Investigating Perceived Control, Privacy Values, and Emotions in the Context of Smart Home Devices

Greta Papke
Behavioural Management and Social Sciences, University of Twente
Conflict, Risk, and Safety Psychology
June 30, 2022

Word Count: 8532

Abstract

Smart home devices are of ever growing relevance to the modern world and with a steadily increasing number of smart homes worldwide, they are no longer a concept of science-fiction, but a reality of our globalised life. This is shedding light on the significance of smart home technology, while also raising questions about related privacy implications and respective emotional responses of users. The aim of this paper is to first find out how privacy values may explain positive or negative emotions towards smart home devices and additionally, check for perceived control as a potential moderator influencing this relationship. For this purpose, a scenario study was developed with a between subjects design manipulating perceived control by providing the participants with one of two different scenarios. The aim was to create one high and one low control condition by which it can be observed how privacy values affect emotions based on the induced levels of perceived control. The results of 54 participants showed that firstly, privacy values have a negative influence on emotions towards smart home devices, and secondly that perceived control positively affects the emotions. Because the intended manipulation failed, perceived control was analysed without the manipulation. The results showed that perceived control as such indeed moderates the relationship between privacy values and negative emotions. In conclusion, privacy values and perceived control over personal data seem to be important factors in understanding users' emotions towards smart home devices and should thus be further investigated.

Introduction

Smart devices are of ever-growing significance to the modern world, especially in the context of domestic living. In 2021, there were a total of 258.54 million smart homes worldwide (Statista, 2022), making smart homes not only a concept of science-fiction, but a reality of modern life. Further, the number of smart homes is expected to almost double by 2025, with an estimation of 478.22 million smart homes worldwide (Statista, 2022) underlining the importance of smart homes both in the present moment and in the future.

Smart homes implement various interconnected devices such as smart speakers by using information and communication technologies (Abdi et al., 2019; Guhr et al., 2020), and while there are several benefits attached to the implementation of smart home devices, there are also some concerns to be considered (Wilson et al., 2017). One such concern that has been identified are privacy risks, especially in regards to the continuous collection of personal data and the ability of communication with web devices, posing possible threats to the privacy of personal information (Chhetri & Motti, 2019). To give an example, such threats may be that the user is not even being fully aware about the fact that the device is gathering data at a given moment, or that data is generated without the user's permission (Arabo et al., 2012). In addition, privacy risks have also been found to impact people's intention to use smart home technologies (Guhr et al., 2020). Particularly, due to the close interaction between human and smart devices in smart homes, there is an urgent need to understand individuals' decision making in relation to smart home devices and how their values such as privacy influence adoption decisions of smart home technology.

One factor that seems to be particularly instrumental in this context is emotions. Precisely, emotions have been identified as a key component of user experience and as crucial for understanding the interaction between individuals and technology (Saariluoma, 2020). On a similar note, Desmet and Roeser (2015) argue that technology stands in close relation to people's personal values, through which negative and positive emotions are evoked when using technology. To be precise, technologies are, as the authors argue, either in line with or contradicting moral and personal values and thus evoke positive or negative emotions depending on the extent to which personal values are touched upon. This implies that emotions come up in response to those values relevant in the context of human-technology interaction (Desmet & Roeser, 2015). Therefore, when seeking to understand individuals' adoption decisions of smart home technologies, it seems worthwhile to consider personal values attached to the emotional responses towards the use of technologies.

Based on the abovementioned, when looking at the use of smart home devices, privacy is an important aspect to consider while aiming to understand people's adoption behaviour of said technologies. Moreover, research has shown that values and emotions are key factors considering user experience, and further, that certain values even directly evoke positive or negative emotional responses towards technology. Additionally, privacy has been brought into relation with intentions to use technology several times, indicating that privacy values seem to be an important factor when looking into human-technology interactions. However, less extensively has been measured how privacy applied as such a value relates to the emotions towards smart home devices in particular.

Therefore, the aim of this research is to apply privacy as a personal value to find out whether privacy values indeed influence people's emotions towards smart home devices, as has previously been found for other personal values. For this purpose, an extension of the Schwartz Value Scale (Schwartz et al., 2012) will be employed. Schwartz has extensively researched different values, however, Schwartz' measurement does not include privacy which is why for this study, an independent extension derived from the Schwartz scale will be implemented (Huijts, N.M.A. (manuscript) Do privacy and safety as values influence emotions towards a smart home device?). Whilst this measure for privacy has already been developed, it has not yet been tested much, which will be done within the scope of this study.

Next to investigating emotions towards smart home devices as influenced by privacy values, this study additionally aims to identify whether perceived control over personal data may moderate this relationship between privacy values and emotions. To elaborate, a link between privacy and perceived control has already been found in previous research (Li, 2012; Rieks et al., 2020; Wilkowska et al., 2015). This study aims to take a step further and investigate not only perceived control in relation to privacy, but also to identify a possible influence of perceived control on the relationship between privacy values and emotions. Therefore, the underlying research question of this study is:

"What is the relationship between privacy values and emotions towards smart home devices, and what effect does perceived control over personal data have on this relationship?"

Smart Home Devices

In this study, smart technology in smart homes is going to be investigated. Therefore, it seems worthwhile to first look into the concept of smart homes itself before defining smart devices in the home. While there is no universal definition of the notion of 'smart home', Gram-Hanssen and Darby (2018) provide a concise understanding, stating that a smart home

incorporates communicating, IoT connected (smart) devices to assist in everyday operations. In short, the Internet of Things (IoT) is a network of interconnected smart things, including smart devices (Silverio-Fernández et al., 2018). This interconnectivity of different devices can be understood as the key defining feature of a smart home as it makes use of different devices communicating with one another, allowing a bridge between digital and human interaction (Strengers, 2020). Consequently, the involvement of smart devices is a necessity when it comes to defining smart homes, as they cannot be considered smart without the integration of smart devices which give them their distinguishing features and functions.

While the definition of the IoT and the relation to smart homes may seem readily comprehensible, the definition of a smart device as such has been frequently discussed in literature. Silverio-Fernández et al. (2018) identified connectivity, autonomy, and context awareness as key features defining smart devices. Firstly, connectivity has stood out as the most important feature, being defined as capable of connecting to a network of any size. Secondly, autonomy describes the ability of the device to perform tasks without direct instruction by the user, and lastly, context awareness stands for the capability of the device to detect information about the surroundings by means of a variety of sensors such as microphones or cameras, GPS or accelerometers, distinguishing them from devices such as a keyboard. One aspect that has been outlined by the authors but has not specifically been emphasised as a major feature is the storage of data as part of the previously mentioned aspects. The storage of data, however, may also raise concerns especially in the context of smart homes and related privacy risks.

Privacy

Privacy, as previously mentioned in regards to data collection and handling, is a serious concern in relation to a sensitive context such as smart homes. Even though privacy occurs in different circumstances and the concern for privacy may differ among individuals, the concern for privacy commonly relates to how information is gathered and accessed (Stuart et al., 2019). Viewing this in regards to smart home devices, several issues may occur.

While the context awareness of smart home devices and thus the use of sensors such as cameras or microphones can be of help to the user, it also affects the privacy of their users. Generally, voice assistants do not always ask for permission to perform certain tasks, posing a violation to the user's privacy (Weaver et al., 2020). As an example, Weaver et al. (2020) state the smart speaker Amazon Echo can listen to or record conversations without having been activated by a certain wake word. Moreover, as data gets stored, this may enable outside

parties to access private documents, underlining the threat of possible privacy attacks due to the growing deployment of internet connected smart devices within the home in recent years (Apthorpe et al., 2017). In sum, privacy risks arise when smart devices such as voice assistants gather information by, for example, unknowingly recording the user, or data accessed by unauthorised outside parties, drawing attention to the storage of data as a potential privacy risk since the storage of personal information leaves several options for unauthorised access and the misuse of data.

Considering privacy in the light of smart homes, yet another specific concern regarding privacy may arise. Whilst people are buying smart devices for their home, this does not only affect the person purchasing the device, but also others living in the same household (Zeng & Roesner, 2019). Particularly, in an environment of shared living space, it appears difficult to restrict the use of smart devices to those having purchased the device (the owner of the device), while not also affecting those sharing the same living space in which the smart device is being used. Due to the fact that smart home devices collect personal information, this may give reason for concern about the loss of control over the collection of personal information, leading to unwanted data collection.

Based on the above mentioned discussion about the concept of privacy, privacy values in respect to this study can be understood as valuing the ability to have control over personal data collection and over who can access such personal information.

Values and Emotions

The focus of past research shows that there is a gap in research about the psychological aspects that stand in relation with privacy (Margulis, 2003). Also more recent research shows that, while there is predominantly research done on the technical aspects of smart homes, little has been discussed about the user perspective (Marikyan et al., 2019, as cited in Sovacool & Del Rio, 2020). With the ongoing advancements in technological fields, a direct challenge for people to exercise privacy occurs (Stuart et al., 2019), while at the same time, privacy risks have been found to impact people's intention to use smart home technologies (Guhr et al., 2020). Precisely, an issue arises since on the one hand, there is growing concern for privacy with relevance to the smart home environment while on the other hand, privacy values influence people's adoption behaviour of smart home devices. This, in turn, stresses the importance of considering values such as privacy when looking at individuals' acceptance of smart home technologies.

Moreover, an interview study conducted by Emami-Naeini et al. (2019) has shown that after factors such as functionality and price, privacy has been among the most important factors for interviewees when considering the purchase of an IoT device, stressing the role of user perspective in regards to privacy and smart home devices yet again. This is also in line with what Shuhaiber and Mashal (2019) concluded in their study, stating that the valuing of privacy and thus associated privacy concerns, especially in regards to losing personal data, negatively impact the intention to use smart homes.

Based on these research findings, it seems evident that values, and particularly privacy values play an important role in people's intention to adopt smart home devices. But what has, in addition to that, also been stressed in research is the role that values play in regards to their impact on emotions towards technology. Corroborating this notion, Stuart et al. (2019) have put emphasis on privacy as an important aspect of psychological functioning, especially in regards to emotional well-being, demonstrating the correlation between privacy values and emotions in a broader sense.

A clear demonstration of the correlation between values and emotions in particular towards technology is provided by Contzen et al. (2021). In their work, the authors specifically argue that values explain emotions. Precisely, they argue that positive or negative emotional responses reflect whether or not characteristics of the technology are congruent with these values. This means that positive or negative emotions are evoked when technologies either support or threaten people's core values, showing how values have an immediate impact on people's emotions towards technology.

The results outlined above stress the relevance of these factors and particularly how values and emotions are correlated. Considering the discussion above, it seems reasonable to suggest that privacy values play a role in understanding people's emotions towards smart home devices. However, privacy values alone might not be sufficient to fully explain emotions towards smart home devices as there might be yet other influences on individuals' emotional responses to the use of smart home technology. Thus, it may be advisable to look for more factors other than privacy to understand the emotions of people towards smart home devices. Referring back to the work of Contzen et al. (2021), it can be argued that privacy values may only have an impact on emotions when they are in incongruence with the technology. However, as will be discussed below, there may be factors mitigating this negative impact of privacy values on emotions in the context of smart home technology which is why it seems worthwhile to further look into that.

Perceived Control

Aiming to identify further factors that can influence the relationship between the value privacy on the one hand and emotions on the other hand, conclusions drawn from past research give reason to believe that perceived control may be one such factor as will be explained below. For a better understanding of perceived control and for the purpose of this study, a definition was derived taking into account the privacy risks of smart homes that were discussed above. That is, perceived control over personal information can be understood as:

"The perceived control over the extent to which the user is able to have influence on the data gathered by the device, the way the data is stored, and what happens to the data in hands of outside parties.".

To elaborate on the suggested mitigating influence of perceived control on privacy values and negative emotions, a look can be taken at research proposing a link between privacy values and perceived control. Firstly, Westin (1967) outlined control as an important aspect of privacy, measuring privacy by asking questions such as whether consumers feel like they have lost control over their personal information (Westin, 1967, as cited in Stuart et al., 2019). Additionally, several authors have outlined that there is a correlation between people's perception on privacy risks and their perceived control over a secure use of smart devices with special regard to the handling of data (Klobas et al., 2019; Xu, 2007; Xu et al., 2011).

Similar findings were reported by Li (2012) stating that the perceived ability of control has a negative impact on privacy concerns, indicating that privacy control is a direct precursor of privacy concerns. Consequently, the perceived control over personal data influences individuals' privacy behaviour (Li, 2012). Lastly, Wilkowska et al. (2015) state that the wide deployment of technologies at home may raise privacy concerns and a loss of control. The results of this study have shown that perceived control was a factor that was attributed with high importance in regards to privacy requirements (Wilkowska et al., 2015).

Considering that control is an important aspect of privacy (Westin, 1967, as cited in Stuart et al., 2019), a link between privacy, perceived control and emotions also becomes clear. That is the possible downside of smart home devices, namely loss of control over the data that is gathered and stored during the use of smart devices. Precisely, at this point there is an incongruence between valuing privacy, and the characteristics of smart devices, that threaten the aspect of control in privacy. Resorting to Contzen et al. (2021) this is the point where it is reasonable to assume that perceived control influences the relationship between privacy values and emotions towards smart home devices.

To elaborate on the reasoning behind why to expect such a link presuming that privacy is a core value, this value will have an influence on an individual's emotions if not congruent with the device's characteristics (Contzen et al., 2021). That is, if using the device implies a threat to the person's privacy values, said values will negatively influence the emotions towards the device. Elaborating on this, the use of smart home devices imply threats or risks for example when data about the user is gathered without consent (Arabo et al., 2012), conflicting with the user's privacy values.

While the link between privacy and perceived control has previously been established, it can be expected that, in the presence of perceived control over personal information, the threat to the individual's privacy values will be perceived less heavily. To elaborate, it can be reasonably assumed that perceived control over personal data mitigates the perception of threat to privacy values caused by the device, since more control over personal information would suggest a higher sense of privacy. In turn, since the presence of perceived control arguably mitigates the threat to privacy values, and emotions would only be negatively influenced when these values are under threat, emotions towards the technology would not be influenced as negatively when perceived control functions as a moderator between these two variables.

In sum, despite the fact that there is not yet literature on combining the three variables privacy, perceived control, and emotions, in previous research, perceived control and privacy have been linked in several ways. In this study, however, it is of particular interest how privacy as a value has stronger or weaker effects on emotions depending on the level of perceived control. Concretely, based on the preceding argumentation, it can be expected that privacy will have less of an impact on emotions under the presence of perceived control mitigating this influence. Consequently, the effect of privacy on emotions towards smart home devices depends on the level of perceived control. To be precise, higher perceived control means that the impact of privacy concerns on negative emotions would be lower.

All in all, this research first seeks to find out how values such as privacy may explain positive or negative emotions towards smart home devices and additionally, check for perceived control as a potential moderator of this relationship.

Hypotheses

In order to provide answers to the questions raised above, several hypotheses can be formulated based on the aforementioned discussion of literature. A conceptual model of which is displayed in figure 1. Firstly, privacy has generally been outlined as a factor of

relevance in regards to the use of smart home devices. Further, it has been shown that values can generally influence people's emotions towards smart home technology. Now in respect to privacy values in particular, this value will have an influence on an individual's emotions if there is incongruence with the device's characteristics. That is, if using the device implies a threat to the person's privacy values, privacy will negatively influence the emotions towards the device. Therefore, the first hypothesis is:

H1: *The value privacy is negatively correlated with emotions towards smart home devices.*

It is hypothesised that an individual in need of having control over the collection of their personal information would have more negative emotions towards smart home devices if perceived control is low. In contrast, if the person has a perception of control over the smart device and thus their personal information, it could be argued that this person may have more positive emotions towards the smart home device. Moreover, as technologies cannot only threaten values, but can also support them, namely if they are congruent with the values (Contzen et al., 2021), the perceived control of someone valuing their control over smart home devices may thus imply positive emotions towards the technology. Therefore, the second hypothesis is:

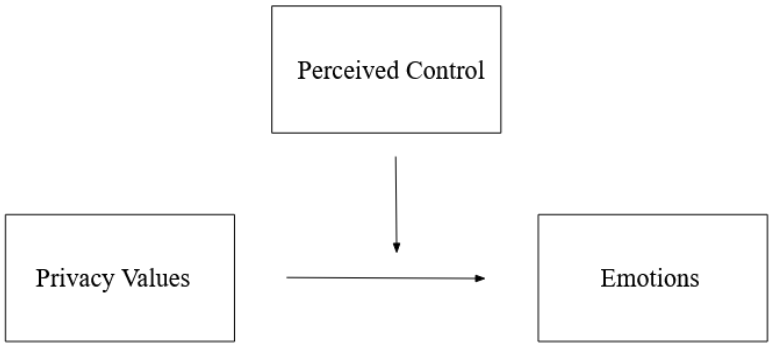
H2: *Perceived control has a positive correlation with emotions towards smart home devices.*

Thirdly, based on the research implications of Contzen et al. (2021) which were discussed above, perceived control over personal data may be able to mitigate the perception of threat to privacy values caused by the technology, since more control over personal information would imply a higher sense of privacy. Precisely, it is hypothesised that the presence of perceived control weakens the threat to privacy values, and because emotions would only be negatively influenced when these values are under threat (Contzen et al., 2021), emotions towards the technology would not be influenced as negatively when perceived control functions as a moderator between these two variables. Consequently, the last hypothesis is:

H3: *The correlation of the value privacy with emotions is weaker when the perceived control over private data is higher.*

Figure 1

Conceptual Model



Methods

Research Design

The dependent variable that was investigated is *emotion*. The variable *emotions* entails the feelings that are triggered by or relate to the smart home device in question. The *privacy value* in the context of the first hypothesis, or *perceived control* in regards to the second hypothesis thought to influence these emotions was therefore the independent variable. First, the aim was to test the direct effect of the value-emotion relationship. Next, the variable *perceived control* was tested for moderation. Precisely, the aim was to manipulate perceived control using two experimental conditions by means of two different scenarios of which only one was presented to the participants, indicating high and low control to test the hypothesised effect of the *perceived control* variable on the relationship between privacy values and emotions.

Participants

The questionnaire of this study was administered to participants that were recruited using the SONA-system for students of the University of Twente. Additionally, a convenience sampling method was used, that is, further 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 be 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. The participants signed up voluntarily and the study has been approved by the university's ethics committee.

The initial data set consisted of 87 participants that completed the questionnaire. Of these, 26 participants had to be excluded due to missing answers, 7 further responses were excluded because of a failed attention check. This left a final number of 54 participants between the ages of 18 and 58 (M = 24.61, SD = 10.37). Concerning the two experimental conditions used in the questionnaire, the participants were equally divided upon the conditions which left a total of 27 participants per condition. The majority of respondents was female (N = 30, 55.6%). As for education, most respondents indicated having achieved their high-school diploma (N = 37). There was one response for having achieved a Havo degree indicating the lowest possible category, while there were two responses for the highest possible category 'PhD'. Moreover, 8 participants specified "other". In Table 1, the complete information on demographic data is provided.

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 have been informed about the purpose and implications of the study and were asked to give consent. Afterwards, the participants were provided with a general section in which they had to fill in demographics such as gender, nationality, age, or education. The section that followed next included the questions about the participants' values regarding privacy. In addition, distractor items had to be answered as part of this section in order to avoid making the participants aware of the explicit purpose of the study. The order of the items of this section was completely randomised. Next, they were provided with general information on what a smart device is and what it is capable of in terms of performed tasks (Appendix A).

Afterwards, the participants were randomly assigned for one of two possible experimental conditions. These conditions used to test *perceived control* as the presumed moderator aimed to either test for high control or low control relating to the smart speaker. This was operationalised by providing two scenarios, one for the high control condition and one for the low control condition. In short, this was manipulated using the scenario of being the owner of the smart speaker for high control as opposed to not being the owner of the device for low control over personal data. The full version of both scenarios can be found in Appendix A.

Lastly, after reading through the given scenario, participants received the part of the questionnaire entailing the scales testing for the emotions of the participants, the scale testing for the potential moderator *perceived control*, and the scales for presumed corresponding moderators irrelevant for this specific research question. However, participants were provided with the items of all scales in addition to the scale of perceived control due to the joined research process.

Measurements

As implied above, it needs to be noted that this research was conducted in cooperation with several researchers. Therefore, the questionnaire used also contained scales testing different potential moderators not used for the current study. For answering the research question of the current study, three different scales were used. The first scale aiming to measure the independent variable *privacy*, was derived from the Schwartz scale, employed in the style of the PVQ items as a supposed independent extension (Huijts, N.M.A. (manuscript) Do privacy and safety as values influence emotions towards a smart home device?) (Appendix A). In between 22 distractor items on other values (Appendix A), the privacy scale

entails three items for which an example would be “It is important to me to protect my privacy”.

The dependent variable *emotion* was measured in a scale using a total of eight items following a structure such as “to what extent do/would you feel *emotion* about the device?” (Appendix A). The feelings in question were grouped into negative and positive emotions that seem to be reasonable reactions to the smart home devices. That is, for example, 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.” as example items for both possible negative and positive feelings towards the chosen smart home device.

Finally, the scale *perceived control* (Appendix A) was specifically designed for the purpose of this study. It consisted of 7 items in total including items such as “I feel in control of what happens to my data”, or “I feel in control of the amount of personal information the smart speaker collects about me”. All scales were labelled using a 7-point Likert scale ranging from 1 = completely agree to 7 = completely disagree. Furthermore, to ensure consistency among the items of the questionnaire and to avoid possible confusion among participants, all items including those derived from the Schwartz scale were adopted and formulated in a first-person perspective. An additional reason for that was to potentially make it easier for participants to relate to the questions as the questionnaire was set up in a way asking participants to imagine themselves in a given situation.

Data Analysis

To test the hypotheses, a number of statistical analyses were run using the software RStudio.

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 by computing the Kaiser-Meyer-Olkin measure and conducting a Bartlett sphericity test for each set of relevant variables. One set of data included the emotion items, another set contained the privacy value items, and additionally security items taken from the Schwartz Value Scale (Appendix A). To elaborate, both security and privacy values were tested for, since the privacy scale was derived from the security scale so there might be overlap. Moreover, security was included as a control variable. Finally, the last data set contained only the potential moderator perceived control. 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, showing 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 by computing Cronbach's alpha. Additionally, it was considered whether dropping some items might lead to a higher measure of internal consistency of the factors. However, no item was excluded.

Afterwards the reliable items were combined into the respective variables, perceived control, negative emotions, positive emotions, and privacy values by averaging them. Then, a correlation matrix was computed on all relevant variables. Next, a number of 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.

Results

Factor Analysis

First of all, the reliability of the newly employed privacy scale was established by doing a factor analysis. In order to check the scales' eligibility for factor analysis, the Kaiser-Meyer-Olkin criterion and Bartlett sphericity test were conducted. The privacy value scale as well as the security scale have been found to be suitable for factor analysis. Therefore, a factor analysis was performed on both scales together. The eigenvalue and a scree plot (Figure B1) suggested 2 factors as two values were reported above 1. The factor analysis for the personal values (security and privacy) loaded properly on the intended factors, except for security item 1 "It is important to me to be personally safe and secure.", which loaded more on the privacy factor (Table B1). This shows that there is indeed some overlap. However, as the security scale was only used as a control variable in this study and has previously been validated, the item was left in the 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 (Figure B2). Here, the factor loadings showed that positive and negative emotions are two separate factors with the factor loadings properly indicating that the items fit their respective emotion (Table B2).

As well as the previous scales, the perceived control scale was found to be suitable for factor analysis according to all the statistical criteria. According to the Kaiser's criterion, 1

factor was identified, as well as the scree plot (Figure B3) showing 1 factor with the factor loadings loading properly on that one factor (Table B3).

For the scales' reliability, Cronbach's alpha was considered. The privacy scale's reliability is good with $\alpha = .775$. Both emotion scales performed well, with $\alpha = .891$ for positive emotions and $\alpha = .853$ for negative emotions. With $\alpha = .903$, the perceived control scale was also deemed reliable.

Descriptives

Next described are the descriptive statistics for the privacy scale and the perceived control scale. On the privacy scale ($M = 5.17$, $SD = 1.27$), respondents indicated a moderately high level of agreement with the items. Lastly, a moderately low mean score of $M = 2.59$ with a standard deviation of $SD = 1.11$ was reported for the items of the perceived control scale.

Correlations

Further, a correlation matrix was computed yielding the results as specified in Table 2.

Table 2

Correlation Matrix

Variable	*M*	*SD*	1	2	3
1 Privacy	5.17	1.27			
2 Perceived Control	2.59	1.11	-0.27*		
3 Negative Emotions	4.11	1.21	0.33**	-0.23	
4 Positive Emotions	3.62	1.22	-0.34**	0.40**	-0.61***

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

Manipulation Check

To check if the manipulation of perceived control was successful, first a manipulation check was performed using a two-sided t-test in order to identify the group means and whether they are truly different. A difference in means of the two conditions could be identified in line with the expectations. Precisely, the mean score of the high control condition was $M = 2.66$, whereas the mean of the low control condition was $M = 2.51$.

However, the t-test showed that the difference was statistically insignificant (t(50.6) = 0.5, p = .617), meaning the manipulation failed or the hypothesised effect did not occur. For this reason, the influence of perceived control as such was measured using the devised scale instead of treating it as a manipulated variable. Therefore, in the following, instead of comparing groups, individual levels were compared.

Regression Analysis

The first hypothesis "*The value privacy is negatively correlated with emotions towards smart home devices.*" was tested specifying a model with privacy as the independent and first negative, then positive emotions as the dependent variable (Table 3). In both cases, the effect was significant. That is, privacy values affect negative emotions (b = 0.31, p = .015) and positive emotions (b = -0.33, p = .012). Since this also aligns with the hypothesised directions, the findings support H1. In a model including security as a control variable (Table B4), privacy values again affect both negative emotions (b = 0.34, p = .015) and positive emotions (b = -0.38, p = .007) significantly. Both the effect sizes and the significance levels of privacy are slightly higher when security as a control variable is included.

Table 3

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

Variable	Estimate	*SE*	*p*
DV: Negative Emotions			
intercept	2.49***	0.67	0.000
Privacy	0.31*	0.12	0.015
R^2	0.11		
DV: Positive Emotions			
intercept	5.31***	0.67	0.000
Privacy	-0.33*	0.12	0.012
R^2	0.12		

For the second hypothesis: "*Perceived control has a positive correlation with emotions towards smart home devices."*, the direct effect between perceived control and emotions was tested using a model with emotions as the dependent variables each, and

perceived control as the independent variable (Table 4). The results show a marginally significant negative effect of perceived control on negative emotions (b = -0.25, p = .096), and a significant positive effect on positive emotions (b = 0.45, p = .003). This is in line with the expected directions, providing support for H2.

Table 4

Regression Table – Main Effects of Perceived Control on Positive and Negative Emotions

Variable	Estimate	*SE*	*p*
DV: Negative Emotions			
intercept	4.75***	0.41	0.000
Perceived Control	-0.25	0.15	0.096
R^2	0.05		
DV: Positive Emotions			
intercept	2.49***	0.39	0.000
Perceived Control	0.45**	0.14	0.003
R^2	0.16		

The last hypothesis *"The correlation of the value privacy with emotions is weaker when the perceived control over private data is higher."* was tested using a model with privacy/perceived control as the independent variables and each negative and positive emotions as the dependent variables to check for the possible moderation of perceived control on privacy and emotions (Table 5). Considering the interaction effect, the regression analysis showed an insignificant positive effect of privacy on positive emotions (b = 0.159, p = .129) depending on the level of perceived control. As for negative emotions, the regression analysis showed a significant negative effect of privacy (b = -0.313, p = .003) moderated by perceived control. These results support H3 indicating a moderating effect of perceived control on privacy values and emotions.

A simple slopes analysis was performed for a visualisation of this interaction effect (Figure 2). Looking at the slopes, first, it is visible that increasing privacy values lead to increased negative emotions. Furthermore, negative emotions for individuals with lower levels of perceived control are relatively high when having high privacy values. Lastly, higher-than-average levels of perceived control with the same level of privacy values

correspond to lower scores of negative emotions, showing the moderating effect of perceived control on the relation between privacy values and negative emotions.

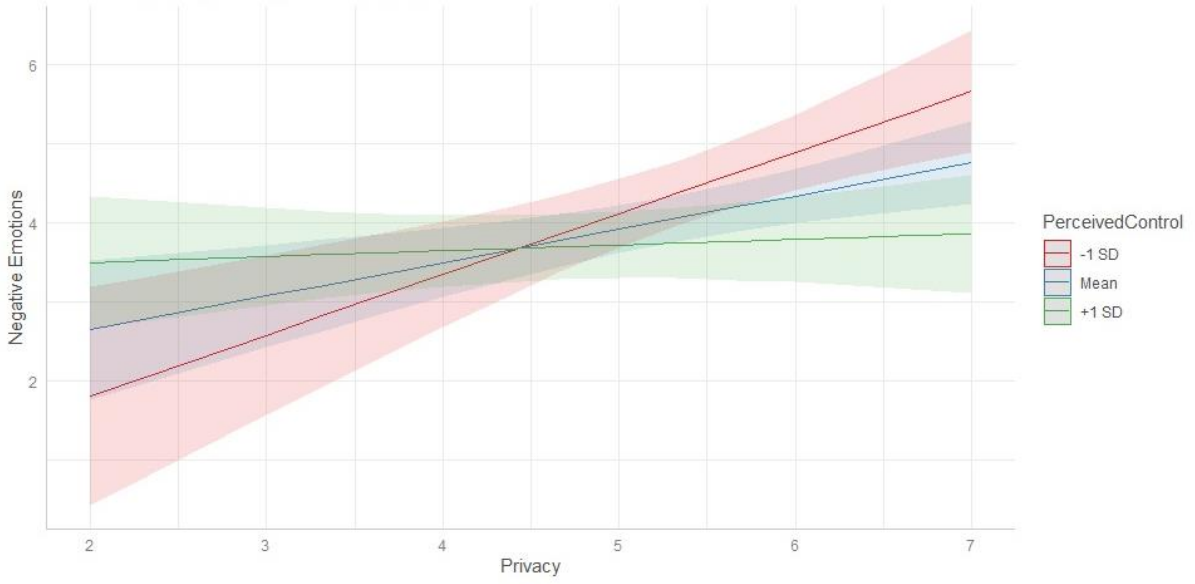
Table 5

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

Variable	Estimate	*SE*	*p*
DV: Negative Emotions			
intercept	-1.76	1.78	0.327
Privacy	1.23***	0.33	0.001
Perceived Control	1.38*	0.52	0.012
Privacy*Perceived Control	-0.31**	0.1	0.003
R^2			
DV: Positive Emotions			
intercept	6.42***	1.81	0.001
Privacy	-0.73*	0.34	0.035
Perceived Control	-0.43	0.53	0.425
Privacy*Perceived Control	0.16	0.1	0.129
R^2			

Figure 2

Predicted Scores of Negative Emotions for different Levels of Perceived Control moderating Privacy



Discussion

The aim of this study was to establish the relationship between privacy values and emotions towards smart home devices. Further, an experimental manipulation of perceived control was used to find out if perceived control moderates the relationship between privacy and emotions. That is, the focus of this research was on studying the relation between all three variables which has not been studied before, answering the question if the effect of a person's privacy values on the related emotions depend on their perceived control over their personal data which the smart home device (smart speaker) gathers.

Findings

Regarding the first hypothesis which aimed to test emotions considering privacy values, it was expected that a high value of privacy in a person would negatively influence their emotions towards smart home devices. Indeed, the results were significant for both negative and positive emotions in line with the expected outcome, supporting the hypothesis. These findings imply that a high importance of privacy positively correlates with negative emotions, meaning that with a high sense of privacy, emotions towards smart home devices

are more negative. In turn, the results show that higher values of privacy correspond to decreasing positive emotions towards smart home devices.

The second hypothesis aimed to test the direct effect of perceived control on emotions towards smart home devices with a hypothesised positive correlation between perceived control and emotions. The results showed significant effects of perceived control on emotions in line with the expected directions, indicating that individuals with a higher sense of perceived control have less negative emotions, and by the same token more positive emotions towards smart home devices

Lastly, the third hypothesis aimed to identify if perceived control moderated the relationship between privacy values and emotions. The aim was to manipulate perceived control by providing two different scenarios for high control and low control to observe how their privacy values affect emotions based on the induced levels of perceived control However, the manipulation check showed no significant effect. Nonetheless, a trend towards the expected differences between the groups of high and low control could be observed showing higher levels of perceived control in participants allocated to the high control condition and lower levels for those in the low control condition.

Several reasons can be considered providing possible explanations for the failed manipulation. The first possible reason to think of is that the choice for and formulation of the scenarios was not optimal, leading to no significant difference in the groups per scenario. To elaborate, the difference of the two situations that should manipulate the sense of perceived control may not have been strong enough, thus not causing the desired difference in the participants' understanding of perceived control in regards to the situation they were given.

Another reason for the failed manipulation may be that participants were not aware that there was another possible situation thus not paying much attention to the respective level of perceived control in their given situation. Instead, their focus may have rather been on their general perception of control, regardless of considering what being or not being the owner would imply as this comparison between both situations was not possible due to the lacking awareness of the respective other possible situation.

Yet another possible reason may be the very limited overall number of participants and thus a limited number of respondents per scenario. As a trend towards the expected outcome was visible, it may be that the difference would become significant with an increasing number of participants. To see if this would indeed be the case, further research should be conducted with a larger sample size. Additionally, Yao et al. (2019) stress the

importance of considering not only the privacy perceptions of end users or device owners, but also those of people who are not the owners such as family members or visitors. This supports the suggestion that there may indeed be a difference in privacy perceptions between owners and non-users. Further, the authors explicitly mention asking for control over the device as one identified mitigating factor of privacy concerns, highlighting the link between perceived control and privacy perceptions (Yao et al., 2019).

Considering the results for Hypothesis 3 treating perceived control as such, that is without considering the experimental conditions because of the failed manipulation, the findings of this study indeed show that perceived control plays a role in privacy values and their influence on emotions. Precisely, the findings provide significant results showing that the base relationship between high privacy values and negative emotions depends on the extent of perceived control, indicating that if an individual has high perceived control, the strength of the base relationship decreases. Therefore, negative emotions do not increase as strongly as a result of high privacy concerns due to the influence of perceived control. However, no significant moderation was found for positive emotions.

Limitations

Despite the valuable findings this study provided which are outlined above, there are also some limitational factors that need to be considered. One limitation of this study was a considerably small sample size. Due to a very limited time frame, only a small number of respondents could be recruited for this study. Furthermore, as true for all studies, needs to be taken into account that the possibility of a biassed sample exists. Due to the nature of the data collection process, mostly young participants of academic backgrounds took part in this study. Consequently, this sample may not be representative of the population, leaving the possibility that this influenced the results of the study because of possible factors that may only be characteristic for this specific group.

Additionally, a further limitation was the failed manipulation of perceived control. Despite the fact that perceived control as such could successfully be measured, the experimental control manipulation was insignificant. This may indeed suggest that the respondents' focus may have rather been on their general perception of control, instead of putting much importance on the context in which they should imagine using the smart device, since the findings for overall perceived control were significant. Nonetheless, when aiming to study manipulated perceived control, improvement for the implemented manipulation of perceived control is suggested.

Implications and Recommendations

The findings of this study shed light on the relevance of privacy values in the smart home context, and additionally on the role of perceived control in relation to privacy concerns and emotions towards smart home devices. Thus, it would generally be recommendable to enhance people's perceived control over their personal data and therefore decrease people's privacy concerns and their negative emotions towards the devices. This, however, leads to the question if this influence is achieved by perceived control or perhaps rather because of actual control over the handling of one's own data. It may be reasonable to suspect that with increasing actual control, an individual's perceived control may increase as well. Therefore, it seems appropriate to consider improving the ways in which people can have actual control over the handling of their data, for example by improving people's access to certain privacy settings or providing more information on privacy implications regarding the smart home device in use, which in turn, would arguably increase their sense of perceived control and thus positively influence privacy concerns and respective emotions towards the device.

An alternative, yet not necessarily opposing view on perceived control in this regard is suggested by Rieks et al. (2020), stating that the link between privacy values and perceived control might be under the influence of a third variable. As an example, the researchers argue that an individual's knowledge about privacy in general, and privacy policies or possible ways to ensure the protection of privacy in particular would reasonably have an impact. Namely, individuals with higher privacy values may put more effort into protecting their privacy and thus may seek for more knowledge about ways to control their personal data.

Applying that to the context of this study, greater knowledge about how to control personal information may arguably also lead to greater perceived control, and thus to a positive influence on emotions towards the smart home devices in question. This would be in line with the third hypothesis, since a greater value of privacy and thus, as the authors argue, a potentially increased need for knowledge followed by higher perceived control would then lead to a decrease in negative emotions towards the device. Additionally, it underlines the recommendation of enhancing people's perceived control by improving the information about privacy implications available to them and the ways in which these can be accessed.

However, in contrast to this recommendation stands the fact that in terms of both privacy and perceived control, it is still difficult for users to act in a way to exert their need for control over personal data and thus their privacy. As outlined by Tucker (2018), people

have difficulties gaining such knowledge as it takes too long to read through the privacy implications given by providers. Precisely, even 10 years ago, it was unrealistic to assume consumers would be able to read through privacy policies and inform themselves properly about the ways in which their data is used, since reading the privacy information would take around 244 hours per year (McDonald & Cranor, 2008, as cited in Tucker, 2018). Noting this estimate was made 2008, with ongoing advancements of technologies, the increase of time of reading through policies can be reasonably imagined. Consequently, more difficulties to properly comprehend privacy information due to such limiting factors would also potentially lead to less perceived control and in turn to more privacy concerns negatively impacting the emotions towards these smart home technologies.

Therefore, a future recommendation for providers of smart home devices would be to improve the situation concerning individuals' possibilities to exert actual control over their protection of their data and ensure better ways to access information about privacy implications. A concrete example for how this could be achieved is making privacy policies more accessible in terms of phrasing or making it mandatory for the service provider to start off the policy with a list of bullet points, summarising the most important takeaways from the policy. In line with this is the recommendation given by Yao et al. (2019), which was specifically formulated aiming to improve privacy implications in the context of smart homes. The authors highlight transparency as one important factor when it comes to privacy perceptions, and thus argue that sufficient information should be provided. Precisely, the authors state that purposes of smart home devices should be clear to the user, and information such as whether or not data is collected and stored should be provided by the manufacturer of the device. Their specific recommendation for this is to use a poster with a QR code with which such information can be provided (Yao et al., 2019).

Another recommendation for the improvement of providing information that goes well in line with the previous suggestion would be combining the QR code with the device's app in which privacy policies are provided in a comprehensible, concise manner. A way to further enhance the user's actual control would be to not only provide the privacy information in the app, but also enable them to switch settings in the app easily, based on the information provided there, which should not be lengthy, but readily understandable.

Lastly, Yao et al. (2019) have made yet another recommendation which also reflects the previous suggestion for easily changeable settings, which is the implementation of different modes of the device. To elaborate, the authors suggest that the device's functions can be selectively disabled by means of different modes. This way, different modes could

allow or restrict specific privacy settings which ideally match the user's privacy needs in order to increase the user's perceived control over the information the device gathers and stores, and thus decreasing privacy concerns and negative emotions towards the device.

Finally, several suggestions for further research arise based on the information discussed above. First of all, it can be suggested that further research is conducted accounting for the limitations of this study improving the research. That is, for a possible future study, it should be aimed for a greater sample and when aiming to study the manipulation of perceived control, the conceptualisation of the manipulation should be improved. This could be achieved by providing a more explicit difference between the control conditions, for example by making respondents aware of differing control and privacy implications of the respective situation. Furthermore, a pilot test for the manipulation could be conducted to avoid a failed manipulation.

In addition, future researchers may want to look into possible influences of further variables like knowledge about privacy policies, as suggested by Rieks et al. (2020), or further study the factors Yao et al. (2019) outlined in relation to differences between user and non-user privacy perceptions. Basing further research on the findings of Yao et al. (2019) is of particular interest in the light of this study as the focus has been put on the distinction between ownership of the device and non-ownership with respect to related privacy implications. Further research on this may especially provide valuable insights when not only looking into user and non-user perspectives and the related findings of Yao et al. (2019, but if also special attention is paid to perceived control particularly.

Conclusion

All in all, aiming to determine the relationship between privacy values and emotions towards smart home devices, and additionally how perceived control influences that relationship, the study provided valuable insights especially in regards to the way perceived control influences privacy perceptions. Furthermore, this study implemented a newly developed measurement for privacy, displaying good reliability and a significant effect of privacy on emotions, which showed that this measurement indeed makes sense in explaining how people emotionally respond to smart home devices. Moreover, this paper contributes to the literature as this study focused on variables which have previously not been brought into relation in such a way, and indeed, the relation between privacy values and emotions moderated by perceived control showed a significant effect.

However, as the field of smart home technology is undergoing steady advancements, and there are alternative viewpoints that can be considered when dealing with perceived control as an influencing factor on privacy, a replication study taking into consideration this study's limitations, or future research within this field in general is suggested.

References

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 451-466).

Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., & Feamster, N. (2017). Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. https://doi.org/10.48550/arXiv.1708.05044

Arabo, A., Brown, I., & El-Moussa, F. (2012). Privacy in the Age of Mobility and Smart Devices in Smart Homes. *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*. https://doi.org/10.1109/socialcom-passat.2012.108

Chhetri, C., & Motti, V. G. (2019, March). Eliciting privacy concerns for smart home devices from a user centered perspective. In *International Conference on Information* (pp. 91-101). Springer, Cham. https://doi.org/10.1007/978-3-030-15742-5_8

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

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.

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

Gram-Hanssen, K., & Darby, S. J. (2018). "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science*, *37*, 94-101. https://doi.org/10.1016/j.erss.2017.09.037

Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*, *2*(2), 1-12. https://doi.org/10.1007/s42452-020-2025-8

Klobas, J. E., McGill, T., & Wang, X. (2019). How perceived security risk affects intention to use smart home devices: a reasoned action explanation. *Computers & Security*, *87*, 101571. https://doi.org/10.1016/j.cose.2019.101571

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems*, *54*(1), 471-481. https://doi.org/10.1016/j.dss.2012.06.010

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of social issues*, *59*(2), 243-261. https://doi.org/10.1111/1540-4560.00063

Rieks, A. R., Dedrick, J., & Stanton, J. (2020). Risks, benefits, and control of information: Two studies of smart electric meter privacy. *Journal of the Association for Information Science and Technology*, *71*(9), 1060-1073. https://doi.org/10.1002/asi.24374

Saariluoma, P. (2020). User psychology of emotional interaction—usability, user experience and technology ethics. In *Emotions in technology design: From experience to ethics* (pp. 15-26). Springer, Cham. https://doi.org/10.1007/978-3-030-53483-7_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. https://doi.org/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

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device?-a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, *6*(1), 1-10. https://doi.org/10.1186/s40327-018-0063-8

Sovacool, B. K., & Del Rio, D. D. F. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews*, *120*, 109663. https://doi.org/10.1016/j.rser.2019.109663

Statista. (2022, February 7). *Smart home - Statistics & Facts*. https://www.statista.com/topics/2430/smart-homes/#dossierKeyfigures

Strengers, Y. (2020). Envisioning the smart home: Reimagining a smart energy future 1. In *Digital materialities* (pp. 61-76). Routledge.

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

Tucker, C. (2018). Privacy, Algorithms, and Artificial Intelligence. In *The Economics of Artificial Intelligence: An Agenda* (pp. 423-437). University of Chicago Press.

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

Wilkowska, W., Ziefle, M., & Himmel, S. (2015, August). Perceptions of personal privacy in smart home technologies: do user assessments vary depending on the research method?. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 592-603). Springer, Cham. https://doi.org/10.1007/978-3-319-20376-8_53

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy*, *103*, 72-83. https://doi.org/10.1016/j.enpol.2016.12.047

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. http://aisel.aisnet.org/icis2007/12

Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-24. https://doi.org/10.1145/3359161

Zeng, E., & Roesner, F. (2019). Understanding and Improving Security and Privacy in {Multi-User} Smart Homes: A Design Exploration and {In-Home} User Study. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 159-176).

Appendix

Appendix A
Questionnaire

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

Imagine that you decided to buy a smart speaker. You have just purchased and installed the smart speaker 'Amazon Echo' 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.

Scenario 2

Imagine that you live in a shared home and your housemate 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.

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.

Distractor Items

1. It is important to me to have a good time.
2. It is important to me to enjoy life's pleasures.
3. It is important to me to take advantage of every opportunity to have fun.
4. Learning things for myself and improving my abilities is important to me.
5. Freedom to choose what I do is important to me.
6. I am always looking for different kinds of things to do.
7. Excitement in life is important to me.
8. I think it is important to have all sorts of new experiences.
9. Being very successful is important to me.
10. Being wealthy is important to me.
11. It is important to me to be the one who tells others what to do.
12. Protecting my public image is important to me.
13. Having order and stability in society is important to me.
14. It is important to me to maintain traditional values or beliefs.
15. It is important to me to follow rules even when no-one is watching.
16. I always try to be tactful and avoid irritating people.
17. I try not to draw attention to myself.
18. I go out of my way to be a dependable and trustworthy friend.
19. Caring for the well-being of people I am close to is important to me.
20. I think it is important that every person in the world has equal opportunities in life.
21. I strongly believe that I should care for nature.
22. It is important to me to listen to people who are different from me.

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.

5. I am scared about the Amazon Echo.

6. I am frustrated with the Amazon Echo.
7. The Amazon Echo makes me feel worried.
8. The Amazon Echo makes me react cautiously.

Perceived Control

1. I feel in control of the amount of personal information the smart speaker collects about me.
2. I feel in control of what type of data the smart speaker gathers about me.
3. I feel in control of when the smart speaker is collecting data about me.
4. I feel in control of what happens to my data.
5. I feel in control of who accesses my data.
6. I feel in control of the protection of my data from unauthorised access.
7. I feel in control of how my data is being processed by Amazon.

Schwartz Personal Security Items

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.

Appendix B

Statistical Results

Figure B1

Scree Plot of Privacy and Security Scale

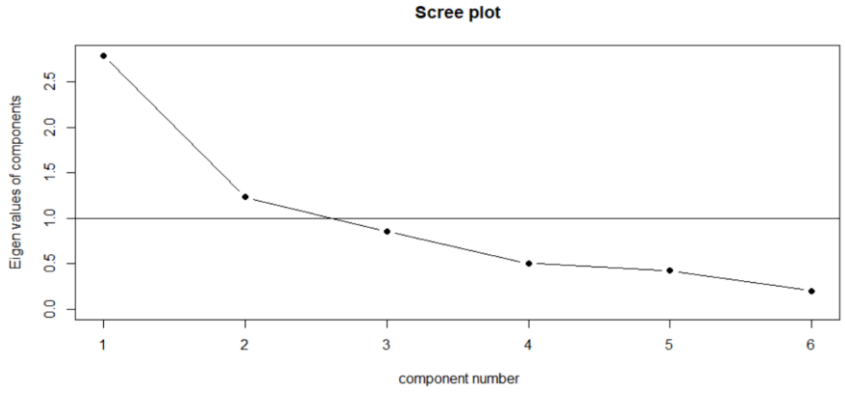


Table B1

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

Figure B2

Emotions Scree Plot

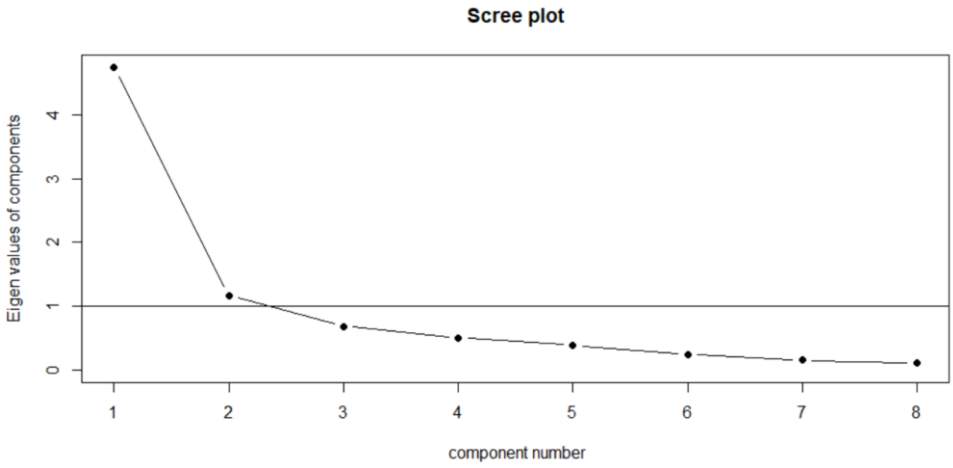


Table B2

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

Figure B3

Scree Plot Perceived Control

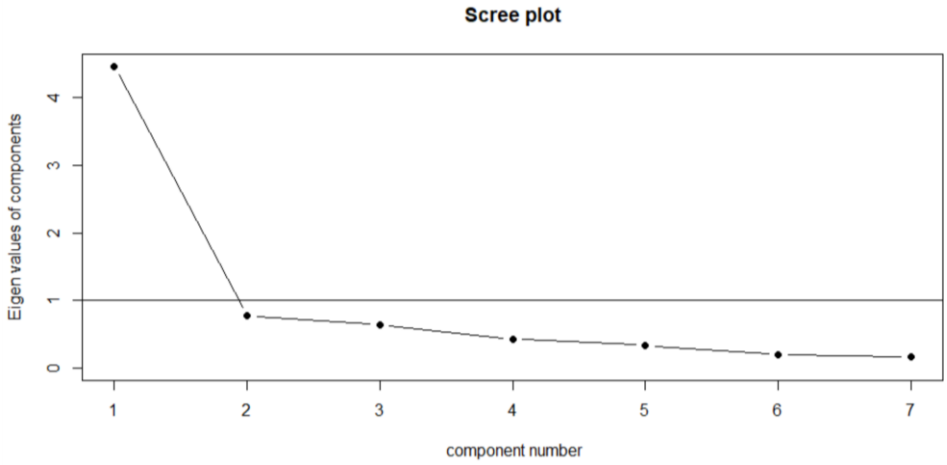


Table B3

Factor Loadings of Perceived Control (Varimax)

Loadings	Factor 1
Item 1	0.836
Item 2	0.815
Item 3	0.751
Item 4	0.628
Item 5	0.808
Item 6	0.727
Item 7	0.745

Item Labels

Item 1: I feel in control of the amount of personal information the smart speaker collects about me.

Item 2: I feel in control of what type of data the smart speaker gathers about me.

Item 3: I feel in control of when the smart speaker is collecting data about me.

Item 4: I feel in control of what happens to my data.

Item 5: I feel in control of who accesses my data.

Item 6: I feel in control of the protection of my data from unauthorised access.

Item 7: I feel in control of how my data is being processed by Amazon.

Table B4

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

Variable	Estimate	*SE*	*p*
DV: Negative Emotions			
intercept	2.96**	1.09	0.009
Privacy	0.34*	0.13	0.015
Security	-0.11	0.20	0.583
R^2	0.11		
DV: Positive Emotions			
intercept	4.45***	1.09	0.000
Privacy	-0.38**	0.13	0.007
Security	0.20	0.12	0.317
R^2	0.13		