Investigating the effects of powerlessness, privacy as a value and surveillance anxiety on privacy risk perception and protective behaviors in the context of smart speakers

Jonah Justin Shepherd

Bachelor Thesis
1st Supervisor: Dr. Nicole Huijts
2nd Supervisor: Dr. Mariëlle Stel

Department of Psychology of Conflict, Risk and Safety
Faculty of Behavioral Management and Social Sciences
University of Twente

Abstract

The use of smart speakers has become increasingly popular in recent years, partially due to their practical benefits. Like any other new technology, the public perception of smart speakers has produced varied opinions, with a very common one referring to the potential risks associated with the use of smart speakers. The aim of the current study is to further investigate different factors influencing privacy risk perception and protective behaviors based on a model created by Hapke. Her predictors were included in the study, while three additional variables were added, namely, powerlessness, privacy as a value and surveillance anxiety. The data collection consisted of an online survey, with a sample including 117 participants. Participants were between the ages of 18 to 65, with most of them being German, both owning and not owning a smart speaker. The results showed a positive correlation between privacy as a value and protective behaviors, and between surveillance anxiety and privacy risk perception and protective behaviors. The regression analysis revealed a significant effect of surveillance anxiety on both privacy risk perception and protective behaviors. The findings of this study suggest that surveillance anxiety can be a valuable addition to the preexisting model by Hapke.

Keywords: privacy, smart speakers, privacy risk perception, protective behaviors, surveillance anxiety

Investigating the effects of powerlessness, privacy as a value and surveillance anxiety on privacy risk perception ad protective behaviors in the context of smart speakers

Since the introduction of the first smart speaker (Echo) by Amazon in 2014, the interest in and adoption of smart speakers and smart devices has continuously increased (Ashfaq et al., 2020). The 2022 US. Smart Home Consumer Adoption Report showed that more than half of all adults living in the United States use smart home devices, with 30% of those being controlled through voice assistants (Kinsella, 2022). As shown in the forecast by Gillett (2020), the European market is also expected to see a noticeable adoption of smart speakers, as by 2024, 57.5 million households are expected to own smart speakers (Gillett, 2020). Furthermore, the United Kingdom Media Report by Ofcom (2021) shows that 50% of all households in the UK claim to own a smart speaker (Brause & Blank, 2023). According to Brause & Blank (2023), the increased prevalence of smart speakers has brought on reports of certain privacy related issues. The growing concern over privacy has evoked researchers to investigate several aspects of smart speaker usage and the associated risks. Risks associated with smart speakers include data breaches, unauthorized access, and user surveillance amongst others. Understanding these perceived risks is crucial for developing effective protective measures and improving overall user trust. In a study conducted by Hapke (2023), several risk perception factors and protective behaviors related to smart speakers were researched and 'combined' into a model to examine the effects and relations between them. This study aims to extend the model and re-examine the effects of the variables in the model on a new dataset.

Literature review

A smart speaker is a voice activated and controlled device which can communicate with its user through using natural language processing and artificial intelligence (Dubois et al., 2020). It uses Natural Language User Interface models to transform human intention into "device control commands" (de Barcelos Silva et al., 2020). After the activation through a "wake word", smart speakers can perform several tasks such as controlling smart homes, sending messages, setting reminders or alarms, playing music, obtaining data, forecasting the weather, or shopping online (Priyanka, 2024; Sahawneh, 2022). Popular smart speakers can be upgraded through Add-ons (Extension) which are described as skills (Alexa) or actions (Google Home) (Bentley et al., 2018).

Skills can be created and released by third party companies and added to the smart speaker. Skills range from games like jeopardy or quizzes, to ordering Domino's pizza or planning a trip with transportation companies like Uber or Lyft (Bentley et al., 2018). Besides the previously mentioned physical advantages that smart speakers present, studies have also shown that smart speakers can have positive psychological effects on their users (Park & Kim, 2022). For example, the longitudinal analysis by Park & Kim (2022) tested the effects of smart speakers' usage in 291 elderly people on depression and loneliness, showing the use of AI based voice recognition devices decreased feelings of depression and loneliness.

Smart speakers are activated through a wake word, but they remain in a constant state of listening mode, enabling users to have a hands-free, easy to use personal assistance device in their households (de Barcelos Silva et al., 2020). This however also raises privacy concerns, as smart speakers use cloud computing to store, analyze and transmit substantial amounts of its user's behavioral patterns and voice data to their remote internet-based cloud servers (Liao et al., 2019). The research paper by Dubois et al., (2020) which focused on mis-activations of the wake word of smart speakers, presents illustrations of this privacy concern. The “Google Home Mini bug” was a malfunction that caused smart speakers to continuously send voice recordings to Googles servers, where they were further used for financial gain by third-party companies. This led to private and intimate conversations being shared with unintended parties (Dubois et al., 2020). In another instance, Brause & Blank (2023) describe a case in which a smart speaker user was notified that a private conversation between her and her husband had accidentally been sent to one of her contacts. Pfeife (2018) showed another instance, where Amazons smart speaker echo dot (Alexa) was served two warrants by the Bentonville police department to gain access to its recordings as it was potential evidence in a murder investigation. Amazon initially declined the request, taking a stance in protecting user privacy data but eventually agreed to provide the required data (Pfeifle, 2018). These examples show the complex nature of privacy risks associated with smart speakers, underlining how certain malfunctions, or mis-activations and legal aspects can compromise user confidentiality in unpredicted and concerning ways.

Research shows different attitudes towards the risks associated with owning smart speakers. Haug et al., (2020) showed in their study focusing on individuals' perception of security and privacy risk towards smart speakers, that users are strongly concerned about security risks associated with the use of smart speakers. Through their daily use of smart speakers, participants

grew increasingly conscious of potential risks, especially concerning how their data might be used by third parties for e-commerce purposes (Haug et al., 2020). This increased awareness often comes from the understanding that their spoken commands and conversations, meant to control the smart speaker, are being recorded and might be analyzed or shared. Moreover, participants voiced concerns about the security risks linked to integrating smart speakers with other smart home devices. Such connections could potentially open their homes to security breaches, as smart speakers can connect to devices like smart locks and video cameras (Haug et al., 2020). In the worst-case scenario, these integrations could allow an unintended individual to gain control over these devices, thereby compromising home security. This interconnectivity, while convenient, also amplifies the vulnerability to unauthorized access, highlighting the complex balance between convenience and security in smart home technology (Haug et al., 2020). Regarding privacy concerns, all participants of the study were concerned even before the use of smart speakers and aware of the possible risks, but still decided to use them. Nonetheless, participants reported an indecisive attitude towards privacy, as they expressed a feeling of digital resignation. They report not being in control of their privacy data regardless and were forced to trust the companies to adhere to adequate data handling (Haug et al., 2020).

In a study by Malkin et al. (2019) about privacy attitudes of Smart Speaker Users a survey was conducted involving 116 participants in which they were presented with questions gauging their beliefs and attitudes about smart speaker privacy. The finding showed that about half of the participants were not aware that their voice recordings are stored forever or were able to review their data. Adding to that, less than 3% knew that they were able to review their voice recordings or delete them (Malkin et al., 2019). Furthermore, participants of the study were asked if they were aware of the mute feature provided for smart speaker users. Less than 10% of participants stated that they used the mute function. Even though the study showed that participants found it “unacceptable” that the default settings enabled companies to store their data forever, the study reported that the majority of participants did not perceive their interactions as meaningful or considered them sensitive (Malkin et al., 2019).

A study conducted by Hapke (2023) explored various variables to understand the antecedents of privacy risk perception and protective behaviors in relation to smart speakers by developing a comprehensive model. This model incorporated six independent variables: perceived enjoyableness, perceived usefulness, trust in smart speakers, nothing-to-hide beliefs, resignation

towards lack of privacy, and privacy self-efficacy, which were analyzed in relation to two dependent variables—privacy risk perception and protective behavior. Although Hapke's research offers significant insights, enhancing and expanding the model could provide deeper understanding into privacy risk perception and the reasons why individuals do or do not engage in protective actions.

To further refine and improve the model, three additional variables have been identified: first, a measurement of powerlessness will be added to gauge its impacts and understanding of how feelings of inability to control privacy affect behaviors. Second, the model will be extended to include surveillance anxiety, examining how the fear of being constantly monitored affects privacy concerns and protective actions. Third, the variable privacy as a value will be incorporated, assessing how much individuals value their privacy and how this valuation influences their protective behaviors. Adding these variables should provide a more comprehensive understanding of the factors that influence protective behaviors and privacy risk perception.

The first added variable, powerlessness, can be defined as an individual's "incapability of protecting oneself from potential risks to their privacy data" (Lutz et al., 2020). In the context of privacy concerns, powerlessness specifically refers to an individual's perceived lack of influence over external forces that could compromise their data privacy/security. Lutz et al., (2020) showed in their study that powerlessness causes individuals to "resist, withdraw, resign" when trying to protect their data from perceived threats. Furthermore, Meng et al., (2021) presented in their study on privacy risk perceptions how participants felt powerless in protecting their data, as they expressed how they feel that they lack control over their data. Additionally, Meng et al., (2021) observed a lack of control and transparency for participants as they felt powerless to use protective measures and felt as if they could not prevent companies or third parties from accessing their data. In Hapke's (2023) study one of the variables, resignation towards a lack of privacy, was revealed to consist of two distinct constructs. One being as intended, resignation towards a lack of privacy and the second one being powerlessness. Due to this, the hypothesis did not include powerlessness as a construct which could be a valuable addition. Due to the insights from previous research and the results from Hapke's (2023) study, the variable of powerlessness has been incorporated into Hapke's model. This addition aims to enhance the model's accuracy and depth, providing a more comprehensive understanding of how feelings of powerlessness affect privacy-related risk

perception and protective behaviors of smart speakers. The second factor which will be added to the existing model and is of interest in the context of privacy risk perception and protective behavior is surveillance anxiety. Surveillance anxiety defined by Kowalczuk (2018) entails the fear of being monitored or observed. As described by Frick et al., 2021, the "surveillance effect" is a global phenomenon in which people fear being listened to by their smart devices, as seen, for example, in tailored advertising in their smartphones or computer devices. Frick et al. (2021) identified that the phenomenon of being monitored or spied on through one's smart devices for the purpose of e-commerce and similar privacy intrusive reasons, has not been adequately named yet, and therefore defined it as "Surveillance effect". For this study's purpose, the term surveillance effect will be addressed as surveillance anxiety, as the definitions overlap. While there is no concrete evidence that companies are using voice recordings to tailor ads to their customers (Frick et al., 2021), 'surveillance anxiety' is a common fear among users. It would be a reasonable assumption that individuals who score higher on surveillance anxiety in general would perceive more privacy risks concerning smart home devices which therefore would lead them to perform more protective behaviors against those privacy risks.

Haug et al., (2020) showed in his study how participants differ on the factor of surveillance anxiety, as some participants acknowledge and accept the possibilities of being constantly under surveillance as their microphone is on while others express their concerns ("I think it might be critical, if the microphone is always active"). Furthermore, participants expressed how this is a risk which keeps them from adopting a smart speaker. Opposing views on surveillance anxiety have been shown in the study of Chalhoub & Flechais (2020). Participants disregarded the perceived risk towards the adoption of smart speakers, since they pointed out how government institutions are nonetheless capable of surveillance, unrelated to smart speakers, as they can use smartphones for example (Chalhoub & Flechais, 2020). Because of the previously mentioned findings and the fact that the surveillance effect is a "global phenomenon" (Frick et al., 2021), surveillance anxiety will also be used as a factor in the extension of Hapkes (2023) model, with the goal of strengthening it and investigating its relationship between privacy risk perception and protective behavior.

Lastly, the third variable which will be added to the existing model is privacy as a value. The study by Huijts and Haans (2024) investigated the effects of values (hedonism, security and

privacy) on positive or negative emotions towards smart home devices, explaining individuals' acceptability towards them. The value of privacy in this context is of particular interest. Privacy encompasses the regulation of interpersonal transactions or institutions, serving to enhance individual autonomy and mitigate vulnerabilities (Lukács, 2016). In the digital context, the term information privacy has been established. Information privacy refers to the ability of individuals or groups to control the collection, use, and dissemination of their personal information (Lukács, 2016). The research by Huijts and Haans, (2024) revealed that information privacy as a value was negatively correlated with positive emotions about smart speakers, indicating that the higher individuals valued their information privacy, the less inclined they were to experience positive emotion towards smart speakers. As Huijts and Haans (2024) point out, information privacy as a value has not been sufficiently researched in today's digital society, especially considering the increasing prevalence of smart speakers. They have developed a new privacy as a value measurement and determined it as a reliable tool. Additionally, information privacy as a value was a factor in understanding both the positive and negative emotions related to a smart device (Huijts and Haans, 2024). In the current study, information privacy as a value will be used to strengthen the model created by Hapke (2023) exploring the relationship it has on perceived risks and protective behaviors in the realm of smart speakers.

Current study

The current study aims to understand the predictors of privacy-related risk perceptions and protective behaviors in the context of smart speakers. This will be achieved through adding three new variables, namely, powerlessness, privacy as a value and surveillance anxiety to Hapke's (2023) model and reexamining it. Understanding these predictors is important as it may offer insights and knowledge into improving protective behaviors, enhancing user security, and creating greater trust in smart speaker technology. The research provided on the three distinct factors indicate the interest in the relationships, therefore the following hypotheses were established:

H1: Powerlessness has a positive effect on (a) privacy risk perception and (b) protective behavior.

H2: Privacy as a value has a positive effect on (a) privacy risk perception and (b) protective behavior.

H3: Surveillance anxiety has a positive effect on (a) privacy risk perception and (b) protective behavior.

Methods

Participants

Participants were recruited using SONA, the University of Twente's system for providing students with empirical research experience. Additional participants were sourced through social media platforms (WhatsApp, Facebook) and the Survey Circle website. The survey was conducted from April 17, 2024, to May 9, 2024, attracting 144 respondents. However, 27 were excluded due to incomplete questionnaires (16), failing attention checks (9), or being under 18 (2), resulting in a final sample of 117 participants for further analysis.

The demographic breakdown of the sample was 37.6% male and 58.1% female, with ages ranging from 18 to 65. The remainder identified as non-binary, non-conforming, or preferred not to disclose their gender. 70 participants were students. Most participants were German (80.3%), with 5.1% from the Netherlands and 14.5% identifying as 'other'. Regarding smart speaker ownership, 35.0% owned one, while the remaining 65.0% were asked to imagine being gifted one for the purpose of the study. Educational backgrounds varied: 33.3% had completed high school, 24.8% had a professional education, 24.5% held a bachelor's degree, 13.7% had a master's degree, and 1.7% had a PhD. The study received ethical approval from the BMS ethical committee / Domain Humanities & Social Sciences.

Materials

Variables from Hapke's study. The variables of Hapke (2023) were included in the questionnaire, however they were adapted to fit the new focus of people who already owned a smart speaker. Additionally, only the items for which Hapke developed a hypothesis were analyzed. The following section will list all these variables and include one item example to reflect the formulation. The mean, standard deviation, and Cronbach's alpha of these variables can be found in Table 1. All variables were measured on a 5-point Likert scale. Perceived enjoyableness was measured using items such as "I think I would have fun using a smart speaker that I received

as a gift." Perceived usefulness was measured using items such as "Using a smart speaker that I received as a gift would make my life easier.". Trust in smart speaker companies was measured using items such as "Smart speaker companies care about protecting my data to maintain their positive brand image.". Nothing to hide beliefs was measured using items such as "I have nothing to hide, so no one would find anything interesting about me in my data.". Resignation towards lack of privacy was measured using items such as" In order to adopt new technologies, I have to give up my privacy.". Privacy self-efficacy was measured using items such as "I feel in control over the information I provide on my smart speaker".

Table 1

Descriptive statistics and internal consistency measurement for Hapkes (2023) variables

Variable	*M*	*SD*	Cronbach's alpha
Perceived enjoyableness	3.15	0.41	0.75
Perceived usefulness	2.28	0.95	0.90
Trust in smart speaker companies	2.27	0.76	0.86
Nothing to hide beliefs	2.88	0.81	0.69
Resignation towards lack of privacy	3.14	0.66	0.54
Privacy self-efficacy	2.34	0.77	0.85

Powerlessness. Powerlessness was measured with five items which were taken from a study by Lutz et al., (2020). Lutz items for powerlessness were prioritized over Hapke's items, because Hapke (2023) only found through the factor analysis that her intended construct of "resignation towards privacy" encompassed two distinct constructs, the second being powerlessness. Consequently, her measurement of powerlessness consisted of only three items. The items developed by Lutz et al. (2020) were considered more suitable as they were precise and comprehensive, effectively capturing individual's perceptions of powerlessness. The items measure the feeling of powerlessness participants experience in relation to the control they have, to protect their personal data. This has been assessed using a 5-point Likert scale ranging from 1 "strongly disagree up to 5 "strongly agree". An example of an item is "I don't have the power to protect my personal data effectively from all the possible dangers on the Internet" and "In the end, I can't prevent others from accessing my data." All 5 items used to measure powerlessness load on one factor (powerlessness). The factor analysis can be found in Appendix B. The items were averaged to form the scale (M=3.61 SD=0.85 α =0.84)

Privacy as a value. The items for privacy as a value were taken from the study by Huijts and Haans (2024), as the study demonstrated how privacy as a value can be added to Schwartz values scale. The scale measured all 19 values, with one item for each value, besides information privacy which was measured with 3 items. While Schwartz`s scale had three items for each value, this study shortened the number of items to one per value to limit the length of the questionnaire. A 6-point Likert scale has been used here to assess the answers ranging from 1 “strongly disagree" to 6 “strongly agree”. Examples of items here are “It is important to him to have full control over who accesses personal information about him” or “It is important to him to protect his privacy". All items used to measure the participants' values load on factor (privacy as a value). The factor analysis can be found in Appendix B. The items were averaged to form the scale (M=4.46 SD=0.93 α =0.75)

Surveillance Anxiety. The first 4 items measuring Surveillance Anxiety were taken from the study by Kowalczuk (2018) and the last two items from the study by Frick (2021). All items were measured on a 5-point Likert scale with answer possibilities ranging from 1 “strongly disagree” to 5 “strongly agree”. Examples of the items are “The idea that I would be under surveillance by a smart speaker frightens me” and “I am concerned that my smart device is capturing information even though I am not actively using it. All 6 items used to measure Surveillance Anxiety load on one factor (surveillance anxiety). The factor analysis can be found in Appendix B. The items were averaged to form the scale (M=3.59 SD=0.87 α =0.86)

Privacy risk perception. The 3 items measuring privacy risk perception were taken from the study by Hapke (2023). All 3 items were measured on a 5-point Likert scale with answers ranging from 1 “None at all” to 5” A great deal". An example of the items is “How large do you think the risk is that your privacy is invaded by your smart speaker?” All items used to measure the participants' privacy risk perception load on one factor (privacy risk perception). The factor analysis can be found in Appendix B. The items were averaged to form the scale (M=3.23 SD=0.97 α=0.80)

Protective behaviors. To measure protective behavior, 19 items were used on a 5-point Likert scale with combined questions from Hapke (2023). Examples of the items are “I delete my smart speaker recordings” or “I muted the smart speakers microphone when I am not using it”. The items used from Hapke were modified to better fit this study's research goals. Furthermore, items from Lutz (2019) were added to extend the items measuring protective behavior. Overlapping items between Hapke and Lutz (2019) were excluded to ensure a more precise measurement of the construct and several items from Lutz (2019) were excluded as they did not fit the measurement. All items used to measure the participants' protective behaviors can be found in Appendix B. The items were averaged to form the scale ($M=2.56$ $SD=1.10$ $\alpha=0.93$). The factor analysis revealed that the items measured 4 different components of protective behaviors. The first component can be described as “passive protective behavior” with items such as “I will speak very quietly around the smart speaker, in case I don't want to be recorded.”. This component seems to measure passive strategies used by individuals to change their behavior around the smart speaker, rather than interacting with it.

The second component can be described as “physical protective behavior” with items such as “I will turn off the smart speaker when I am not using it.”. This component measures proactive strategies, involving direct contact with the smart speaker device. The third component can be described as “privacy settings protective behavior” with items such as “I will review the privacy settings of my smart speaker in the providers account.”. This component measures strategies involving reviewing and changing the privacy settings of the smart speaker device. The fourth component can be described as “security protective behavior” with the item “I will not write down the password on a piece of paper or share it otherwise with house members or visitor.". This component measures secure access strategies with a focus on managing the access towards the smart speaker device, for example through safe passwords. However, the last component had only one item in it. All factor loadings can be found in Appendix B.

Due to the small sample size, all the items were included and analyzed as one component to ensure a more stable and comprehensive model. Since each sub-dimension still reflects aspects of the broader concept of protective behaviour with smart speakers, combining them into a single construct allowed for a comprehensive analysis of how participants perform protective behaviours.

Procedure

The design of this research project consisted of an online survey, created through Qualtrics (Appendix A). The survey started by guiding the participants through informed consent. After agreeing, 5 demographic questions were asked about the participants' age, country of origin, gender, education level and if they currently are a student. Next, the participants were asked if they own a smart speaker in their household or their parent's' household. If the answer was no, the participants were asked to imagine a scenario in which one was gifted to them. Further, the survey consisted of questions used in Hapke's (2023) research, and additional questions which aimed to measure the variables of the current study. The questionnaire included additional questions aimed at other objectives not reported in this study. The study finished with a request for participants to refer eligible friends or acquaintances to the survey without discussing its content, to maintain the integrity of the results. Lastly, the contact information of the researchers was displayed for any further questions.

Data Analysis

The data was analyzed using the statistical program IBM SPSS 29.0. To measure the demographics, frequencies and descriptive statistics were performed. Reliability analyses were used to analyze the measurement scales. Factor analyses have been performed to verify the validity of the five constructs measured by the questionnaire's items. Pearson's correlation analysis was performed to analyze the six hypotheses. Additionally, a multiple linear regression analysis was used to reevaluate the model by Hapke (2023), including the new variables. The analysis did not differentiate between participants who owned a smart speaker to those who were given the scenario of being gifted one because of the small number of participants.

Results

Hypothesis testing

Pearson's correlation and statistical significance of the three variables investigated in this study and the controlling variables are in Table 2.

Table 2.

Pearson's correlation and statistical significance for Privacy risk perception and Protective behaviors with the independent variables and controlling variables (n=117)

	Privacy risk perception	Protective behaviors

	r	*p*	*r*	*p*
Powerlessness	.13	.169	-.05	.565
Privacy as a value	.13	.179	**.26**	**.005**
Surveillance Anxiety	**.46**	**<.001**	**.48**	**<.001**
Perceived enjoyableness	.11	.368	.07	.532
Perceived usefulness	-.14	.216	.15	.212
Trust in companies	**-.42**	**<.001**	-.13	.175
Nothing to hide beliefs	**-.27**	**.005**	**-.30**	**.001**
Resignation towards privacy	-.10	.278	**-.26**	**.002**
Privacy self-efficacy	**-.19**	**.043**	.11	.234
Privacy risk perception			**.38**	**<.001**

Note. The significant correlations are marked in bold. ($p < .05$)

In contrast with Hypothesis 1a and 1b, the results show that powerlessness does not have a significant positive relationship with privacy risk perception or protective behaviors. This indicates that feelings of powerlessness do not significantly influence an individual's privacy risk perception towards smart speakers or their engagement in protective behaviors.

For Hypothesis 2a and 2b, the results show that privacy as a value does have a statistically significant positive relationship with protective behaviors but not with privacy risk perception. This indicates that value placed on privacy does not significantly influence an individual's privacy risk perception however it does influence their protective behaviors towards smart speakers.

In line with hypothesis 3a and 3b, the results show that surveillance anxiety has a significant positive relationship with privacy risk perception and with protective behavior regarding smart speakers. This suggests that individuals who experience higher surveillance anxiety tend to perceive greater privacy risks and engage in more protective behaviors regarding smart speakers. Regarding the controlling variables, trust in companies, nothing to hide beliefs and privacy self-efficacy were found to have a negative and significant correlation with privacy risk perception. Resignation towards privacy and nothing to hide beliefs were found to have a negative and significant correlation with protective behaviors.

Regression analysis

A regression analysis was done for privacy risk perception and protective behaviors including the whole sample, meaning that individuals who own and those who do not own a smart speaker were included. The analysis included the independent variables introduced in this study,

namely powerlessness, privacy as a value and surveillance anxiety, and the control variables from Hapke's (2023) study. The regression analysis was performed for privacy risk perception and protective behaviors separately, as two dependent variables. Security self-efficacy was not included in the regression analysis as there was no hypothesis for this variable in Hapkes (2023) research.

Table 3.

Regression analysis with Privacy Risk Perception as the Dependent variable (n=117)

Variable	*B*	*SE*	β	*t*	*p*
Powerlessness	.00	.02	.00	.03	.97
Surveillance Anxiety	**.07**	.02	.38	3.6	**<.001**
Privacy as a value	-.1	.10	-.1	-1.0	.31
Perceived enjoyableness	0.25	.17	.13	1.5	.15
Perceived usefulness	-.04	.1	-.05	-.4	.68
Trust in companies	**-.05**	.02	-.27	-2.5	**.01**
Nothing to hide belief	-.04	.02	-.15	-1.5	.13
Resignation towards privacy	.02	.04	.06	.55	.59
Privacy self-efficacy	.00	.03	-.27	-2.5	.87

Note. The statistically significant effects are marked in bold. ($p < .05$)

In line with hypothesis 3a, the results of the regression analysis show that surveillance anxiety has a moderate positive relationship with privacy risk perception (Table 3). Hypothesis 1a, 1b, 2a, 2b and 3b were not supported when other variables were controlled for in the analysis. Trust in

companies was found to have a weak negative relationship with privacy risk perception. The remaining variables did not have a statistically significant relationship with the dependent variable.

Table 4. *Regression analysis with Protective Behaviors as the Dependent variable (n=117)*

Variable	*B*	*SE*	β	*t*	*p*
Powerlessness	.01	.28	.04	.41	.682
Surveillance Anxiety	**.08**	.02	.40	3.7	**<.001**
Privacy as a value	.03	.12	.02	.23	.821
Perceived enjoyableness	.22	.19	.09	1.1	.266
Perceived usefulness	-.19	.11	-.16	-1.6	.101
Trust in companies	.02	.02	.11	1.0	.317
Nothing to hide belief	-.05	.03	-.17	-1.7	.085
Resignation towards privacy	-.07	.04	-.16	-1.6	.113
Privacy self-efficacy	.04	.03	.15	1.5	.130

Note. The statistically significant effects are marked in bold. ($p < .05$)

The results of the regression analysis show that in line with hypothesis 3b, surveillance anxiety has a moderate positive relationship with protective behaviors towards smart speakers (Table 4). The remaining variables did not have a statistically significant relationship with the dependent variable, protective behaviors. Hypothesis 1a, 1b, 2a, 2b and 3a were thus not supported when other variables were controlled for in the analysis.

Discussion

The aim of this research was to investigate the factors influencing privacy risk perception and protective behaviors regarding smart speakers by extending Hapke's (2023) model with three new variables: powerlessness, surveillance anxiety, and privacy as a value. The most valuable finding in terms of a potential addition to the model, is the effect that was found between surveillance anxiety and privacy risk perception and protective behaviors. There was a positive correlation between this factor and both dependent variables, and a significant effect was found in the regression analysis. Privacy as a value was found to have a weak positive correlation with proactive behaviors, and no significant results were found for powerlessness. In the following section, each hypothesis will be discussed and interpreted in more detail.

Hypothesis 1a and 1b investigated a potential positive relationship between powerlessness, privacy risk perception and protective behaviors, respectively. The analyses did not yield any significant results for this variable; therefore, this hypothesis was not supported. This indicates that feeling incapable of protecting one's data does not necessarily translate into heightened privacy concerns or increased protective actions. This could suggest that individuals might resign to a perceived lack of control without necessarily changing their behavior in response. The non-significant findings for powerlessness oppose the findings from Lutz et al. (2020) and Meng et al. (2021), who identified powerlessness as an important factor in privacy risk perception. A potential reason for these contradicting findings could be the notable difference in the sample size of the current study, compared to Lutz et al. (2020). Furthermore, in the study conducted by Hapke (2023), there was a significant effect found between powerlessness and privacy risk perception for participants who did not own a smart speaker. Due to the small sample size of the current study, no distinctions were made between participants who owned a smart speaker and those who did not. Therefore, an attempt should be made to redo the study on a larger group and further investigate the effects of powerlessness, while particularly focusing on non-owners of smart speakers.

Hypothesis 2a and 2b investigated the potential positive relationship between privacy as a value, privacy risk perception and protective behaviors, respectively. In line with hypothesis 2b, privacy as a value was found to have a weak, marginally significant, positive correlation with protective behaviors. In contrast with hypothesis 2a, privacy as a value did not have a significant correlation with privacy risk perception. When controlling for the effect of other predictors in the regression analysis, no significant effect was found for privacy as a value. The overall findings imply that while valuing privacy does lead individuals to take more actions to protect their data, it does not necessarily heighten their perception of risk. A reason for this could be due to the fact that individuals who value their privacy more are more prone to perform protective measures which decreases their perception of risk. The significant relationship between privacy as a value and protective behaviors supports the work by Huijts and Haans (2024), who demonstrated the importance of privacy as a value in understanding user behavior. In terms of extending Hapkes (2023) model, with a lack of significant effect found in the regression analysis, privacy as a value does not seem to be a valuable addition to the model.

Hypothesis 3a and 3b investigated the potential positive relationship between surveillance anxiety, privacy risk perception and protective behaviors, respectively. In line with the hypothesis, surveillance anxiety was found to have a positive correlation with both dependent variables. Moreover, surveillance anxiety was the only new variable which had a significant effect when controlling for the other variables in the study. These findings imply that individuals who experience higher levels of anxiety about being monitored by their smart speakers perceive greater privacy risks and are more likely to engage in protective behaviors. These findings align with previous research by Kowalczuk (2018) and Frick et al. (2021) on surveillance anxiety, which found that concerns about being monitored are common amongst individuals and significantly influence privacy-related behaviors. It is unclear which protective behaviors the participants were most likely to engage in, as no distinctions were made in this study. However, future research might consider investigating this aspect further. Considering the positive effects found for surveillance anxiety in relation to privacy risk perception and protective behaviors, this variable has the potential for being a valuable addition to the model by Hapke (2023).

The current study included the variables investigated by Hapke (2023) and new ones, to further explore their effects on privacy risk perception and protective behaviors in the context of smart speakers. When comparing the correlations of Hapkes (2023) original variables in her study and the correlations of her variables conducted in this study, some discrepancies were found. Here, less significantly correlated relationships were found, and the ones who proved to be statistically significant had weaker correlations. For the significant correlations, the direction of these relationships were in line with Hapkes (2023) findings. When considering her variables in the regression analysis, the only one found to have a significant effect was trust in companies, with privacy risk perception as the dependent variable. Similar results were found in her study, which has a positive and a negative consequence. The results of both Hapkes (2023) and the current study are in line, which suggests that the anticipated relationship is further supported. When considering the new variables, the only one with a significant effect was surveillance anxiety, with both privacy risk perception and protective behaviors as dependent variables. This finding can be regarded as beneficial to Hapkes (2023) study in two ways. Firstly, the variable of surveillance anxiety could be considered as an addition to Hapkes (2023) model, with the potential of strengthening it. Secondly, the role of surveillance anxiety and its relation to privacy risk perception and protective behaviors can be used for information in creating an intervention aimed

to increase protective action. Surveillance anxiety is centered around the fear of being monitored and listened to, which is a common fear when considering the use of smart speakers. A potential intervention in this case could involve the creation of easy-to-follow guides and tutorials for users, about how exactly they are being monitored, and what is done with the gathered information. The tutorials could be educational as well as practical, by providing individuals with information and diverse ways to tackle their fear.

Limitations

There were a few limitations in this study which might have hindered the results. Firstly, the sample size was small and inadequate when considering the type of research at hand. Due to the sample size, the researcher was unable to differentiate between smart speaker owners and non-owners in the analysis. Due to this, the extent and precision of the findings were limited. Additionally, the sample size may limit the generalizability of the findings to broader populations. Furthermore, the sample did not have an adequate population representation, as most of the participants were students, German and female. Moreover, the current research shared the data collection process with two other students investigating Hapkes (2023) model. Due to that, the questionnaire included items from the search by Hapke (2023), the current study and the other two students' study. In order not to overwhelm the participants, and ensure a certain level of engagement and focus, fewer items could have potentially simplified the questionnaire. Lastly, the survey is cross sectional, and does not allow to draw conclusions on cause and effect.

Future research

Future research should consider the possibility of conducting longitudinal studies to better understand the causal relationships between the discussed variables. Additionally, investigating other potential factors, such as cultural differences or technological knowledge, could provide a broader understanding of perceived risk perception and protective behavior towards smart speakers. Understanding these factors can help in designing more secure and user-friendly devices, create suitable policies and laws, and enlighten users, companies and institutions about the psychological mechanism influencing perceived risk perception and protective behaviors. Furthermore, certain limitations mentioned in this study should be implemented in future research, such as gathering a more sizeable and representative sample. This change will promote generalizability of the findings and allow the analysis to differentiate between owners and non-

owners of smart speakers. Aforementioned, a significant effect was found between powerlessness and privacy risk perception in the study conducted by Hapke (2023), for participants who did not own a smart speaker. Here, no significant effects were found for powerlessness, and future research could include this relationship again, in a more sizeable sample.

Conclusion

In conclusion, this study aimed to investigate the role of powerlessness, privacy as a value and surveillance anxiety in relation to privacy risk perception and protective behaviors. This analysis was meant to extend Hapke's (2023) model by incorporating the new variables and reexamine the original variables from the model. The findings revealed a significant role of surveillance anxiety in the context of the model, and no significant effects were found for powerlessness and privacy as a value. While powerlessness and privacy as a value did not show a significant impact on the dependent variables, the overall results contribute to a further understanding of the complex dynamics influencing smart speaker users' privacy management. It became apparent that including the distinction between users and non-users of smart speakers in the analysis is something to consider for future research. The current study's findings provide a limited addition to the study by Hapke (2023) but should be considered for any future examinations of the model. The practical implications of this study provide an insight into different factors that influence risk perception and the performing of protective behaviors in the context of smart speakers. These insights can inform about ways in which user perception of privacy and safety actions can be enhanced in the digital age.

References

Ashfaq, M., Yun, J., & Yu, S. (2020). My smart speaker is cool! Perceived coolness, perceived values, and users' attitude toward smart speakers. *International Journal of Human–Computer Interaction*, 37(6), 560–573. https://doi.org/10.1080/10447318.2020.1841404

Bentley, F., Luvogt, C., Silverman, M., Wirasinghe, R., White, B., & Lottridge, D. (2018). Understanding the long-term use of smart speaker assistants. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(3), 1–24. https://doi.org/10.1145/3264901

Brause, S. R., & Blank, G. (2023). 'There are some things that I would never ask Alexa' – privacy work, contextual integrity, and smart speaker assistants. Information, Communication & Society, 27(1), 182–197. https://doi.org/10.1080/1369118x.2023.2193241

de Barcelos Silva, A., Gomes, M. M., da Costa, C. A., da Rosa Righi, R., Barbosa, J. L., Pessin, G., De Doncker, G., & Federizzi, G. (2020). Intelligent personal assistants: A systematic

literature review. Expert Systems with Applications, 147, 113193. https://doi.org/10.1016/j.eswa.2020.113193

Dubois, D. J., Kolcun, R., Mandalari, A. M., Paracha, M. T., Choffnes, D., & Haddadi, H. (2020). When speakers are all ears: Characterizing misactivations of IoT smart speakers. Proceedings on Privacy Enhancing Technologies, 2020(4), 255–276. https://doi.org/10.2478/popets-2020-0072

Edwards, K. J., Jones, R. B., Shenton, D., Page, T., Maramba, I., Warren, A., Fraser, F., Križaj, T., Coombe, T., Cowls, H., & Chatterjee, A. (2021). The use of smart speakers in care home residents: Implementation study. *Journal of Medical Internet Research*, 23(12). https://doi.org/10.2196/26767

Gillett, F. (2020). By 2024, 57.5 million EU-5 households will have smart speakers. Forrester. https://www.forrester.com/report/By-2024-575-Million-EU5-Households-Will-Have-Smart-Speakers/RES158859

Haug, M., Rössler, P., & Gewald, H. (2020). How users perceive privacy and Security Risks Concerning Smart speakers. AIS Electronic Library (AISeL). https://aisel.aisnet.org/ecis2020_rp/129/

Kinsella, B. (2022, June 20). Over half of U.S. adults have smart home devices, nearly 30% use voice assistants with them - new report. Voicebot.ai. https://voicebot.ai/2022/06/20/over-half-of-u-s-adults-have-smart-home-devices-nearly-30-use-voice-assistants-with-them-new-report/

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. Journal of Research in Interactive Marketing, 12(4), 418-431.

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the role of privacy and trust in Intelligent Personal assistant adoption. Information in Contemporary Society, 102–113. https://doi.org/10.1007/978-3-030-15742-5_9

Lukács, A. (2016). What is privacy? The history and definition of. https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy attitudes of smart speaker users. Proceedings on Privacy Enhancing Technologies, 2019(4), 250–271. https://doi.org/10.2478/popets-2019-0068

Meng, N., Keküllüoğlu, D., & Vaniea, K. (2021). Owning and sharing. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW1), 1–29. https://doi.org/10.1145/3449119

Park, S., & Kim, B. (2022). The impact of everyday AI-based smart speaker use on the well-being of older adults living alone. Technology in Society, 71, 102133. https://doi.org/10.1016/j.techsoc.2022.102133

Pfeifle, A. (2018). Alexa, what should we do about privacy? Protecting privacy for users of voice-activated devices. UW Law Digital Commons. https://digitalcommons.law.uw.edu/wlr/vol93/iss1/9/

Priyanka, A. L. (2024). Smart speakers. Advances in Media, Entertainment, and the Arts, 415–440. https://doi.org/10.4018/979-8-3693-0639-0.ch018

Sahawneh, F. (2022). Smart Speakers: Can They Be Trusted? *TECHNOLOGY INTERFACE INTERNATIONAL JOURNAL, 34.*

Appendix A

Questionnaire

Informed Consent

Project Title

Which factors influence people's privacy risk perceptions of smart speakers?

Researchers

Jonah Shepherd (B.Sc. student) and Dr. Nicole Huijts, Department of Psychology of Conflict, Risk, and Safety, University of Twente, Netherlands.

Purpose

This study aims to advance our understanding of privacy perceptions about smart speakers.

You are being asked to participate in this study because you found this survey online or were asked

to participate by one of the researchers or data collectors and because we are interested in these processes in a wide variety of people. We are seeking individuals who are at least 18 years old. If you are under 18, please do not participate.

Procedure

If you agree to participate, you will be asked to answer questions concerning your privacy perceptions regarding smart speakers. Afterwards, several demographics (age, gender, nationality, and education) will be measured. Finally, you will be provided with more details about this study.

Your participation will take approximately 20 minutes.

Participant Rights

Your participation in this study is completely voluntary. You are free to decline to participate, refuse to answer any individual questions, or withdraw from the study at any time without the need to give any reason.

Risks and Benefits

There are no known or anticipated risks associated with this study.

Confidentiality

Your responses are completely anonymous and cannot be traced back to you because no personally identifying information such as names is asked in this survey. The information you provide will not be disclosed to third parties, and it will be aggregated with the responses of other participants and examined for hypothesized patterns. Your anonymous responses will be used for scientific research into various aspects of personality and social psychology. Data from this study may be stored in an online repository and shared publicly to adhere to best practices in scientific transparency.

Anonymity and Confidentiality

Your responses will be strictly anonymous; we will not be collecting or retaining any information about your identity. The information you provide will not be disclosed to third parties, and it will

be aggregated with the responses of other participants and examined for hypothesized patterns. Data from this study will be stored in an online repository and shared publicly to adhere to best practices in scientific transparency.

Questions

If you would like to talk with someone other than the researchers to discuss any problems or concerns, to discuss situations in the event that a member of the research team is not available, or to discuss your rights as a research participant, please contact the Ethical Review Committee of the Behavioral and Management Sciences Faculty, University of Twente, Netherlands, ethicscommittee-bms@utwente.nl.

Consent and Authorization Provisions

In order to continue with this survey, you have to agree with the aforementioned information and consent to participate in the study. Clicking "I agree and consent to participating in this study and confirm that I am over 18 years old" indicates that you have been informed about the nature and method of this research in a manner that is clear to you, you have been given the time to read the page, and that you voluntarily agree to participate in this study.

Demographic questions

- What is your age?
- Which country are you from? (Germany; The Netherlands; Other, please indicate)
- What is your gender? (male/female/nonbinary/prefer not to say)
- What is your highest completed level of education? (Primary school, Highschool, Professional education, Bachelor, Master, PhD)
- Are you a student? (Yes, no)

Values male

Here we briefly describe some people. Please read each description and think about how much each person is or is not like you. Mark the box that shows how much the person in the description is like you.

5-point Likert scale (1= strongly disagree, 5 = strongly agree) for the following questions measuring values

1. He wants the state to be strong so it can defend its citizens
2. Following his family's customs or the customs of a religion
3. It is important to him to follow rules even when no one is watching.
4. He thinks it is important never to be annoying to anyone.
5. It is important to him to be humble.
6. He goes out of his way to be a dependable and trustworthy friend.
7. Caring for the well-being of people he is close to is important to him.
8. He thinks it is important that every person in the world have equal opportunities in life.
9. It is important to him to work against threats to the world of nature
10. It is important to him to listen to people who are different from him.
11. It is important to him to have full control over who accesses personal information about him.
12. It is important to him to not share personal information (for example about personal preferences, one's health, or political and religious beliefs) with unknown others.
13. It is important to him to protect his privacy.

Values female

Here we briefly describe some people. Please read each description and think about how much each person is or is not like you. Mark the box that shows how much the person in the description is like you.

5-point Likert scale (1= strongly disagree, 5 = strongly agree) for the following questions measuring values

1. She wants the state to be strong so it can defend its citizens.
2. Following her family's customs or the customs of a religion is important to her.
3. It is important to her to follow rules even when no one is watching.
4. She thinks it is important never to be annoying to anyone.
5. It is important to her to be humble.
6. She goes out of her way to be a dependable and trustworthy friend.

7. Caring for the well-being of people she is close to is important to her.
8. She thinks it is important that every person in the world have equal opportunities in life.
9. It is important to her to work against threats to the world of nature.
10. It is important to her to listen to people who are different from her.
11. It is important to her to have full control over who accesses personal information about her.
12. It is important to her to have full control over who accesses personal information about her.
13. It is important to her to protect her privacy.

Description of a smart speaker

A smart speaker is a voice-controlled internet-enabled device that streams audio, provides information, and interacts with other smart devices. Examples include Amazon's Alexa and Google's Homepod.

Control question:
Is there a smart speaker in your household? (Please also answer 'Yes' if you are a student and there is one in your parent's house)?
If yes:
Which statement best describes your situation regarding the smart speaker?

- *I am the main owner*
- *I use it, but I am not the owner*

Did you install the smart speaker yourself?

- *Yes*
- *No*

For how long have you been using the smart speaker?

- *less than 1 month*
- *2-3 months*
- *4 months to 1 year*
- *1-2 years*
- *Morer than two years*

For the remainder of the survey, please think about the smart speaker you were relating to just now, while answering the questions.

If no:
For the rest of the survey please imagine you received a smart speaker as a birthday gift and you installed it in your home.

Think about this new smart speaker when answering the following questions.

Keeping in mind that you have been gifted a smart speaker, what would you do?

I will install the smart speaker that has been gifted to me

- Yes
- No

I will use the smart speaker that has been gifted to me

- Yes
- No

Protective behavior (gifted scenario)
For the following questions imagine that you do install and use the device. Please indicate how likely you are to engage in the following behaviours regarding your gifted smart speaker.

5-point Likert scale (1= Extremely unlikely, 5 = Extremely likely)

1. I will turn off the smart speaker when I am not using it
2. I will unplug the smart speaker when I am not using it

3. I will unplug the smart speaker when I am having serious/private conversations
4. I will turn off the smart speaker when I am having serious/private conversations
5. I will mute the smart speakers microphone when I am not using it
6. I will review the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account
7. I will review which applications/services have access to my smart speaker
8. I will restrict the amount of data that the device is allowed to collect through the smart speakers settings
9. I will delete my smart speaker recordings
10. In the app I will delete sensitive information that the smart speaker stored about me.
11. I will speak very quietly around the smart speaker, in case I don't want to be recorded

12. I will moderate my language around the smart speaker so that it doesn't record private matters, even if accidentally
13. I will avoid sensitive/private conversations around the smart speaker
14. If I have a visitor, I will inform them that I have a smart speaker
15. I will consider where to place the smart speaker so that it is not positioned in areas where I typically engage in conversations involving sensitive or private information
16. I will set a new difficult password for my smart speaker that I don't use for other applications
17. I will not write down the password on a piece of paper or share it otherwise with house members or visitors

Protective behavior (owning)

5-point Likert scale (1= Extremely unlikely, 5 = Extremely likely

1. I turned off the smart speaker when I was not using it
2. I unplugged the smart speaker when I was not using it
3. I unplugged the smart speaker when I was having serious/private conversations
4. I turned off the smart speaker when I was having serious/private conversations
5. I muted the smart speakers microphone when I was not using it
6. I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account
7. I reviewed which applications/services have access to my smart speaker
8. I restricted the amount of data that the device is allowed to collect through the smart speakers settings
9. I deleted my smart speaker recordings
10. In the app I deleted sensitive information that the smart speaker stored about me.
11. I spoke very quietly around the smart speaker, in case I did not want to be recorded
12. I moderated my language around the smart speaker so that it didn't record private matters, even if accidentally
13. I avoided sensitive/private conversations around the smart speaker
14. When I had a visitor, I informed them that I have a smart speaker
15. When I had a visitor, I offered to switch the smart speaker off
16. ... I placed the smart speaker so that it was not positioned in areas where I typically engaged in conversations involving sensitive or private information
17. ... I set a new difficult password for my smart speaker that I don't use for other applications
18. ... I did not write down the smart speakers password on a piece of paper or shared it otherwise with house members or visitors
19. ... I changed the password again after using the smart speaker for some time

Perceived enjoyableness (5-point Likert scale 1= Strongly disagree 5 = Strongly agree)

1. I think using a smart speaker that I received as a gift would be enjoyable.
2. I think I would have fun using a smart speaker that I received as a gift.
3. It would not be interesting to use a smart speaker that I received as a gift.

4. Using a smart speaker that I received as a gift would not give me pleasure.

Perceived usefulness (5-point Likert scale 1= Strongly disagree 5 = Strongly agree)

1. Using a smart speaker that I received as a gift would improve my productivity in my daily life
2. Using a smart speaker that I received as a gift would make my life easier
3. Using a smart speaker that I received as a gift would enable me to accomplish my tasks more quickly.
4. Using a smart speaker that I received as a gift would enhance my effectiveness in daily tasks.
5. I would find it useful to use a smart speaker that I received as a gift at home.

Privacy risk perception gifted (5-point Likert scale 1= none at all, 5 = a great deal)

1. To what extent do you think your privacy is at risk now that you installed a smart speaker in your house?
2. How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?
3. How large do you think the risk is that your privacy is invaded now that you have this smart speaker installed?

Privacy risk perception owning

1. To what extent do you think your privacy is at risk with a smart speaker in your house?
2. How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?
3. How large do you think the risk is that your privacy is invaded by your smart speaker?

Trust in companies (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. Smart speaker companies are trustworthy in handling the data the smart speaker collects about me.
2. I trust that smart speaker companies keep my best interests in mind when dealing with the information collected about me.
3. Smart speaker companies are in general predictable and consistent regarding the usage of the information provided by me.
4. Smart speaker companies are careful with sharing my personal data with third parties.
5. Smart speaker companies are always honest with customers when it comes to using information that they provide.
6. Smart speaker companies intend to protect my data well because they want to keep their market shares.

7. Smart speaker companies care about protecting my data to maintain their positive brand image.

Nothing to hide (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. I have nothing to hide, so no one would find anything interesting about me in my data.
2. I do not admit to anything that would incriminate me in front of my smart speaker.
3. I have nothing to hide because I do not do anything criminal in my house.
4. I am not doing much in my house that I do not want other people to know about.
5. My life is very boring, so the data collected about me is of little interest to others.

Resignation towards lack of privacy (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. Companies like Amazon and Google already have so much data about me, that the data a smart speaker collects is just a small amount of added information stored online.
2. In order to adopt new technologies, I have to give up my privacy.
3. Protecting my privacy is so inconvenient that I do not care anymore who has my data.
4. Consumers have lost all control over how personal information is collected and used by companies.
5. It does not matter what I do regarding the settings of the smart speaker, companies collect loads of information about me anyway.
6. I am powerless when it comes to protecting my data from the manufacturer of the smart device.

Powerlessness (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. I believe that even if I try to protect my data, I can't prevent others from accessing them.
2. I believe that in the end, I can't prevent others from accessing my data.
3. I believe that I don't have the power to protect my personal data effectively from all the possible dangers on the Internet.
4. I believe that it would be naive to think that I can protect my personal data online reliably.
5. I believe that if someone is determined to access my personal data, there is nothing I can do to stop them.

Surveillance Anxiety (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. The idea that I would be under surveillance by a smart speaker frightens me.
2. I find it objectionable when I do not know what will be recorded by smart speakers.
3. It bothers me that others see my activities via the smart speaker.
4. It disturbs me that the smart speaker permanently monitors me.
5. I worry that my smart device is recording conversations when I talk to my friends.
6. I am concerned that my smart device is capturing information even though I am not actively using it.

Self-Efficacy (5-point Likert scale 1= Strongly disagree, 5 = strongly agree)

1. I feel confident in my ability to protect myself by using the privacy settings of my smart speaker.
2. I feel in control over the information I provide on my smart speaker.
3. Privacy settings allow me to have full control over the information I provide to my smart speaker.
4. I feel in control of who can view my information collected through my smart speaker.
5. I am able to protect my personal information from external threats.
6. I am able to protect the data on my smart speaker from being damaged or altered by external parties.
7. I am capable of responding well to malicious software such as viruses.
8. I am able to detect that my smart speaker is hacked.
9. I am able to erase malicious software from my smart speaker.

Thank you very much for participating in our study!

Information about the Study

From qualitative research, we know that people have various beliefs and reasons for why they are more or less concerned about their privacy regarding smart speakers. These may include valuing the usability of smart speakers more than their privacy, believing that having so much data out there already means that some more does not make a difference anymore, trusting the manufacturers of the smart devices to care for their privacy, etc.

This study aimed to investigate (lack of) privacy risk perception of smart devices and protective behaviour, to identify key beliefs and misbeliefs that keep people from taking protective action, and for gaining insights into possible helpful interventions.

We thank you for your help and the decision to participate in our study. If you know of any friends or acquaintances that are eligible and interested to participate in this study, please forward them the link to this survey and do not discuss it with them until after they have had the opportunity to participate. Prior knowledge of questions asked during the study can invalidate the results. We greatly appreciate your cooperation.

If you have any questions about the rights of research participants, please contact the Ethical Review Committee of the Behavioral and Management Sciences Faculty, University of Twente, Netherlands, ethicscommittee-bms@utwente.nl.

Thanks again for your participation.

Appendix B

Complete factor analysis

Table 1B

Factor loadings for powerlessness

Construct	Item	Factor loadings
Powerlessness	I believe that even if I try to protect my data, I can't prevent others from accessing them	.812
	I believe that in the end, I can't prevent others from accessing my data.	.786
	I believe that I don't have the power to protect my personal data effectively from all the possible dangers on the Internet.	.707
	I believe that if someone is determined to access my personal data, there is nothing I can do to stop them	.776
	I believe that it would be naïve to think that I can protect my personal data online reliably.	.590

Table 2B

Factor loadings for privacy as a value

Construct	Item	Factor loadings
Privacy as a value	It is important to her to have full control over who accesses personal information about her/him.	.885
	It is important to her/him to not share personal information (for example about personal preferences, one's health, or political and religious beliefs) with unknown others.	.765
	It is important to her/him to protect her/his privacy.	.754

Table 3B

Factor loadings for surveillance anxiety

Construct	Item	Factor loadings
Surveillance anxiety	It disturbs me that the smart speaker permanently monitors me.	.767
	I worry that my smart device is recording conversations when I talk to my friends.	.793
	It bothers me that others see my activities via the smart speaker.	.768
	The idea that I would be under surveillance by a smart speaker frightens me.	.590
	I find it objectionable when I do not know what will be recorded by smart speakers.	.566
	I am concerned that my smart device is capturing information even though I am not actively using it.	.635

Table 4B

Factor loadings for privacy risk perception

Construct	Item	Factor loadings

Privacy risk perception	How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?	.904
	How large do you think the risk is that your privacy is invaded now that you have this smart speaker installed?	.892
	To what extent do you think your privacy is at risk now that you installed a smart speaker in your household?	.855

Table 5B

Factor loadings protective behaviors

Construct	Item	Factor loadings			
Passive protective behavior	I will speak very quietly around the smart speaker, in case I don't want to be recorded	.791	.185	.140	.193
	I will avoid sensitive/private conversations around the smart speaker	.747	.439	.277	.122
	I will moderate my language around the smart speaker so that it doesn't record private matters, even if accidentally	.738	.362	.221	.062
	If I have a visitor, I will inform them that I have a smart speaker	.655	.254	.258	-.391
	I will consider where to place the smart speaker so that it is not positioned in areas where I typically engage in conversations involving sensitive or private information	.641	.285	.233	.068
	I will set a new difficult password for my smart speaker that I do not use for other applications	.632	-120	.543	.134
physical protective behavior	I will turn of the smart speaker when I am not using it	.138	.880	.159	.047
		.239	.809	.160	.038

	I will unplug the smart speaker when I am not using it	.340	.718	.328	-.124
	I will mute the smart speakers microphone when I am not using it	.527	.595	.302	.137
	I will turn off the smart speaker when I am having a serious/private conversations	.562	.570	.099	.125
	I will unplug the smart speaker when I am having a serious/private conversations	.156	.255	.826	.038
Privacy settings protective behavior	I will review the privacy settings of my smart speaker in the provider's account	.286	.093	.803	-.161
	I will review which application/services have access to my smart speaker	.153	.253	.770	.188
	I will restrict the amount of data that the device is allowed to collect through the smart speakers' settings	.355	.491	.622	.140
	In the app I will delete sensitive information that the smart speaker stored about me				
Security protective behavior	I will delete my smart speakers' recordings	.254	.519	.547	.091
	I will not write down the password ono a piece of paper or share it otherwise with house members or visitors.	.201	.097	.117	.910

Appendix C

SPSS codes

Frequencies and Descriptives for Demographics

```
FREQUENCIES VARIABLES=Age Gender Education
  /ORDER=ANALYSIS.

DESCRIPTIVES VARIABLES=Age Gender Education
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Reliability Analysis for Powerlessness

```
RELIABILITY /VARIABLES=Powerlessness_1 Powerlessness_2 Powerlessness_3
Powerlessness_4 Powerlessness_5
  /SCALE('Powerlessness') ALL /MODEL=ALPHA.
```

Reliability Analysis for Surveillance Anxiety

```
RELIABILITY /VARIABLES=SA_1_ SA_2_ SA_3_ SA_4_ SA_5_ SA_6
  /SCALE('Surveillance Anxiety') ALL /MODEL=ALPHA.
```

Reliability Analysis for Privacy as a Value (Male)

```
RELIABILITY /VARIABLES=PAV1m PAV2m PAV3m
  /SCALE('Privacy as a Value (Male)') ALL /MODEL=ALPHA.
```

Reliability Analysis for Privacy as a Value (Female)

```
RELIABILITY /VARIABLES=PAV1_female_ PAV2_female_ PAV3_female_
  /SCALE('Privacy as a Value (Female)') ALL /MODEL=ALPHA.
```

Reliability Analysis for Protective Behaviour

```
RELIABILITY /VARIABLES=PBg1 PBg2 PBg3 PBg4 PBg5 PBg6 PBg7 PBg8 PBg9 PBg10
PBg11 PBg12 PBg13 PBg14 PBg15 PBg16 PBg17
  /SCALE('Protective Behaviour') ALL /MODEL=ALPHA.
```

Reliability Analysis for Privacy Risk Perception

```
RELIABILITY /VARIABLES=prp01 prp02 prp03
  /SCALE('Privacy Risk Perception') ALL /MODEL=ALPHA.
```

Pearson's Correlation

```
CORRELATIONS
  /VARIABLES=NEWPower NEWSA NEWPAV NEWNTH NEWtrustinNew NEWSE
NEWPENJOY NEWPUSE ProtectiveBcombined RiskPerrceptionSUM
  /PRINT=TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

Multiple Linear Regression for Protective Behaviour

```
REGRESSION
  /DEPENDENT=ProtectiveBcombined
  /METHOD=ENTER NEWPower NEWSA NEWPAV NEWNTH NEWtrustinNew NEWSE
NEWPENJOY NEWPUSE.
```

Multiple Linear Regression for Privacy Risk Perception

```
REGRESSION
  /DEPENDENT=RiskPerrceptionSUM
  /METHOD=ENTER NEWPower NEWSA NEWPAV NEWNTH NEWtrustinNew NEWSE
NEWPENJOY NEWPUSE.
```

Factor Analysis

```
FACTOR
  /VARIABLES=Powerlessness_1 Powerlessness_2 Powerlessness_3 Powerlessness_4
Powerlessness_5
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES=SA_1_ SA_2_ SA_3_ SA_4_ SA_5_ SA_6
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.
```

```
FACTOR
  /VARIABLES=PAV1m PAV2m PAV3m PAV1_female_ PAV2_female_ PAV3_female_
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.


FACTOR
  /VARIABLES=prp01 prp02 prp03
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.



FACTOR
  /VARIABLES=PBg1 PBg2 PBg3 PBg4 PBg5 PBg6 PBg7 PBg8 PBg9 PBg10 PBg11 PBg12
PBg13 PBg14 PBg15 PBg16 PBg17
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.


FACTOR
  /VARIABLES=Powerlessness_1 Powerlessness_2 Powerlessness_3 Powerlessness_4
Powerlessness_5
        SA_1_ SA_2_ SA_3_ SA_4_ SA_5_ SA_6
        PAV1m PAV2m PAV3m PAV1_female_ PAV2_female_ PAV3_female_
        prp01 prp02 prp03
```

```
    PBg1 PBg2 PBg3 PBg4 PBg5 PBg6 PBg7 PBg8 PBg9 PBg10 PBg11 PBg12 PBg13
PBg14 PBg15 PBg16 PBg17
  /CRITERIA=PIN(.5) MINEIGEN(1) ITERATE(25)
  /EXTRACTION=PRINCIPAL
  /CRITERIA=ITERATE(25)
  /ROTATION=VARIMAX
  /METHOD=CORRELATION.
```