling so much data privacy concerns arise (Li et al., 2021; Weaver et al., 2020; Zheng et al., 2018). Zheng et al. (2018) for example, point out that these concerns include questions regarding what kind of data is gathered, how it is processed, who is capable of tracking and accessing it and who owns it.

Another concern is user activity detection (Ukil et al., 2014). The problem here is that daily behavioural patterns can be identified and exploited (Khan et al., 2021) endangering the user's security. Moreover, this might allow for inferences about personally identifiable information, such as user identity, occupation and location-based information, like the home address (Khan et al., 2021).

In conclusion, there are several security and privacy risks associated with smart home devices. As such, both the use of and the preceding step, acceptance of smart home devices seems to be subject to a competition of values: indulging in the benefits and pleasures of the conveniences of smart home devices versus refraining from doing so in favour of personal security and privacy.

Security

Considering next the concept of security, Duezguen et al. (2021) provide an overview of what cybersecurity and attached risks entail in the smart home context. Essentially, security hinges on encryption and authentication protocols that are in place to avoid crimes being done with the information that these devices or otherwise potential eavesdroppers might be able to pick up. These crimes could for example include identity theft and subsequent fraud. Kalofonos and Shakhshir (2007) argued that one of the major threats in the smart home is actually a lack of understanding of the security protocols on the side of the user. As such they might not enable the right settings and leave the system vulnerable. By the same token, Haney et al. (2020) identified a lack of user technical understanding as a major challenge to smart home security.

Moreover, a (potentially) misplaced trust in IoT manufacturers to take proper care of device security was mentioned as mitigating the users' security concerns (Duezguen et al., 2021). In sum, smart home security is the level of encryption and authentication of smart devices, however, users lack an understanding to properly configure them, while at the same time believing the manufacturer to have sufficiently taken care of any cybersecurity issues.

An overlap with security as a value can be found in the conceptualisation of personal security as “secure surroundings” and an “avoidance of danger” (Schwartz et al., 2012). To be precise, a smart home would constitute the surroundings of a person, which also happen to be the main personal space of an individual. Moreover, the physical safety aspect of security can also come under threat. As Cook (2012) explained, with a lack of cybersecurity, user activity could be detected from outside the home. This might allow to time breaking and entering to a moment the home is not monitored properly.

Taking into account, the risks that have been mentioned above and further ones that shall be mentioned below, there is sufficient reason to believe that someone who values their personal security will take a less favourable stance towards smart home devices, seeing as they have the potential to pose a threat right inside someone’s personal space.

Privacy

Since privacy issues are at the heart of this research, it is important to understand what privacy actually is. Margulis (1977) for example defines privacy as follows: “selective control over transactions between self (or one's group) and others, the ultimate aim of which is to enhance autonomy and/or to minimise vulnerability” (as cited in Stuart et al., 2019, p.2) A similar definition is given by De Wildt et al. (2021) in which they define privacy as: “Other people not interfering with our affairs, as people having no specific knowledge about us (i.e., in informational terms) or in terms of our ability to control who has what information about us (i.e., in terms of control and informed consent)” (p.434). Bringing these definitions together, privacy is about the ability to control who can access personal information about oneself to keep a level of autonomy.

In addition, there are certain aspects of privacy that seem especially debatable in the smart home environment. Lin and Bergmann (2016), for example, identified two key issues in this context, access and confidentiality. Both aspects interplay and refer to the idea that data should be kept private in the sense that only authorised individuals should have access to the user data, whereas unauthorised entities, including machines and algorithms, should be barred from any kind of access.

However, despite user’s concerns about the level of protection in this regard being among the most prevalent, there is only little information available about the privacy and security status of the devices on the market (Emami-Naeini et al., 2019; Zheng et al., 2018). Still, at least a third of respondents asked in the Global Consumer Survey 2021 indicated that safety in the smart home context is of particular importance to them; for some countries this

was indicated by more than half of the respondents (Sava, 2022). In sum, the privacy and security values seem to be a recurring theme for smart home users.

Trust

Yet, while values have been found to impact emotions towards innovative technologies (Contzen et al., 2021) and the security and privacy values in particular to factor into the adoption behaviour of smart home devices (Emami-Naeini, et al. 2019), it has also been found that this is not always the case. In fact, especially privacy, while being a concern, does not predict the intention to use a smart device (Jaspers & Pearson, 2022). Barth and De Jong (2017), refer to this phenomenon as the privacy paradox, meaning that privacy concerns do neither translate into actual behaviour nor behavioural intention. In consequence, this might also hold for the resulting emotions. It could be suggested that this is due to a lack of risk perception or understanding thereof which has been claimed to be necessary in order to take protective action against the privacy or security threat (Duezguen et al., 2021). At this point it is also useful to refer back to the role of trust in mitigating these concerns about security and privacy threats (Duezguen et al., 2021). In sum, trust plays an important role, both in privacy and security perceptions of IoT users.

To elaborate, according to Jaspers and Pearson (2022) trust in the service provider, as opposed to singular privacy concerns, translates into behavioural intention. Moreover, they conclude that trust is explicitly related to privacy concern and that the correlation is negative, that is, trust decreases privacy concern. Another study also highlights the importance of trust drawing a clear relation to privacy in the context of smart home devices (Daubert et al., 2015). To be precise, they make a case for the idea that the personal need for privacy correlates to a higher need for trusting the service provider in the consideration to share personal information using a technology.

Furthermore, since mutual trust between consumers and service providers has been considered a highly relevant factor in the marketing area (Liu et al., 2021), it seems worthwhile to investigate. In particular, better understanding the role of trust in the smart home context might allow for drawing conclusions for stakeholders in the industry such as policy makers, developers and managers to influence this factor and consequently, the consumer's behaviour concerning smart home devices with particular regard to privacy and security of the consumer.

Trust, however, can refer to a plethora of ideas and relationships. For instance, trust can concern the service or the device, but also the service provider, their intention and

capability (Daubert et al., 2015; Jaspers & Pearson, 2022). Poore, as cited in Daubert et al. (2015) defines trust as the mutual idea that personal information "will be only used as agreed and will be protected against unauthorized access" (p. 2666). Additionally, some authors point out two aspects that play a particular role regarding the service provider of technologies and that is competence-based trust and character-based trust (Beldad & Kusumadewi, 2015). These concepts refer to, for one the ability of the service provider and secondly, the willingness or intention of the same. Therefore, in this study trust will be defined as "the belief in the ability and intention of the service provider to keep any personal data gathered by the smart home device safe from unauthorized access".

In this study, trust will be incorporated since the aforementioned studies give reason to believe that it can add value to the explanatory power of the privacy value towards emotions. Specifically, it is expected to fill the role of a moderator. To elaborate, Contzen et al. (2021) found that emotions as a response to technological innovations are influenced by values in accordance with the extent to which these technologies are in alignment with those values. That is, for the values privacy and security, whilst someone might value them, this will not have an effect if the technology does not give reason to believe that privacy or security are under threat. As trust in the service provider essentially means that consumers believe them to take care of their privacy and security interests, trust can reasonably be expected to mitigate the perception of threat to personal values by technologies. Therefore, in the presence of trust, threat perception is low, and security and privacy values have less of an impact in regards to emotions toward smart home devices.

By the same token, since trust had a significant positive relation to the willingness to provide personal information (Kim et al., 2019) it is reasonable to assume that privacy concerns will not have as much of an impact when trust is high, as the providing of personal information is then not as strongly associated to their loss. In turn, emotions are expected to remain more positive.

In sum, it can be assumed that trust will moderate the relationship between privacy values and emotions towards smart home devices. So even with a high value of privacy, emotions will be relatively positive if trust is high. That is, when the user trusts in the intention of the service provider to keep their personal information safe, their emotions towards the smart home device are expected to remain relatively positive, even when the individual values their privacy rather highly.

Perceived Risk

Next, a factor that keeps getting mentioned along with trust every so often is perceived risk. For example, Beldad and Kusumadewi (2015) claim that the risks related to using a certain technology actually influence the prominence of trust in contemplating whether to use it. In turn, Malhotra et al. (2004) make a case for trust influencing the risk beliefs. By the same token, in relation to privacy trust has been found to decrease perceived risk (Kim et al., 2019). A similar effect has been found by Gerber et al. (2018). In sum, there seems to be some important relation between these two variables, and it seems further worthwhile to investigate them together.

Moving on to what perceived risk means in the context of smart home devices, Koohikamali et al. (2015) provide the following definition: “the users' beliefs about potential negative outcomes”. While they focused on the use of social network applications, they mainly related the idea of perceived risk to sharing personal information with the service. Potential negative outcomes in this situation could mainly refer to the loss of or abuse of one’s personal data. Kim et al. (2019) provide the example of leakage of personal data, presumably to third parties or the general public. As such, this definition is easily applied to the potential of smart home devices gathering private information which are particularly sensitive. Thus, this study is going to work with the definition as follows: “The users' beliefs about potential negative outcomes of using smart home devices”.

Similar to the role of trust in the relationship between privacy and security values and emotions toward smart home devices, privacy values seem likely to be more prevalent when perceived risk is high due to a belief in higher association with their loss and therefore perception of threat towards the personal values, privacy and security (Contzen et al., 2021; Desmet & Roeser, 2015; Kim et al., 2019), as opposed to trusting beliefs which mitigate this worry about loss. As such, emotions towards smart home devices are probably more negative when perceived risk is high. Therefore, this study investigates the potential interaction effect of perceived risk.

Hypotheses

As the purpose of the current study is to understand the explanatory power of the values on emotions towards smart home devices better, a number of hypotheses need to be tested. They all follow the assumption that values impact emotions toward technologies (Contzen et al., 2021). More precisely, here the effect of the particular values, security (Schwartz, 2012) and privacy (Huijts, N.M.A. (manuscript)), on smart home devices as a

specific technology, are tested. Furthermore, based on the above detailed findings this direction is expected to be negative. Thus, the first two hypotheses are:

Ha1: The value security is negatively correlated with emotions towards smart home devices.

Ha2: The value privacy has a negative correlation with emotions towards smart home devices.

Moreover, in line with earlier findings on trust and privacy concerns (Jaspers & Pearson, 2022), Trust is expected to moderate the effect of privacy on Emotions, yielding these two hypotheses as follows:

Ha3: Trust in the service provider has a positive correlation with emotions towards smart home devices.

Ha4: The correlation of the value privacy and the value security with emotions towards smart home devices is stronger when trust in the service provider is low.

Figure 1

Hypothesis 4 – Moderation effect of trust on privacy values

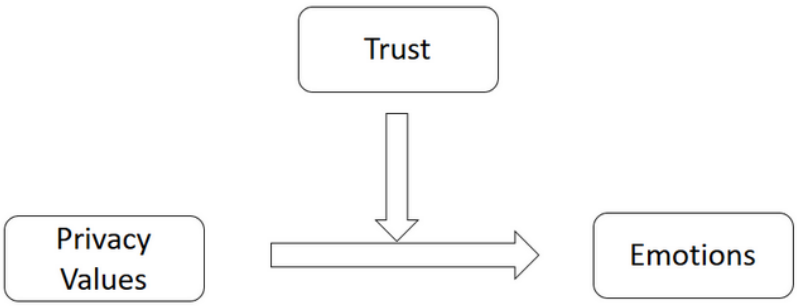
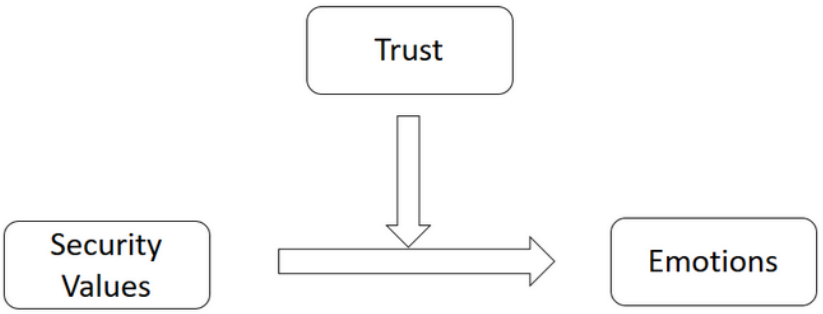


Figure 2

Hypothesis 4 – Moderation effect of trust on security values



In terms of the findings regarding perceived risk, the following is hypothesised:

Ha5: Perceived Risk has a negative correlation with emotions towards smart home devices.

Ha6: The negative correlation of the value privacy and the value security on emotions towards smart home devices is stronger when perceived risk is high.

Figure 3

Hypothesis 6 – Moderation effect of perceived risk on privacy values

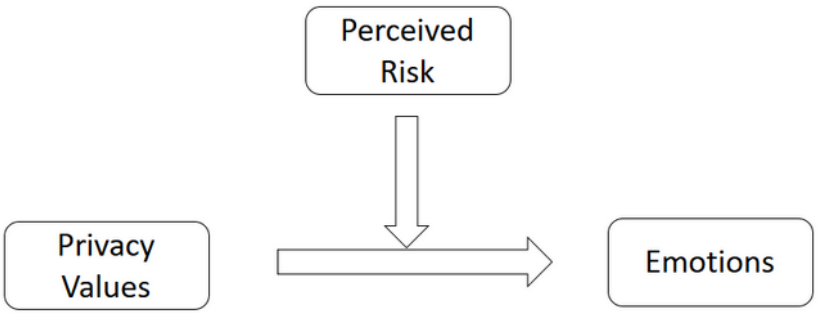
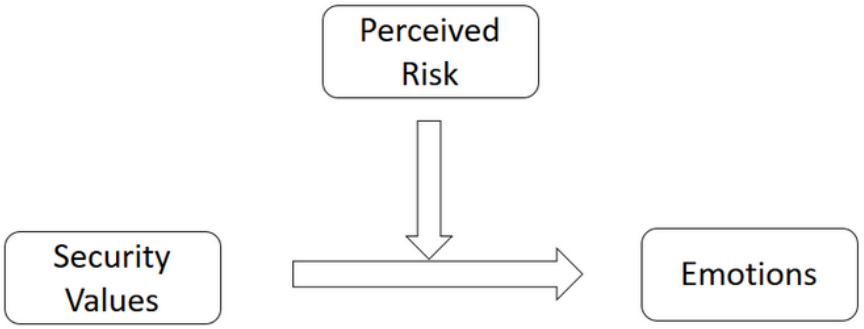


Figure 4

Hypothesis 6 – Moderation effect of perceived risk on security values



Methods

Participants and Design

The study design used a between subjects design with two experimental conditions manipulating the moderator perceived control. Notably, the data collection and therefore the

study design was a joined process with a related study. The variable perceived control was not interesting for the research aim of this particular study which is why it was disregarded.

Moreover, the questionnaire of this study was administered to participants that were recruited using the SONA-system. Additionally, it was made use of a convenience sampling method, that is, participants were recruited using social media and WhatsApp groups. Participants recruited via the SONA-system were compensated by means of credit points. Furthermore, Participants were made aware of the requirements to participate in the study. To be precise, they should have a fair command of the English language and being capable of giving informed consent to participate. A minimum of 18 years of age has been decided as a further requirement for participation. Moreover, it was explicitly stated that participants did not need to own a smart device in order to participate.

87 people filled out the survey, but 33 participants had to be excluded. 26 did not finish the survey to the necessary extent, and an additional 7 failed the attention check. This left a final sample of 54 participants as can be seen in table 1. As such, the final sample consisted of 24 males and 30 females, ranging from 18 to 56 years of age (M = 24.61 SD = 10.37). The participants signed up voluntarily and the study has been approved by the university's ethics committee.

Table 1

Characteristics of the Sample Population (N = 54)

Characteristics		Frequency	Percentage (%)
Age	18 - 28	48	88.89
	29 - 39	0	
	40 - 50	1	1.85
	51 or above	5	9.26
Gender	Female	30	55.6
	Male	24	44.4
	Other	0	
	Prefer not to say	0	
Education	Havo / equivalent	1	1.9
	VWO / A-Levels / equivalent	37	68.5
	Bachelor's degree	5	9.3
	Master's degree	1	1.9
	PhD	2	3.7
	Other	8	14.8

Procedure

First, in the beginning of the questionnaire, the participants were informed about the purpose and implications of the study and were asked to give their consent. Afterwards, the participants were provided with a general section in which they had to fill in demographics such as age, gender and education. The following section of the questionnaire contained the questions about the participants' values regarding security, and privacy as detailed above amidst the distractor items on other values in order to avoid making the participants aware of the explicit purpose of the study. Furthermore, these items were presented to the participants in a randomised order. Next, the participants were provided with general information on what a smart device is and what it is capable of concerning its performance and tasks.

Afterwards, the participants were randomly assigned to one of two possible experimental conditions that concerned perceived control as part of the other related study. In any case, within these conditions they were asked to imagine a variation of the scenario that a smart speaker is being installed in their home (Appendix A). One scenario asked the participants to imagine they themselves had bought and installed the smart speaker, whereas the other scenario was about their roommate having done this. After reading through the given scenario, the participants received the second part of the questionnaire asking about the emotions of the participants regarding the scenario. This section also included the questions on the potential moderators *trust* and *perceived risk*, which along with the items on *emotions* were presented in a random order intermingled. After this section a short debrief followed that specified to the participants the values that this study was interested in.

Measurements

The questionnaire designed for this study contained six items on the independent variables *privacy* and *security values* in between 22 distractor items on other values used in the Schwartz value scale. The dependent variable *emotions towards smart home devices* was measured using eight items, along with five items each for the moderators *perceived risk* and *trust in the service provider*. The items on *perceived risk* and *trust* were taken from Malhotra et al. (2004) and adjusted to fit the purpose of this study better. Precisely, the original items referred to online companies in general, but this study was on smart speakers, specifically Amazon Echo. For example, an item like "I trust that online companies would keep my best interests in mind when dealing with (the information)" (Malhotra et al., 2004, p. 352) was rephrased to "I trust that Amazon would keep my best interest in mind (…)".

Moreover, all items besides the demographics were measured on a 7-point Likert scale ranging from completely agree to completely disagree. See Appendix A for the Questionnaire. That is, for example for the dependent variable *emotions* participants had to indicate how much they agree with such statements as: “I am satisfied with the Amazon Echo.” or “I am frustrated with the Amazon Echo.” to cover both possible negative and positive feelings towards the chosen smart home device.

The dependent variable that was investigated, is *emotion*. Emotions in this context can be understood as the feelings that are triggered by or relate to the smart home device in question. Therefore, *emotion* is measured in a questionnaire using items such as “To what extent do/would you feel *emotion* about this device?”. The feelings in question are grouped into negative and positive emotions that can seem to be reasonable reactions to the smart home devices.

The values thought to influence these *emotions* were the independent variables. To measure these values, items of the PVQ and definitions as provided by Schwartz were employed. The first independent variable was the *security value*, which Schwartz (2012) defined as: “safety, harmony, and stability of society, of relationships, and of self” (p. 6).

The second independent variable of interest in this study was *privacy value*, which was defined as valuing “the ability to control who can access personal information about oneself to keep a certain level of autonomy”. The items used to measure this were in the style of the PVQ items but are supposed to be an independent extension (Huijts, N.M.A. (manuscript)).

Next, two variables were tested for moderation. Firstly, the individual level variable *Trust*, which can be understood as *trust* in both the intention and capability of the service provider to protect and properly encrypt the private data of the device users (Beldad & Kusumadewi, 2015). Secondly, the individual level variable *perceived risk*, which refers to the users' beliefs about potential negative outcomes of using smart home devices.

Data Analysis

To test the hypotheses, several statistical analyses were run using the software RStudio.

Preparing Data Set

To prepare the data for the analysis, the data set has first been cleaned. Respondents who did not complete the survey to a necessary degree were excluded. Moreover, 7

respondents had to be excluded failing the attention check. One item of the perceived risk scale was reversed and had to be recoded.

Factor Analysis

In order to establish the validity of the employed items, a factor analysis was conducted. To begin with, suitability of the variables for a factor analysis was determined computing the Kaiser-Meyer-Olkin measure and conducting a Bartlett sphericity test for each set of relevant variables. That is, one set of data included the emotion items, another set contained the value items, and a last data set contained only the potential moderator(s) perceived risk and trust. Next, a factor analysis was conducted on each of the data sets, computing the eigenvalues and creating a scree plot determining the number of potential factors in each data set. Lastly, the factor analysis that was run, showed which items measured the same underlying construct.

Next, those items measuring the same construct were each put into a single data set on which to apply classical test theory establishing the items' reliability was determined, first computing Cronbach's alpha. Additionally, it was considered whether dropping some items might lead to a higher measure of internal consistency of the factors.

Afterwards the reliable items were combined into the respective variables, trust, perceived risk/control, negative emotions, positive emotions, privacy values and security values by averaging the items. Then, a correlation matrix was computed on all relevant variables. Next, several regression analyses were run separately on negative and positive emotions as the dependent variable with various combinations of independent variables as it fit the hypotheses testing, including models on the potential moderation effects. In case of significant findings for the interaction effect, a simple slope analysis followed.

Results

Factor Analysis

To begin with, the reliability of the newly employed privacy scale was established doing a factor analysis on both the security and privacy scales together. To do that, first eligibility of the security and privacy scales for factor analysis was tested using the Kaiser-Meyer-Olkin criterion and Bartlett sphericity test which showed that both scales were suitable for factor analysis. Next, considering the eigenvalue and a scree plot (Appendix B) 2 factors were suggested as two eigen values were indicated to be above 1. Moreover, the factor analysis for the personal values loaded properly on the intended factors except for the

security item “It is important to me to be personally safe and secure.”, which loaded more heavily on the privacy factor (Appendix B, Table B1). The factor loading on the security factor however was not all that much lower which is why this item was still decided to be put into the security factor. That is also because the original security scale has been used and validated often prior to this study. It must be noted however, that there is some overlap between the newly devised privacy scale and the original security scale.

Next, the emotion items were also found to be suitable for factor analysis. Two factors were identified looking at the Kaiser’s criterion. The same was found looking at the scree plot (Appendix C). Here, the factor loadings showed that positive and negative emotions are to be considered two separate factors with the factor loadings properly indicating that the items fit their respective emotion (Appendix C, Table C1).

Considering the items that were intended to measure perceived risk and trust, it has been found that they too are suitable for factor analysis. A factor analysis also established that these items measure two separate factors, both when looking at the number of eigenvalues above 1 and the scree plot (Appendix D). The items also did load properly on the separate factors as they were expected to (Appendix D, Table D1). Therefore, Perceived Risk and Trust were considered separate variables.

For the scales’ reliability, Cronbach's alpha was considered. The privacy scale’s reliability is good with $\alpha = .775$. Looking at the security scale, $\alpha = .594$ was observed, which is poor but not yet unacceptable. In contrast, both emotion scales performed well, with $\alpha = .891$ for positive emotions and $\alpha = .853$ for negative emotions. The scales for perceived risk and trust were also both considered reliable with $\alpha = .817$ for the former and $\alpha = .854$ for the latter.

However, Cronbach's alpha for the trust scale could be improved by deleting the item “Amazon tells the truth and fulfils promises related to the information provided by users of the smart speaker.” to $\alpha = .877$. The fact that this item might not have performed as it should have, could be due to its phrasing. Specifically, the phrasing might imply that telling the truth and fulfilling promises is to be understood as a fact rather than an “I trust that this is the case”. As such, it does not necessarily measure trust when respondents take it to mean a factual thing that could simply be true or false. The comparatively low factor loadings for this item (Trust 2) additionally show that it might not measure what it was intended to measure (Appendix D, Table D1). Consequently, this item was taken out of the final variable.

Moreover, the Perceived Risk Item “I would feel safe giving my information to Amazon.” loaded more heavily on the other factor which includes the Trust items. This could

be due to the phrasing which leaves room for different reasons to feel safe. Feeling safe could either result from trusting the service provider's intention and ability to protect the users' interests, but also from a generally low risk perception or awareness. As such it was considered too ambiguous for being vague in regard to reason and was taken out of the final Perceived Risk variable.

Descriptives

Next described are the descriptive statistics for the Security and Privacy scales, and the scales of Trust and Perceived Risk. On both the Security scale (M = 5.54, SD = 0.85) and the Privacy scale (M = 5.17, SD = 1.27), respondents indicated a moderately high level of agreement with the items. A smaller level of agreement with the items can be observed in the Trust scale (M = 2.75, SD = 1.24), whereas a slightly higher level was indicated with the items of the Perceived Risk scale (M = 4.44, SD = 1.05).

Correlations

Next, a correlation matrix was computed yielding the results as specified in table 2.

Table 2

Correlation Matrix

Variable	*M*	*SD*	1	2	3	4	5
1 Privacy	5.17	1.27					
2 Security	5.54	0.85	0.36**				
3 Trust	2.75	1.24	-0.29*	-0.15			
4 Perceived Risk	4.44	1.05	0.38**	0.18	-0.51***		
5 Negative Emotions	4.11	1.21	0.33**	0.05	-0.41***	0.80***	
6 Positive Emotions	3.62	1.22	-0.34**	0.00	0.46***	-0.41***	-0.6***

*p < .05. **p < .01. ***p < .001

Regression Analysis

To test the first Hypothesis Ha1: "*The value security is negatively correlated with emotions towards smart home devices.*" a regression model with negative emotions and then positive as the dependent and security values as the independent variable was specified. The regression analysis for negative emotions was insignificant ($b = 0.07$, $p = .727$). Similarly, there was no effect of Security on positive emotions ($b = 0.00$, $p = .99$). Therefore, the analyses did not support Ha1.

The second hypothesis "*The value privacy has a negative correlation with emotions towards smart home devices.*" was tested specifying a model with privacy as the independent and negative emotions and then positive emotions as the dependent variable. In both cases, the effect was significant. That is, privacy values significantly affect negative emotions ($b= 0.31$, $p = .015$) and positive emotions ($b= -0.33$, $p = .012$). Since this also aligns with the hypothesized directions, the findings support Ha2.

In a model including both privacy and security values, that is controlling for each other, the effect of privacy values remained significant both on positive ($b= -0.38$, $p = .007$) and negative emotions (b= 0.34, $p = .015$). Likewise, there was no effect of security values on either emotion (Table 3). Therefore, Hypothesis 2 was supported by the findings.

Table 3

Regression Table – Main Effects of Security and Privacy on Negative and Positive Emotions

Variable	*b*	*SE*	*p*
DV: Negative Emotions			
intercept	2.964**	1.093	0.009
Privacy	0.34*	0.135	0.015
Security	-0.111	0.201	0.583
R^2	0.113		
DV: Positive Emotions			
intercept	4.446***	1.085	0.000
Privacy	-0.375**	0.134	0.007
Security	0.201	0.199	0.317
R^2	0.133		

*$p < .05$. **$p < .01$. ***$p < .001$

Then, the hypotheses concerning the potential interaction variables were tested. To be specific, Ha3 and Ha5 state that both Trust and Perceived Risk correlate to Negative Emotions towards smart home devices in terms of main effects. Ha4 and Ha6 describe the corresponding interaction effects.

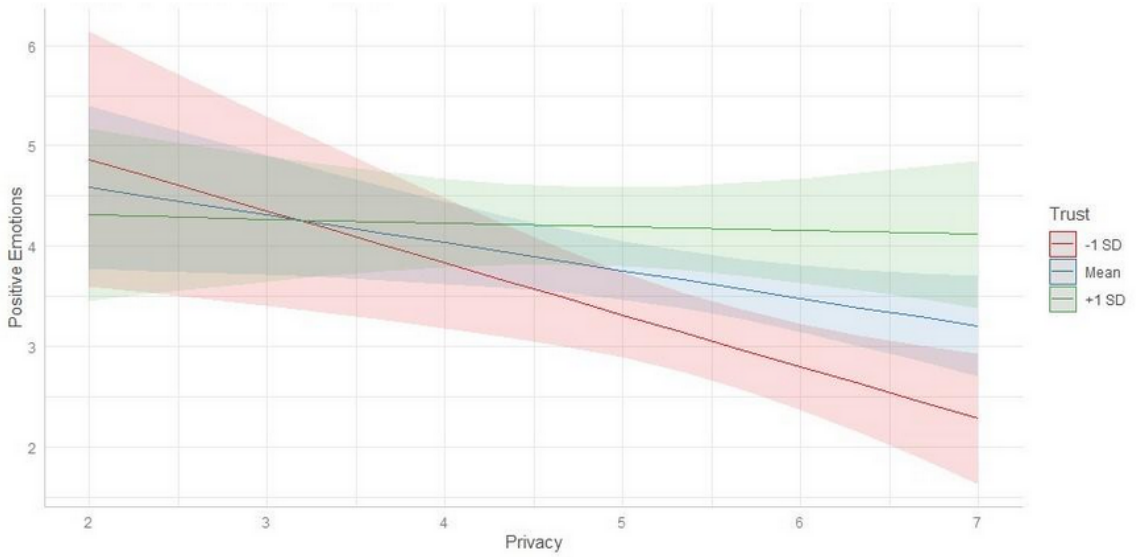
Ha3 was supported as Trust was found to have both a significant positive effect on Positive Emotions (b= 0.45, p = .000) and a significant negative effect on Negative Emotions (b= -0.41, p = .002) which fits the hypothesized direction. Moreover, Perceived Risk had a significant effect on Emotions towards smart home devices in the hypothesized directions, with an effect of b= -0.48, p = .002 on Positive Emotions and an effect of b= 0.92, p = .000 on Negative Emotions.

However, in a model including both variables only Perceived Risk had a significant effect on Negative Emotions (b= 0.91, p = .000), whereas Trust did not have a significant effect at all (b= -0.01, p = .916). Moreover, controlling for each other, both Perceived Risk (b= -0.28, p = .096) had only a marginally significant effect on Positive Emotions whereas the effect of Trust was significant (b= 0.33, p = .02).

Concerning the interaction effects, Privacy as moderated by Trust was found to be significant, but only for Positive Emotions (Table 4). To be precise, Trust did not significantly interact with Privacy in a regression model with Negative Emotions as the dependent variable (b= -.103, p = .266). However, there was a significant interaction effect of Privacy and Trust on Positive Emotions (b= 0.19, p = .029). Looking at the slopes for this interaction effect (Figure 5), it becomes clear that Ha4 can be supported for Positive Emotions as Positive Emotions for people with higher-than-average levels of Trust are relatively high while having high Privacy Values, whereas lower-than-average levels of Trust correspond to lower scores of Positive Emotions at the same level of valuing Privacy. Thus, the effect of Privacy on Positive Emotions depends on the level of Trust.

Figure 5

Predicted Scores of Positive Emotions for different levels of Trust moderating Privacy



In contrast, no support was found for Perceived Risk being a moderator (Table 5). The interaction effect with Privacy on Negative Emotions was insignificant (b= 0.003, p = .969), as was the interaction effect on Positive Emotions (b= -0.17, p = .121). Thus, Ha6 was left unsupported.

Table 4

Regression Table – Interaction Effects of Trust and Privacy on Negative and Positive Emotions

Variable	*b*	*SE*	*p*
DV: Negative Emotions			
intercept	2.261	1.69	0.187
Privacy	0.53	0.304	0.088
Trust	0.188	0.487	0.701
Privacy*Trust	-0.103	0.091	0.266
R^2	0.243		
DV: Positive Emotions			
intercept	6.827***	1.599	0.000
Privacy	-0.81**	0.288	0.007
Trust	-0.613	0.46	0.189
Privacy*Trust	0.194*	0.086	0.029
R^2	0.286		

*$p < .05$. **$p < .01$. ***$p < .001$

Table 5

Regression Table – Interaction Effects of Perceived Risk and Privacy on Negative and Positive Emotions

Variable	*b*	*SE*	*p*
DV: Negative Emotions			
intercept	-0.015	1.742	0.993
Privacy	0.018	0.336	0.956
Perceived Risk	0.891*	0.408	0.034
Privacy*Perceived Risk	0.003	0.075	0.969
R^2	0.638		
DV: Positive Emotions			
intercept	2.59	2.528	0.310
Privacy	0.532	0.487	0.280
Perceived Risk	0.522	0.592	0.383
Privacy*Perceived Risk	-0.172	0.109	0.121
R^2	0.246		

*$p < .05$. **$p < .01$. ***$p < .001$

Discussion

The aim of this study was to find out the contribution that Privacy as a personal value can make towards explaining Emotions towards smart home devices next to personal Security values. Moreover, it was investigated what role Trust in the service provider and Perceived Risk play in this relationship. In short, it has been found that Privacy as a value scale is indeed separately explaining Emotions next to Security which has been found not to have a significant effect in this study. Furthermore, there was support for Trust as a moderator whereas Perceived Risk was found to have a more direct effect. To conclude, some of the hypotheses could be supported as elaborated on in the following.

The role of Security and Privacy Values

Firstly, there was no support found for a correlation between the Security value and Emotions towards smart home devices in either direction, that is neither Positive nor Negative Emotions. Therefore, "*Ha1: The value security is negatively correlated with emotions towards smart home devices.*" must be rejected.

In contrast, the personal Privacy value has been found to correlate with both Negative and Positive Emotions towards smart home devices. Particularly, in line with hypothesis 2, the higher one values Privacy, the more Negative and the less Positive are one's emotion.

Considering the value of the newly devised Privacy scale in addition to Schwartz's Security scale, Kim et al. (2008) point out that Security and Privacy are valued independently from one another. This study shows that this also holds for Security, conceptualised as personal safety, and Privacy. So, the results could add another facet to the fact.

However, it is surprising that the result for Security was insignificant as cybersecurity has been regarded to be a major concern for IoT users, even more so than Privacy (as cited by Khan et al., 2016) and to also play a significant role in the adoption decision of smart devices (Cannizaro et al., 2020). Likewise, Desmet and Roeser (2016) have postulated that values influence Positive and Negative Emotions towards technologies. Considering the prevalence of Security as a concern, it would have made sense to find a correlation albeit it must be noted that their conceptualisation of security was not based on Schwartz's personal security value.

On the other hand, there are potential explanations for the fact that no correlation was found in this study. To begin with, the hypothesis was based on the idea that Security Values would have an effect if perceived to be under threat (Contzen et al. 2021). However, Barth and De Jong (2017) refer to a number of possible biases in the risk evaluation process.

Naturally, this process, however, is necessary to arrive at the conclusion that one's personal security is under threat. One example of such a bias, that Barth and De Jong (2017) refer to, would be lacking awareness of specific negative consequences or an underestimation of their probability, in this case to one's personal security that may result from using a smart home device. This means that, even if there is a general risk perception, this does not need to translate into the perception that one's personal security is under threat if someone lacks the information of the precise negative consequences to their personal security specifically. More specifically, if someone is not aware that a leakage of personal information might lead to identity theft or a burglary in a moment where the house is unsupervised, personal security will not be perceived to be under threat, whereas the perceived risk of data leakage or an uncertainty over who accesses the data might be present.

In sum, this study was not able to show that Security Values have an impact on Emotions towards smart home devices. This circumstance may be due to the fact that some factors were left unaccounted for, such as awareness and probability of specific negative consequences.

The role of Trust and Perceived Risk

Next, Trust in the service provider was found to correlate with Emotions. Therefore, it can be concluded that a higher level of Trust in the service provider is related to more Positive Emotions. In short, there was support for "*Ha3: Trust in the service provider has a positive correlation with emotions towards smart home devices.*"

Similarly, it was found that Trust in the service provider further moderates the relationship between the Privacy value and Positive Emotions towards smart home devices. Particularly, the nature of the relationship between valuing Privacy and Emotions depends on Trust in the service provider with lower-than-average levels of Trust corresponding to a stronger decrease in Positive Emotions with increasing scores on Privacy. In contrast, higher-than-average levels of Trust correspond to a weaker decrease of Positive Emotions with higher scores of Privacy Values. The moderation effect was not however found for Negative Emotions. As such Hypothesis 4 "*The correlation of the value privacy and the value security with emotions towards smart home devices is stronger when trust in the service provider is low.*" could be partially supported.

Turning to the role of Perceived Risk, it has been found to have a strong correlation with Emotions towards smart devices. This holds for both Negative and Positive Emotions. To be precise, a higher level of Perceived Risk relates to a higher level of Negative Emotions,

whereas a lower level of Perceived Risk corresponds to a higher level of Positive Emotions. Thus, "*Ha5: Perceived Risk has a negative correlation with emotions towards smart home devices.*" can be confirmed.

Looking at Perceived Risk as a moderator, no evidence could be found to support Hypothesis 6 "*The negative correlation of the value privacy and the value security on emotions towards smart home devices is stronger when perceived risk is high.*" Thus, the relationship between the privacy value and either kind of emotions towards smart home devices was not dependent on the level of Perceived Risk.

Notably, Shuhaiber and Mashal (2019) have shown a direct effect of both Trust and Perceived Risk on attitude toward smart home devices, where attitude is seen as an antecedent to intention to use. As such, the findings in this study contribute to the body of evidence for these results. Moreover, the study results here provide some more differentiation in that they have shown that Trust is mostly related to Positive Emotions. Next to the direct relationship, Trust was also shown to have a moderating role.

Limitations

A few limitations have to be mentioned. To begin with, looking at the insignificant results of Security, a few things might have played a role there. For one, the Security items have performed quite poorly during the reliability tests in the process of data analysis. As such it is feasible to assume that they may not have adequately measured what they had been intended to. Moreover, the items were designed to measure personal security as a value. However, the effect of Security Values might be more prominent when it is conceptualised as valuing security as a characteristic of the used system or technology or the resulting user safety, as Yan et al. (2014) do. In essence, it might have to be specified to more clearly relate to technology, which then would have to be reflected by the items. So, in short, if the security items had been more particular in their reference to IoT technologies, it is reasonable to believe that the results would have been more in line with other literature on this topic.

Another limitation that has to be noted concerns the results as a whole. This point is the limited sample size. A sample size of 54 is rather small, and some effects may have turned out to be significant after all, if the sample size had been larger. Most reasonably this would pertain to the marginally significant correlation with Positive Emotions of Trust and Perceived Risk controlling for each other. Moreover, a large proportion of the sample are students with a mean age of 24. This means that this sample cannot be representative for another population, because, for example, age and income play a role in the usage behaviour

concerning IoT devices (Jaspers & Pearson, 2022), which are covariates that differ for populations other than students and perhaps also for students of different nationalities.

Implications

To account for the limitations concerning the security items, it would seem useful to devise a set of value items on IoT security. An example might be “It is important to me that any IoT device I use, is secured through reliable and strong encryption whenever connected to the internet.”, as encryption is an example of a security characteristic that Khan et al. (2016) mention. Given the rapidly, ever-growing market for smart home devices (Statista, 2021) and the prime importance of IoT security for users (Khan et al., 2016) this seems like a worthwhile addition to a value scale like the PVQ.

Regarding Perceived Risk and Trust, a qualitative follow-up study might be conducted on trust, in order to find out where trust in the service provider comes from and how it can be influenced. That is, there is reason to believe that this trust in the service provider might be misplaced or even present after the service provider has been identified as a potential adversary (Duezguen et al., 2021; Zeng et al., 2017). Understanding how this dynamic comes to be, is therefore not only interesting but should also be regarded before inferring any practicalities. Moreover, next to further practical implications, a study such as this might provide some more in depth understanding on the topic.

That is, any sort of understanding in this regard can help policy makers in regulating the use of and protecting the users of smart home devices. Particularly, the strong correlation between Perceived Risk and Negative Emotions, which then in turn are relevant for behavioural intentions (Ajzen, 1991), can be used to discourage thoughtless, and risky usage of smart home devices. For example, as risks have been found to be manifold, one could decide to give some sort of mandatory risk warning on the packaging of a smart device, similar to the warnings found on cigarette packaging (in Germany). This might increase the Perceived Risk associated with IoT devices. Consequently, people would have to reformulate the cost-benefit evaluation, which Jaspers and Pearson (2022) refer to, that would lead to a potentially more safe behavioural decision.

Conclusion

In conclusion, the findings of this study could provide some support for findings of previous studies on the topic. Moreover, the role of Trust in the service provider as a moderator and Perceived Risk as a direct influence on Emotions toward smart home devices

were clarified. Also, Privacy Values have been found to be additionally contributing to explaining emotions independently from Security Values. However, the rapidly evolving nature of the smart home industry calls for ever more research on the issue, not only to gain clarity but also to come to an ultimate conclusion of whether the conveniences of using such devices are actually worth the risks to privacy and security.

References

Agarwal, A., & Meyer, A. (2009). Beyond usability: evaluating emotional response as an integral part of the user experience. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems* (pp. 2919-2930). Doi: 10.1145/1520340.1520420

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376. DOI: 10.1109/COMST.2015.2444095

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS quarterly*, 689-710. https://www.jstor.org/stable/pdf/25750701.pdf

Beldad, A., & Kusumadewi, M. C. (2015). Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. Computers in human behavior, 49, 102-110. https://doi.org/10.1016/j.chb.2015.02.047

Bhattarai, S., & Wang, Y. (2018). End-to-end trust and security for Internet of Things applications. *Computer*, *51*(4), 20-27. DOI: 10.1109/MC.2018.2141038

Cannizzaro, S., Procter, R., Ma, S., & Maple, C. (2020). Trust in the smart home: Findings from a nationally representative survey in the UK. *PLoS One*, *15*(5), e0231615. https://doi.org/10.1371/journal.pone.0231615

Contzen, N., Perlaviciute, G., Sadat-Razavi, P., & Steg, L. (2021). Emotions Toward Sustainable Innovations: A Matter of Value Congruence. *Frontiers in Psychology*, *12*, 2583. https://doi.org/10.3389/FPSYG.2021.661314

Cook, D. J. (2012). How smart is your home?. *Science*, *335*(6076), 1579-1581. DOI: 10.1126/science.1217640

Daubert, J., Wiesmaier, A., & Kikiras, P. (2015, June). A view on privacy & trust in IoT. In *2015 IEEE International Conference on Communication Workshop (ICCW)* (pp. 2665-2670). IEEE. DOI: 10.1109/ICCW.2015.7247581

Desmet, P. M., & Roeser, S. (2015). Emotions in design for values. *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*, 203-219. Doi: 10.1007/978-94-007-6994-6_6-1

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring how privacy and security factor into IoT device purchase behavior. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300764

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, *77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Jaspers, E. D., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255-265. https://doi.org/10.1016/j.jbusres.2021.12.043

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2016). Enabling consumer trust upon acceptance of IoT technologies through security and privacy model. In *Advanced multimedia and ubiquitous engineering* (pp. 111-117). Springer, Singapore. DOI: 10.1007/978-981-10-1536-6_15

Khan, A., Khan, M. M. A., Javeed, M. A., Farooq, M. U., Akram, A., & Wang, C. (2021). Multilevel Privacy Controlling Scheme to Protect Behavior Pattern in Smart IoT Environment. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/9915408

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems, 44*(2), 544-564. DOI: 10.1016/j.dss.2007.07.001

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273-281. https://doi.org/10.1016/j.chb.2018.11.022

Koohikamali, M., Gerhart, N., & Mousavizadeh, M. (2015). Location disclosure on LB-SNAs: The role of incentives on sharing behavior. *Decision Support Systems, 71*, 78-87. https://doi.org/10.1016/j.dss.2015.01.008

Laricchia, F. (2022). Number of digital voice assistants in use worldwide 2019-2024. *Statista*. Retrieved, March 2022, from: https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, *80*, 102211. https://doi.org/10.1016/j.erss.2021.102211

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44. https://doi.org/10.3390/info7030044

Liu, Y., Gan, Y., Song, Y., & Liu, J. (2021). What influences the perceived trust of a voice-enabled smart home system: An empirical study. *Sensors, 21*(6), 2037. https://doi.org/10.3390/s21062037

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Sava, J. A. (2022). Smart home attitudes: Security/safety vs. concerns of being spied on 2021, by country. *Statista*. Retrieved from: https://www.statista.com/forecasts/1227824/smart-home-security-safety-vs-privacy-concerns

Schwartz, S. H. (2012). An Overview of the Schwartz Theory of Basic Values. *Online Readings in Psychology and Culture, 2*(1). https://doi.org/10.9707/2307-0919.1116

Schwartz, S. H., & Boehnke, K. (2004). Evaluating the structure of human values with confirmatory factor analysis. *Journal of Research in Personality*, *38*(3), 230–255. https://doi.org/10.1016/S0092-6566(03)00069-2

Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., ... & Konty, M. (2012). Refining the theory of basic individual values. *Journal of personality and social psychology*, *103*(4), 663. Doi: 10.1037/a0029393

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in Society, 58*, 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

Statista (2021). *Smart Home Revenue*. Statista. Retrieved, June 2022, from: https://www.statista.com/outlook/dmo/smart-home/worldwide

Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social and Personality Psychology Compass*, *13*(11), e12507. https://doi.org/10.1111/spc3.12507

Ukil, A., Bandyopadhyay, S., & Pal, A. (2014). IoT-privacy: To be private or not to be private. In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 123-124). IEEE. DOI: 10.1109/INFCOMW.2014.6849186

Weaver, C. E., Lazaros, E. J., Zhao, J. J., Davison, C. B., & Truell, A. D. (2020). The Internet of Things: An overview of selected smart home technology. *Issues in Information Systems*, *21*(2), 43. https://doi.org/10.48009/2_iis_2020_43-48

de Wildt, T. E., van de Poel, I. R., & Chappin, E. J. (2022). Tracing Long-term Value Change in (Energy) Technologies: Opportunities of Probabilistic Topic Models Using Large Data Sets. *Science, Technology, & Human Values*, *47*(3), 429-458. https://doi.org/10.1177/01622439211054439

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications, 42,* 120-134. https://doi.org/10.1016/j.jnca.2014.01.014

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (pp. 65-80).

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-20. https://doi.org/10.1145/3274469

Appendix

Appendix A
Questionnaire

Informed consent

In this online questionnaire, we will ask you a couple of questions about your personal values applied to the smart home context as this is something that has gained relevance in recent years. The survey may take between 20 and 30 minutes.

Your answers will be handled confidentially, which means no third parties can access the answers of the questionnaire. Furthermore, your answers will be anonymised, the answers you give cannot be traced back to you.

Also, please be aware that your participation is voluntary, thus if you no longer wish to participate, you can withdraw from the study at any time. Moreover, while there are no known side effects of participating in this study, if something should come up you can refrain from going on with the questionnaire or withdraw your consent.

If you want to start this survey, please click “yes” to indicate you have understood and consent to the terms of this study.

Questionnaire Part 1

Privacy

1. It is important to me to protect my privacy
2. It is important to me to have full control over who accesses personal information about me
3. It is important to me to not share personal information (for example about personal preferences, one’s health, or political and religious beliefs) with unknown others.

Security

1. It is important to me to be personally safe and secure.
2. It is important to me to avoid anything dangerous.
3. It is important to me to live in safe surroundings.

Information about smart speakers

In the following you are going to read some information relating to smart speakers in the home environment. Please take care to read the information attentively.

A smart speaker is a voice command device with an integrated virtual assistant, usually activated by a specific activation word. Amazon Echo is Amazon's smart speaker which responds to 'Alexa' as the activation word. In the context of smart homes, the smart speaker helps to assist in various tasks such as telling you about the weather, creating shopping lists, playing the radio, or controlling other smart home devices (lights, temperature, music, doors and windows, etc.). For this purpose, the device is gathering personal data to achieve a good performance.

Scenario – 1 or 2 (randomised)

The next section presents a scenario. Please read the text very carefully and imagine yourself in the presented situation.

Scenario 1

Imagine that you decided to buy a smart speaker. You have just purchased and installed the smart speaker 'Amazon Echo' in in the living room and are now using it. You know that you can change a number of settings, such as the activation word, the gender of the voice interface, privacy settings and other gimmicks. Keeping this in mind, please answer the following questions.

Scenario 2

Imagine that you live in a shared home and your house mate has decided to buy a smart speaker. Your housemate has just purchased and installed the smart speaker 'Amazon Echo' in the living room and is now using it. You know that a number of settings, such as the activation word, the gender of the voice interface, privacy settings and other gimmicks can be changed. As you cannot make changes yourself, you could ask your housemate to do this for you. Keeping this in mind, please answer the following questions.

Questionnaire Part 2

Positive Emotions

1. The Amazon Echo makes me feel happy.
2. I am satisfied with the Amazon Echo.
3. I am excited about the Amazon Echo.
4. I am pleased with the Amazon Echo.

Negative Emotions

1. I am scared about the Amazon Echo.
2. I am frustrated with the Amazon Echo.
3. The Amazon Echo makes me feel worried.
4. The Amazon Echo makes me react cautiously.

Trust

1. Amazon is trustworthy in handling the information gathered by the smart speaker.
2. Amazon tells the truth and fulfils promises related to the information provided by users of the smart speaker.
3. I trust that Amazon would keep my best interests in mind when dealing with the information gathered by the smart speaker.
4. I trust that Amazon can protect personal information gathered by the smart speaker from unauthorized access.
5. I trust Amazon to do everything they can to protect personal information gathered by the smart speaker.

Perceived Risk

1. In general, it would be risky to let the smart speaker gather my personal information.
2. There would be high potential for loss associated with giving my personal information to Amazon.
3. There would be too much uncertainty associated with giving my personal information to Amazon.
4. Providing Amazon with my private information would involve many unexpected problems.
5. I would feel safe giving my information to Amazon.

Appendix B

Figure B1

Scree plot of Privacy and Security Values

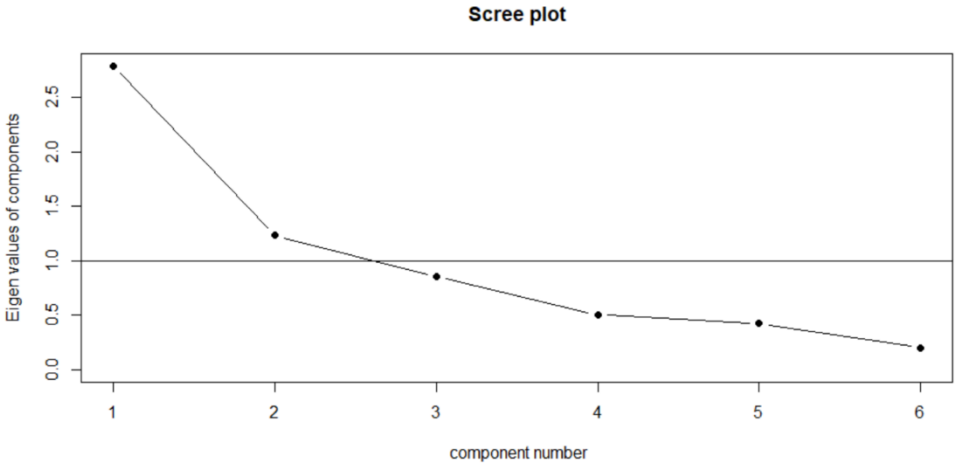


Table B1

Factor Loadings of Privacy and Security Values (Varimax Rotation)

Loadings	Factor 1	Factor 2
Privacy Item 1	0.938	0.255
Privacy Item 2	0.687	0.369
Privacy Item 3	0.596	
Security Item 1	0.402	0.368
Security Item 2	0.280	0.314
Security Item 3		0.997

Appendix C

Figure C1

Scree plot of Positive and Negative Emotions

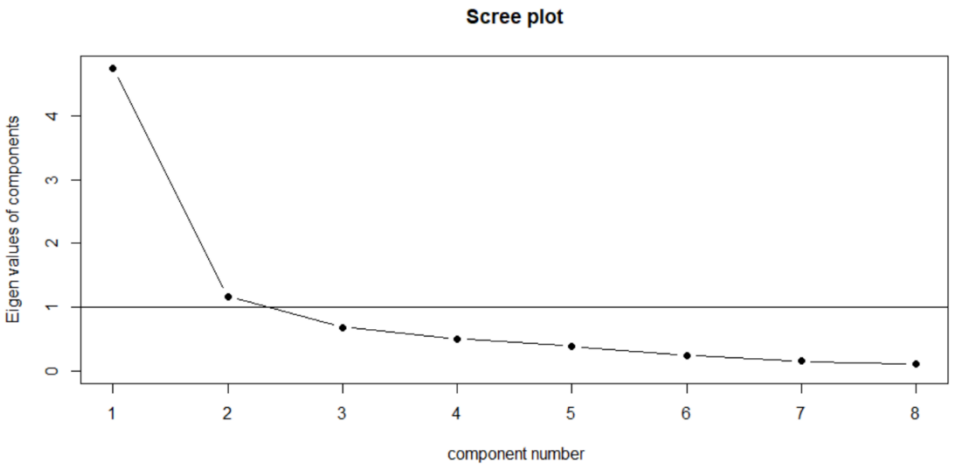


Table C1

Factor Loadings of Positive and Negative Emotions

Loadings	Factor 1	Factor 2
Positive Emotions 1	0.912	-0.255
Positive Emotions 2	0.789	-0.390
Positive Emotions 3	0.560	-0.265
Positive Emotions 4	0.807	-0.306
Negative Emotions 1	-0.158	0.985
Negative Emotions 2	-0.358	0.623
Negative Emotions 3	-0.455	0.693
Negative Emotions 4	-0.383	0.482

Appendix D

Figure D1

Scree Plot for Perceived Risk and Trust

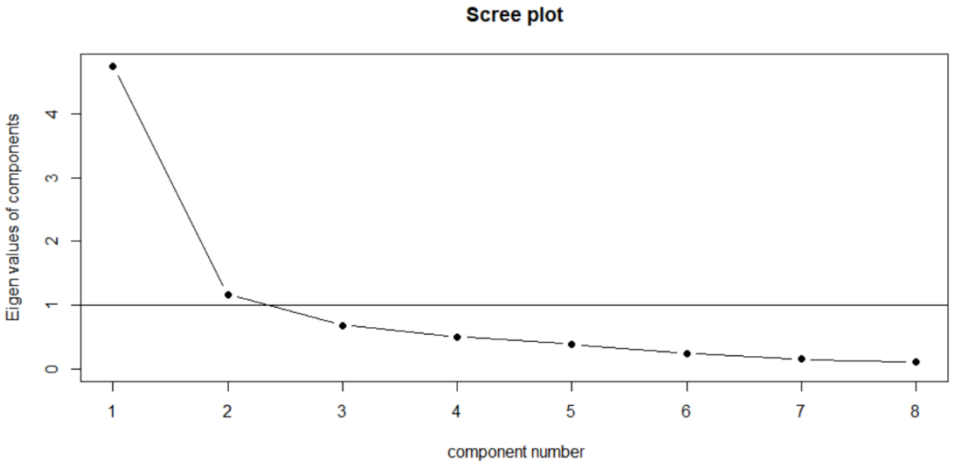


Table D1

Factor Loadings Varimax for Perceived Risk and Trust

Loadings	Factor 1	Factor 2
Trust 1	0.857	-0.232
Trust 2	0.455	-0.143
Trust 3	0.847	-0.220
Trust 4	0.680	-0.232
Trust 5	0.709	-0.269
Perceived Risk 1	-0.274	0.735
Perceived Risk 2		0.669
Perceived Risk 3	-0.365	0.687
Perceived Risk 4	-0.225	0.602
Perceived Risk 5	-0.695	0.371