Assessing Privacy Risk Perception and Protective Behaviours in Relation to Smart Speakers: Expanding a Previous Model

Carl Moritz Pottkamp

Bachelor Thesis

Submitted to the Department of Psychology of Conflict, Risk and Safety

Faculty of Behavioural Management and Social Sciences

University of Twente

1st Supervisor: dr. Nicole Huijts

2nd Supervisor: dr. Marielle Stel

Abstract

Smart home technology has rapidly been integrated in many households, offering convenience and enjoyment through a variety of practical and entertaining applications. Among the most widely used smart home devices is the smart speaker. Despite its functionality, the smart speaker introduces significant privacy risks for its users, that are often overlooked by users. The aim of this study is to re-test the findings of an earlier study that looked at antecedents of privacy risk perception and protective behaviours among smart speaker use. Moreover, it tries to establish additional factors to the former model. This cross-sectional survey study involved 99 participants, including 65 non-owners and 34 owners of smart speakers. The results indicated that perceived creepiness (positive effect) and not likely the target (negative effect) significantly influenced participants' privacy risk perceptions and protective behaviours. Furthermore, each variable from the original study emerged as a significant predictor of either privacy risk perception or protective behaviour at different stages of the analyses or within specific subgroups, thus supporting the former model. The present study also highlighted the differences between owners and non-owners of smart speakers with regard to the factors that influence their protective behaviours. Nevertheless, the study's biggest limitation was the sample size, which did not allow for appropriate comparisons between smaller subgroups. Finally, the study offers evidence supporting privacy interventions, proposes suggestions for methodological improvements, and identifies gaps for further research.

Keywords. smart speakers, privacy, privacy risk perception, protective behaviour, perceived creepiness

Assessing Privacy Risk Perception and Protective Behaviours in Relation to Smart Speakers: Expanding a Previous Model

The prevalence of smart technology in today's homes continues to rise. Since the release of the earliest smart home devices, the industry has produced countless possibilities for integrating smart devices into our internet of things (IoT). The smart speaker is among the most widely adopted smart home systems. It incorporates Smart Home Personal Assistant (SHPA) technology, which is also often applied in smartphones, smartwatches, and smart TVs. Most SHPAs being used are developed by Amazon (Alexa) with about 70% of the US market share and Google with 24% (Google Assistant), while only about 6% come from other companies such as Apple (Siri) (Lutz & Newlands, 2021). Their scale of use is highlighted by recent European statistics indicating that the share of households owning a smart speaker ranges from 18% in France to 40% in Germany (Powell, 2023). As the technology advances, particularly due to developments in Artificial Intelligence (AI), not only sophistication but also the adoption of smart speakers is expected to grow (Fang & Fu, 2020). Simultaneously, this growth might also lead to more exposure to novel privacy threats that often seem to be underestimated by users (Boerman et al., 2021).

A couple of early studies examined the factors influencing the decision to adopt and use smart speakers (Chu, 2019; Kowalczuk, 2018; Voit et al., 2020). They found that privacy concerns are the primary reason for non-adoption (Chhetri & Motti, 2019; Lau et al., 2018), suggesting a crucial role for the evaluation of risk as a decision-making factor. Later studies confirmed this notion when looking at a person's likelihood to engage in privacy protective behaviour (e.g. unplugging their smart speaker when not using it). Here, individuals with higher privacy risk perceptions tended to display protective behaviours more often (Boerman et al., 2021). Hence, it is crucial to understand what underlying factors lead individuals to have a certain level of privacy risk perception. One study that investigated this relationship

identified factors in the literature that potentially lower an individual's privacy risk perception in relation to their smart speaker and tested them in a model (Hapke, 2023). The research resulted in a comprehensive model, however, new insights from qualitative research have yielded new indications for additional factors that could be explored in an extended model (Fruchter & Liccardi, 2018; Haney et al., 2021; Huijts et al., 2023; Kang et al., 2016). At the same time, a more complete model could also test for supporting factors that could explain heightened privacy risk perception, as opposed to be limited to undermining factors.

This study's aim is to enhance the knowledge of the field by identifying factors that influence users' (including both undermining and supporting factors) privacy risk perception as well as their protective behaviours towards smart speakers. The study opts to systematically test the newly identified and original factors (by Hapke 2023) for their relative importance in a predictive model.

Theoretical Background

Smart home technology offers users convenience and comfort in everyday life (Huijts et al., 2023). Some devices offer security applications, as for example the smart doorbell which is providing its users with video and audio recordings of their entrance (Selinger & Durant, 2022). Others are primarily used for entertainment purposes, like smart TVs. In fact, the majority of TVs shipped are incorporating smart functions, resembling the general trend towards more smart home devices (Alam et al., 2017). Typically, smart home devices help users save time and energy by reducing the effort required for a specific task or goal (e.g. Alexa, switch off the lights). Furthermore, the assembly of the different devices is often inter-connected, composing the larger smart home system (SHS) (Chakraborty et al., 2023). One central device that connects the ties of the different technologies is the smart speaker. Usually placed at a strategic place within the home, users can hands-free combine the many use cases of the other devices with the smart speakers' own features by using natural language.

Commands can be, for example, asking about the weather, playing music or to switch on the lights. Nevertheless, the convenience of adopting IoT devices such as the smart speaker, forces us to incorporate a multitude of sensors within our home (Gram-Hanssen & Darby, 2018).

The home has historically served as a central locus of privacy protections for humans (Lau et al., 2018). Others emphasise the home as the place for security and control (Gram-Hanssen & Darby, 2018), suggesting an important difference between smart speakers (at home) and SHPAs (in handheld or portable devices). Metaphorically, the home can be compared to a computer's hard drive. It possesses the capacity to securely store various personal belongings, images, and memories, thereby shaping an individuals' sense of identity, stability, and autonomy (Chesnokova, 2021). Though, with the integration of smart home technologies connecting the computer and its hard drive to the internet, new possibilities emerge for external access and exploitation of this newly created data flow. Consequently, prioritizing privacy in the use of smart speakers becomes imperative. Privacy can be conceptualized as the individual's fundamental right to regulate the collection, utilization, and sharing of their data, thereby ensuring that their personal information remains under their control (Klobas et al., 2019).

Risks for Users

Smart speaker technology poses an imminent privacy threat to its users. SHPA technology relies on microphone input of the surrounding and a fixed connection to the internet to be able to respond to requests appropriately. Smart speakers are "always on", thus constantly listening to their surroundings, waiting for the recognition of the wake word (Lutz & Newlands, 2021). Upon recognition, the device begins recording the user's interactions, enabling natural language interaction. The live audio data is continuously transmitted to the provider, with user recordings stored in the cloud for access by both the manufacturer and the

user. According to Bolton et. al (2021), there are already a significant number of “unwanted” recordings (e.g. recordings without users uttering the wake word) occurring, that are often containing sensitive information. This raises concerns about the potential surveillance capabilities of smart speakers, providing opportunities for malicious actors, such as hackers to capitalize on this data. Such exploitation can extend beyond simply accessing recorded data to tapping into real-time sensor feeds. (Huijts et al., 2023; Lutz & Newlands, 2021).

Equally, some data breaches lack apparent physical manifestations and yet have profound impacts on the individual. As noted, data is stored by manufacturers to improve their service, yet it also grants third-party access to recorded information, creating an accumulation of sensor data retained over extended periods (Lutz & Newlands, 2021). A recent concept devised to capture this phenomenon is the Internet of Behaviour (IoB), which leverages sensory data from the Internet of Things (IoT) and analytical capabilities to predict human behaviour and preferences (Di Gangi et al., 2023).While this data enhances convenience for consumers by optimizing device functionality, it can also be leveraged by the provider to create specific user profiles for individualised marketing purposes, as for example with hiking gear advertisements when it has been previously talked about hiking in the realm of the smart speaker.

The role of Privacy Concerns

In fact, many users have limited or incorrect knowledge about privacy threats related to their smart devices (Bermejo Fernandez et al., 2021; Bombik et al., 2022; Emami-Naeini et al., 2019; Shaikh et al., 2019). This lack of understanding also extends to how one can protect their personal privacy, as many users struggle to find clear and helpful information (Emami-Naeini et al., 2019). Interestingly, in a study about IoT devices, Emami-Naeini et al. (2019) found that, users had few privacy concerns prior to purchasing but developed more concerns afterwards. Applying this to smart speakers seems difficult considering that in general only

few users engage in privacy-seeking behaviours (Lau et al., 2018). Conducting studies investigating the difference between owners and non-owners could help clarify if privacy concerns are often just not translating to protective behaviour or if smart speakers have a dynamic that makes them different to other IoT devices. Support for the difference between owners and non-owners (pre and after purchase) came from the work by Hapke (2023). The study showed that the variables influencing participants privacy risk perception and privacy protective behaviours differed depending on the ownership status, suggesting a distinction for future studies. Thus, given that many researchers are calling for campaigns to raise awareness about privacy matters and provide information on how to protect one's privacy in the use of smart speakers (Emami-Naeini et al., 2019; Gerber et al., 2018; Lau et al., 2018a; Lutz & Newlands, 2021), it may be crucial for future interventions to differentiate between owners and non-owners due to their difference in levels of concern and underlying reason.

To comprehend whether an individual perceives these risks and, subsequently, engages in protective behaviour, it is crucial to understand the factors that precede their privacy risk perception and protective behaviours. There is currently one quantitative model that aims to explain protective behaviour and privacy risk perception in smart speaker use (Hapke, 2023). The present study seeks to extend this model developed by Hapke in 2023. The original model aimed to predict privacy risk perception and the corresponding protective behaviours, using factors identified in qualitative literature and the Protection Motivation Theory (PTM). The current research will delve into more recent qualitative literature, excluding quantitative studies or additional models from its scope.

Originally, Hapke (2023) identified six factors undermining privacy risk perception and protective behaviours; *perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy*, and *privacy self-efficacy*. Later, based on the results of the factor analysis, she proposed the addition of

security self-efficacy derived from privacy self-efficacy. Moreover, the analysis suggested the addition of *powerlessness* as a factor derived from resignation towards a lack of privacy. In contrast to Hapke's original variables, the two additional factors had shown to be supporting factors that would increase instead of decreasing the outcome variables of the study.

Her general findings revealed several significant effects for the factors. During her analysis all identified factors showed significant relationships at some point of the analysis (for the correlational and regression analysis). However, not all variables showed significant effects for both dependent variables. Among the significant predictors for both privacy risk perception and protective behaviour were perceived enjoyableness and resignation towards a lack of privacy. In the regression analysis including all eight predictors, nothing to hide beliefs and perceived usefulness showed no significant effects for both outcomes. Yet, they yielded significant moderate correlations in the correlation analysis. Furthermore, the study found a positive association between privacy risk perception and protective behaviour. This supports previous findings suggesting a co-dependency of the outcome's variables (Boerman et al., 2021). Finally, no factor in the model was found to be obsolete, therefore, future studies could make use of Hapke's (2023) factors as a guide for their model.

This study aims to extend the model of Hapke (2023) by examining recent qualitative literature. At the time of Hapke's study, new qualitative studies have been published that specifically address privacy experiences of users (Haney et al., 2020, 2021; Huijts et al., 2023). The studies hinted towards factors that could act as additional predictors for privacy risk perception and protective behaviours. Accordingly, in the following part, the new factors identified in qualitative studies will be discussed as an extension for the model.

Perceived Regulatory Protection

The first factor identified, Perceived Regulatory Protection, was derived from the work by Haney and colleagues (2021). In their work, they looked at responsibility

perceptions of users towards privacy protection in smart home devices by the means of interviews. Fifteen of the forty interviewed users remarked the government as having at least some responsibility over users' privacy. For example, one user stated that user's privacy is already established by the government in other industries "I think the other half of the responsibility goes on the government to protect your citizens … There's other safety precautions put in other industries. I don't see why that shouldn't be something applied to this industry as well" (Haney et al., 2021, p.9). Given the assumed responsibility of the government to protect users' privacy when using smart home devices, users may underestimate their privacy risk and hence feel secure enough to refrain from additional protective behaviours.

This association has been confirmed in a study by Bombik and Colleagues (2022), which compared privacy risk perceptions towards smart home devices (including smart speakers) among users from the United States, United Kingdom, and German-Speaking countries. The results showed a significant negative relationship between perceived regulatory protection and privacy risk perception. The study showed that perceived regulatory protection can serve as a predictor for privacy risk perception in many countries, including Germany, which will be the main source of participants for this study. Thus, the factor will be included in the model, to test its significance as a predictor for both privacy risk perception and protective behaviour.

Not likely the Target

The second additional factor was identified in a study conducted by Huijts et al. (2023), in which participants received a smart speaker and other devices, that unknowingly simulated cyber-attacks in their home setting. Subsequent, participants were questioned about their experience in interviews that have been coded and analysed. One emerging theme was that people felt that they do not have anything valuable to offer, so nothing could be the

stolen from their devices since they are so ordinary (“I wonder what they are looking for with me. Such a regular family. There are no millions in the home, they cannot find anything here that someone would be happy with. Then I think to myself, well, it will not happen to me, I don’t think so.“ (Huijts et al., 2023, p.2250). Moreover, another participant mentioned that they are neither rich or famous and consequently not interesting for hackers (“ Exactly, because we’re not bankers or Theresa May or someone who is actually, you know, hacking the..” (Huijts et al., 2023, p.2250). Evidence from another study found similar statements (“I don’t have much money to worry about” (Kang et al., 2016, p.47). What may be true about these statements is that influence (e.g. money and fame) can be an incentive for hackers to target specific people. Still, as the minority of people are rich or famous, hackers are often also targeting the small people when they have the opportunity. By believing that cybercrime only happens to the rich and powerful people, individuals might underestimate their privacy risk. Following this line of reasoning, it can be theorised that this “not likely the target” belief could potentially influence privacy risk perceptions, whereby higher mean values of not likely the target correlate with lower risk perceived and vice versa.

In the literature, not likely the target is usually not distinguished from "nothing to hide beliefs (as also identified by Hapke, 2023). However, it is important to differentiate between the two concepts. “Not likely the target” concerns the probability of being targeted, while “nothing to hide beliefs” relate to the expectation of significant negative consequences if targeted. Individuals who believe they have nothing to hide may perceive lower risks of severe negative outcomes from being observed. Nonetheless, they may still acknowledge the possibility of being targeted for malicious intent. This differentiation is crucial as it relates to understanding both the probability and the perceived magnitude of potential consequences and is therefore interesting to confirm in a model with nothing to hide beliefs.

Perceived Creepiness

The concept of creepiness is widespread, finding application in various contexts, from describing the creepy neighbour next door to the strange feeling associated with sitting in a self-driving car. In the territory of technological studies, creepiness has been an established factor in for example in research with human-looking robots, predating the widespread adoption of smart speakers in society (Ho et al., 2008). Creepiness related to technology can be defined as the feeling of unease or discomfort experienced in the interaction with the device. This discomfort can not only stem from factors like design, behaviour, violation of norms, and potential harm but also from privacy concerns due to the collection of data (Wozniak et al., 2021). One related study by Fruchter & Liccardi (2018) looked at privacy concerns in online reviews related to smart speakers and found creepiness to be a prevalent theme, with about 6% of all reviews mentioning some form of "creepiness". Reviewers expressed concerns about the creepy behaviour of the device, noting how their home assistants changed or violated their personal conceptions of privacy in the home environment ("I wanted a smart alarm clock but purchased a SPY." (Fruchter & Liccardi, 2018, p.4). Despite its relevance to feelings of privacy, the factor was not included in the study by Hapke (2023) and has yet received limited attention in the study of privacy risk perceptions and protective behaviours.

One recent study offered indicators for how perceived creepiness could influence privacy risk perception. In the study, Mou and Meng (2023) were interested in the role of creepiness in the resistance towards smart speakers in non-adopters of the technology. They found that consumers privacy concerns are mediated through perceived creepiness, indicating that individuals were more reluctant to adopt a smart speaker due to the creepiness of the device that resulted in more privacy concerns. Following these results, it can be theorised that high levels of perceived creepiness could increase both privacy risk perception and protective behaviours. This could be explained by the notion that feelings of creepiness prompt

individuals to become more cautious and inclined to take proactive measures to alleviate perceived privacy risks when they feel uncomfortable or uneasy. To test whether this can be statistically supported, perceived creepiness will be included in the model.

Current Study

In conclusion, the main aim of this study is to extend Hapke's (2023) model by incorporating the variables perceived *regulatory protection*, *not likely the target*, and *perceived creepiness*. The second aim is to re-test the effects of Hapke's original variables on the outcomes of privacy risk perception and protective behaviour, which include perceived *enjoyableness*, *perceived usefulness*, *trust in smart speaker companies*, *nothing to hide beliefs*, *resignation towards lack of privacy*, *privacy self-efficacy*, *security self-efficacy*, and *powerlessness*. The relationship between the two dependent variables will also be analysed, with privacy risk perception assumed to predict protective behaviours.

Furthermore, similar to Hapke's study, this research will re-test these hypotheses in the subgroups of smart speaker owners and non-owners to determine if the findings are consistent across these groups. The hypotheses identified by Hapke (2023) can be found in Appendix B, but they will not be included in the main hypotheses. The final hypotheses of this study are the following:

H1: Perceived Regulatory Protection has a negative effect on (a) Privacy Risk Perception and (b) Protective Behaviour.

H2: Not likely the target has a negative effect on (a) Privacy Risk Perception and (b) protective behaviour.

H3: Perceived Creepiness has a positive effect on (a) Privacy Risk Perception and (b) Protective Behaviour.

Methods

Participants

The participants for the present study were recruited via the following platforms: The researchers personal social media accounts, and the University of Twente study recruitment website SONA. The participants filled in the survey between the 16th of April to the 9th of May. The G*Power calculation revealed that for a medium effect size ($f^2 = 0.15$) with 11 predictors a sample of 89 participants is required. In total 119 participants completed the questionnaire whereby 20 had been removed due to failures to meet the attention checks. Thus, resulting in enough participants to meet the requirements of the G*Power analysis (n = 99). Out of the final 99 participants about 62% were students, while around 37% indicated to be working, with most people originating from Germany (79%), the Netherlands (5.9%) and Spain (2.9%). Moreover, the participants age ranged from 18 to 65 (*M*=29.47 *SD*=12.4). The gender distribution was approximately 60% male, 37% female, 1% other and 1% preferred not to say. In terms of the education, 1% of the participants completed primary education, 36% completed secondary school, 24% have completed professional education, 24% completed their bachelor's degree, 13% holding a master's degree and 1 having a doctorate.

Regarding the defining questions about the smart speaker use, about 20% of the survey takers were primary smart speaker owner/users (Main owner/user of the device) (*n= 20*) and 14% secondary smart speaker users (Users but not the owners) (*n= 14*). The majority of 66% indicated that they do not own a smart speaker (n= 65). The possession period among participants who own a smart speaker was the highest for the option "More than two years". Furthermore, about 48% of them said that they personally installed the smart speaker and 52% did not. Many of the participants indicated to have heard about someone having encountered a cyber-attack in their life before (48%), of those who did, 6% have only been attacked personally, 10% have heard of someone AND experienced it personally, while 34% have not heard about someone experiencing or experienced a cyber-attack themselves.

Design

The study is designed as a cross-sectional survey with a correlation design. The questionnaire was created with Qualtrics and can be found in the Appendix A. Before starting with the survey, participants gave informed consent, and were then asked to answer smart speaker related questions regarding ownership, use, and possession period. Depending on their ownership, participants were then divided in 2 groups, where those who do not own a smart speaker received a "scenario" in which they were asked to imagine that they have been gifted one. The other group consisted of the people who indicated that they own a smart speaker. Accordingly, participants received the same questions, however, slightly rephrased to match their ownership. Further, the questions were presented in the same sequence, starting with protective behaviours, privacy risk perception, perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, privacy self-efficacy, perceived regulatory protection, not likely the target, perceived creepiness, and experience of a cyber-attack. Finally, the survey ended with questions about participants' demographics.

Materials

The materials part will be split up between the original scales by Hapke (2023) and the Additional/Adjusted scales.

Original Scales (Hapke 2023)

The factors identified by Hapke (2023) will be examined similarly to Hapke's (2023) study and are explained in more detail in her report. Some scales were slightly adjusted in wording to accommodate the two scenarios (owning vs. non-owning a smart speaker), while others remained consistent across both groups. To ensure accuracy, the mean and alpha values were reported either separately (Owning/non-owning) for each group or combined.

The factors adjusted according to group ownership include perceived enjoyableness (Non-owning: M=2.83, SD=1.06, α=.89; Owning: M=3.03, SD=0.57, α=.83), perceived

usefulness (Non-owning: M=2.3, SD=0.91, α=.90; Owning: M=3.06, SD=0.92, α=.84), and privacy risk perception (Non-owning: M=3.37, SD=1.03, α=.92; Owning: M=1.51, SD=0.71, α=.75). Detailed differences in the questions are provided in the questionnaire in Appendix A.

Furthermore, the remaining scales did not require adjustments, so the alpha and mean values are displayed for the entire sample: trust in smart speaker companies (Combined Group: M=2.27, SD=0.74, α=.84), nothing to hide beliefs (Combined Group: M=2.95, SD=0.79, α=.66), security self-efficacy (Combined Group: M=2.24, SD=0.87, α=.79), and privacy self-efficacy (Combined Group: M=2.35, SD=0.77, α=.81). All items from the questionnaire are provided in Appendix A.

Additional and Adjusted Scales

The factor loadings for all adjusted scales, excluding protective behaviours (depicted in Table 1), are available in Appendix C (Powerlessness, Perceived Regulatory Protection, Not Likely the Target, and Perceived Creepiness). More detailed information regarding the origin of the scale, characteristics (Mean, Standard Deviation and Alpha), and their measurement will be provided below.

Powerlessness. As mentioned earlier, the idea for the inclusion of the factor of powerlessness originated from the work by Hapke (2023). However, for this study the scale will be exchanged with the scale from Lutz and Colleagues 2020, as it incorporates more items and captures the concept more comprehensively. The new scale consists out of five instead of three items. An example of a question is as follows: “I believe that even if I try to protect my data, I can’t prevent others from accessing them.” The items had to be answered on a five-point Likert scale (Strongly disagree – Strongly agree). The factor analysis did not reveal more than one factor within the scale and Cronbach’s alpha was also satisfying. As this scale was measured by the exact same questions, regardless of the ownership, hence the combined Cronbach’s Alpha was calculated (Combined Group M=3.63, SD=0.83, α=.82).

Resignation towards a lack of Privacy. This factor was entirely adapted from the study by Hapke (2023). Similar as in Hapke's study, upon examining the eigenvalues, a two-factor solution for the variable seemed to be the most appropriate. However, upon reviewing the scales before and after the factor analysis, two items would have had been deleted due to low factor loading. This would have led to two small scales with only two items that are showing an inacceptable Cronbach's Alpha value. Thus, it seemed to be the most appropriate to leave the scale as it was originally designed (incorporating only one factor). This also brought about the best reliability among all options. This decision is also backed up by the fact that the second factor that was found by Hapke (Powerlessness), is still incorporated with a separate scale in this study (Combined Group M=3.14, SD=0.68, α=.61).

Protective Behaviours. The dependent variable protective behaviour measurement will be partially adopted from the work of Hapke (2023) and also extended by the behaviours found in the work of Lutz and Newlands (2021). The revised protective behaviours can be found in Table 1. In the present measure, participants who did not own a smart speaker were asked to answer 17 five-point Likert scale questions indicating the likeliness of them performing that behaviour (Extremely unlikely – Extremely likely). Concerning the group where people indicated that they own or at least live in a household with a smart speaker, participants answered 19 questions (Two more than in the not owning condition). For the first 16 questions, participants had to indicate on a five-point Likert scale how often they engaged in the proposed behaviours (Never – Always). The last three items of the variable were designed as Yes and No questions since they could have not been answered sufficiently with a Likert scale, however, this was not the case for the not owning condition.

To determine if there are subdimensions of behaviours and if these subdimensions have distinct predictors, the protective behaviours of the two groups (owners and non-owners) were reduced to 14 matching behaviours and combined for factor analysis. After

reviewing the results, particularly the scree plot and the eigenvalues, it became apparent that there are likely two distinct factors within the variable (Eigenvalue 1: 9.19; Eigenvalue 2: 1.16).

After assigning the items to the two factors, Factor One included PB 1, 2, 3, 4, 5, 12, and 13 (see Table 1), while Factor Two included PB 6, 7, 8, and 9. Items PB11 and PB14 showed the lowest factor loadings and the highest uniqueness levels, around .55, explaining only 45% of the variance. Another item that did not discriminate well was Item 10, as it loaded relatively high on both factors (Factor 1: .558; Factor 2: .724), possibly due to shared characteristics between the two factors.

After removing items 10, 11 and 14 for a second factor analysis, the number of factors remained the same with similar values for the items. The resulting two factor model is not in line with what Lutz and Newlands (2021) found in their analysis. Originally, they found three factors: Technical, Data and Social. In the analysis, it appears that the latter social factor is not included but somehow merged with Technical to a “physical” factor, that explained behaviours that are physically observable as for example in “moderating language” in PB12 and “unplugging the smart speaker” in PB2 (Physical: M=2.45, SD=1.31, α=.94). The second factor “Data”, however, can be found in the present protective behaviour as all the questions are relating to some action that secures data privacy with digital behaviour as for example “restrict amount of data” or “delete recordings” (Data: M=3.00, SD=1.39, α=.91). Consequently, for the analysis, the dependent variable protective behaviour is further divided in protective physical behaviour and protective data behaviour.

Table 1

The items measuring protective behaviours of the combined groups and their factor loadings for a two-factor model.

Protective Behaviours (PB)	Factor 1 Loadings	Factor 2 Loadings
PB1. I turned off the smart speaker when I was not using it/ I will turn off the smart speaker when I am not using it	***.734***	*.296*
PB2. I unplugged the smart speaker when I was not using it I will unplug the smart speaker when I am not using it	***.741***	*.302*
PB3. I unplugged the smart speaker when I was having serious/private conversations/ I will unplug the smart speaker when I am having serious/private conversations	**.816**	.303
PB4. I turned off the smart speaker when I was having serious/private conversations/ I will turn off the smart speaker when I am having serious/private conversations	**.823**	.421
PB5. I muted the smart speakers microphone when I was not using it/ I will mute the smart speakers microphone when I am not using it	**.743**	.488
PB6. I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account/ I will review the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account	.341	**.811**
PB7. I reviewed which applications/services have access to my smart speaker/ I will review which applications/services have access to my smart speaker	.358	**.728**
PB8. I restricted the amount of data that the device is allowed to collect through the smart speaker's settings/ I will restrict the amount of data that the device is allowed to collect through the smart speaker's settings	.276	**.832**
PB9. I deleted my smart speaker recordings/ I will delete my smart speaker recordings	.492	**.711**
PB10. In the app I deleted sensitive information that the smart speaker stored about me/ In the app I will delete sensitive information that the smart speaker stored about me.	.558	.724
PB11. I spoke very quietly around the smart speaker, in case I did not want to be recorded/ I will speak very quietly around the smart speaker, in case I don't want to be recorded	.569	.312
PB12. I moderated my language around the smart speaker so that it didn't record private matters, even if accidentally/ I will moderate my language around the smart speaker so that it doesn't record private matters, even if accidentally	**.719**	.394
PB13. I avoided sensitive or private conversations around the smart speaker/ I will avoid sensitive or private conversations around the smart speaker	**.748**	.481
PB14. When I had a visitor, I informed them that I have a smart speaker/ If I have a visitor, I will inform them that I have a smart speaker	.519	.421

Note: Items that load sufficiently for either factor have been marked in bold.

The following factors were identified in the literature to enhance the model.

Perceived Regulatory Protection. This scale was adopted from Bombik et al. (2022) and measured the Concept of Perceived Regulatory Protection for a variety of smart home

devices including smart speakers. Since the original measure only mentions third parties as potential threats to privacy, the scale for the present work will also incorporate regulatory protection against the threat of misuse by the smart speaker company and is hence reformulated from 3 to 4 items. Moreover, it uses a five-point Likert scale (Strongly disagree – Strongly agree) as measure. One example statement is: “I feel that current laws and regulations are adequate to protect my Smart Speaker data from misuse of data by the smart speaker company itself”. (Non-owning M=2.33, SD=1.04, α=.89; Owning M=2.76, SD=1.01, α=.84). The entire scale can be found in Appendix A.

Perceived Creepiness. The Measurement for Perceived Creepiness was adapted from Raff et al 2024. The original scale incorporated 7 questions, however, due to similarities in the formulation, three items have been excluded that did not add additional value. Participants are asked to indicate agreement with the statements on a five-point Likert scale (Strongly disagree – Strongly agree). An example statement for the questionnaire is: “This smart home assistant makes me uncomfortable” (Non-owning M=3.31, SD=1.1, α=.90; Owning M=2.06, SD=0.75, α=.77;). All items of the scale can be found in Appendix A.

Not likely the Target. This scale is self-created since, to the authors knowledge, there have been no scales measuring this concept in the literature. However, it is inspired by findings from qualitative research. For this factor, participants are asked to indicate agreement with three statements on a five-point Likert scale (Strongly disagree – Strongly agree). An example of a statement that has been formulated is as follows: “I feel that, because I am not rich or famous, my data is not worth stealing. (Non-owning M=2.33, SD=0.96, α=.78; Owning M=3.00, SD=0.96, α=.72;). The items belonging to the scale can be found in Appendix A.

Data Analysis Plan

The analysis was done by using R-Studio (Version 2024.04.0+735). First, the demographics have been analysed by using descriptive statistics and frequencies. Then, the scales for the different factors have been analysed for internal consistency and reliability with factor analysis, descriptive statistics, and reliability analyses (Cronbach's Alpha). To be able to reliably use the data for the analysis, the assumptions have been checked (Linearity, Normality Multicollinearity, Independence, and Homoscedasticity). Additionally, a G*Power analysis was conducted (G*Power Version 3.1.9.7) to establish if the sample is large enough for the regression analysis with 11 predictor variables. Then, the hypotheses have been tested utilizing correlational analysis and a multiple regression analysis. After completing the hypothesis testing with the overall protective behaviour factor, the correlational analysis was repeated for the two sub variables found in the factor analysis. Finally, owners and non-owners of smart speakers have been analysed individually in a multiple linear regression model.

Results

Hypothesis Testing

The analysis is divided into two parts. The first part, "Hypothesis Testing," evaluates the significance of the relationships between the predictor variables and the outcomes privacy risk perception and protective behaviours. This part involves conducting a correlational analysis and a multiple linear regression analysis. The second part, "Exploratory Analysis," involves two multiple linear regression analyses, one for each dependent variable, with groups divided based on ownership status (owning versus non-owning). Additionally, a final correlational analysis will be conducted to examine the sub-variables of protective behaviours.

Table 2 presents correlations of each predictor with privacy risk perception and protective behaviour.

Table 2

Pearson's Correlation between the predictor variables and the outcome variables privacy risk perception and protective behaviour

	Privacy Risk Perception		Protective Behaviour	
	r	*p*	*r*	*p*
Privacy risk perception	-	NA	**.44**	**<.001**
Perceived enjoyableness	**-.27**	**.005**	**-.23**	**.018**
Perceived usefulness	**-.26**	**.007**	**-.25**	**.011**
Perceived creepiness	**.55**	**<.001**	**.62**	**<.001**
Perceived trust in companies	**-.41**	**<.001**	-.14	.130
Nothing to hide beliefs	**-.29**	**.003**	**-.34**	**<.001**
Resignation towards a lack of privacy	-.14	.14	**-.32**	**.001**
Not likely the target	**-.32**	**.003**	**-.37**	**<.001**
Privacy Self-Efficacy	-.15	.11	.11	.278
Security Self-Efficacy	-.09	.33	**.20**	**.034**
Powerlessness	.07	.44	-.08	.401
Perceived Regulatory Protection	-.18	.06	-.08	.432

Note: All significant effects are marked in bold

Hypotheses of the Present Work

Based on the correlational matrix with all identified predictor variables and the outcome variables privacy risk perception and protective behaviours, the following can be concluded (see Table 2):

H1: Perceived regulatory protection did not show a significant predict (a) privacy risk perception and (b) protective behaviours and is therefore rejected.

H2: Not likely the target shows significantly predicts privacy risk perception (a) as well as (b) protective behaviour, hence, the hypothesis is supported.

H3: The results showed a statistically significant correlation for perceived creepiness on both (a) privacy risk perception and (b) protective behaviour, thus, the hypothesis is supported.

Hypotheses of the Previous Study

The following conclusions can be drawn regarding the control variables identified in the previous study by Hapke (See Appendix B for the original hypotheses):

H1: Privacy risk perception exhibited a significant positive effect on protective behaviour; thus, the hypothesis is supported. This confirms the findings of Hapke (2023).

H2a & H2b: In support of the hypothesis, perceived enjoyableness showed a significant negative effect on privacy risk perception. Similarly, perceived enjoyableness demonstrated a negative correlation with protective behaviour, supporting the hypothesis. This also confirms the results found by Hapke (2023).

H3a & H3b: Perceived usefulness showed a negative correlation with privacy risk perception, supporting the hypothesis. Likewise, perceived usefulness had a negative association with protective behaviours, resulting in support for the hypothesis. Again, this applied also for the findings of Hapke (2023).

H4a & H4b: Trust in smart speaker companies showed a negative association with privacy risk perception, thus supporting the hypothesis. However, trust in smart speaker companies did not show a significant relationship with protective behaviour, leading to the rejection of the second part of the hypothesis (H4b). H4a and H4b were both significant in the study by Hapke (2023), showing a difference in the findings between the second part of the Hypothesis in the studies.

H5a &H5b: Supporting the hypothesis, nothing to hide beliefs demonstrated a negative relationship with privacy risk perception. Additionally, nothing to hide beliefs had a negative correlation with protective behaviour, supporting the hypothesis. H5a and H5b were both significant in the Study by Hapke (2023).

H6a & H6b: Resignation towards a lack of privacy did not have a significant relationship with privacy risk perception, resulting in the rejection of the hypothesis. However, resignation towards a lack of privacy showed a negative correlation with protective behaviour, supporting the hypothesis. In Hapke's (2023) study H6a and H6b were significant, resulting in a difference Hypothesis 6a between the two studies.

H7a & H7b: Privacy self-efficacy did not demonstrate a significant correlation with privacy risk perception, resulting in the rejection of the hypothesis. Similarly, privacy self-efficacy did not have a significant relationship with protective behaviour, contradicting the hypothesis. The Hypothesis 7a was supported in the former study by Hapke (2023), while H7b was not.

H8a & H8b: Powerlessness did not show a significant relationship with privacy risk perception, contradicting the hypothesis. Likewise, powerlessness did not significantly correlate with protective behaviours, leading to the rejection of the hypothesis. These results were different in Hapke's Study (2023) since H8a was supported and H8b was not.

H9a & H9b: Security self-efficacy did not exhibit a significant association with privacy risk perception, contradicting the hypothesis. However, security self-efficacy demonstrated a positive effect on protective behaviour, supporting the latter hypothesis (H9b). The first part of the hypothesis was supported in the study by Hapke (2023) while the second part was not.

Regression Analysis

To further test the hypotheses, a first regression analysis was conducted with privacy risk perception as dependent variable with all predictor variables on the whole sample (Table 3). The regression analysis revealed only two significant effects for privacy risk perception. The first effect was perceived creepiness which had a moderate positive relationship with privacy risk perception, supporting the hypothesis. Secondly, trust in smart speaker companies, which had a low to moderate negative relationship with privacy risk perception, also supporting its hypothesis.

Table 3

Multiple linear regression of the whole sample with Privacy Risk Perception as the Dependent Variable

Variable	*B*	*SE*	*t*	*p*
(Intercept)	2.93	0.73	3.973	**<.001**
Perceived enjoyableness	-0.01	0.11	-0.156	.873
Perceived usefulness	0.12	0.11	1.086	.286
Perceived creepiness	**0.43**	**0.08**	**5.11**	**<.001**
Trust in smart speaker companies	**-0.33**	**0.14**	**-2.37**	**.019**
Nothing to hide beliefs	-0.04	0.14	-0.33	.737
Resignation towards lack of privacy	-0.11	0.15	-0.76	.442
Not likely the target	-0.07	0.10	-0.71	.479
Powerlessness	0.11	0.12	0.88	.374
Privacy self-efficacy	-0.09	0.17	-0.53	.591
Security self-efficacy	0.05	0.13	0.04	.676
Perceived regulatory protection	-0.03	0.08	-0.41	.670

Note. All significant effects are marked in bold. Model Significance: $F(11, 87) = 5.95$, $p<.001$
R^2=.35 (N = 99)

In Table 4, a similar regression is displayed, however, with protective behaviour as the dependent variable. The findings showed that for the outcome protective behaviours, three of the eleven predictors had a significant effect. Similar to privacy risk perception, perceived creepiness had a significant positive relationship with the outcome variable, showing support

for the hypothesis. Secondly, in support of the hypothesis, resignation towards a lack of privacy had a negative significant relationship with protective behaviours. Furthermore, security self-efficacy had a moderate positive significant relationship with protective behaviour, also supporting its hypothesis. Finally, not likely the target had shown to be marginally significant for the protective behaviours, supporting the hypothesis given an adjusted p. Besides the factors depicted in Figure 1, none of the predictors supported their respective hypotheses.

Table 4

Multiple linear regression of the whole sample with Protective Behaviour as the Dependent Variable

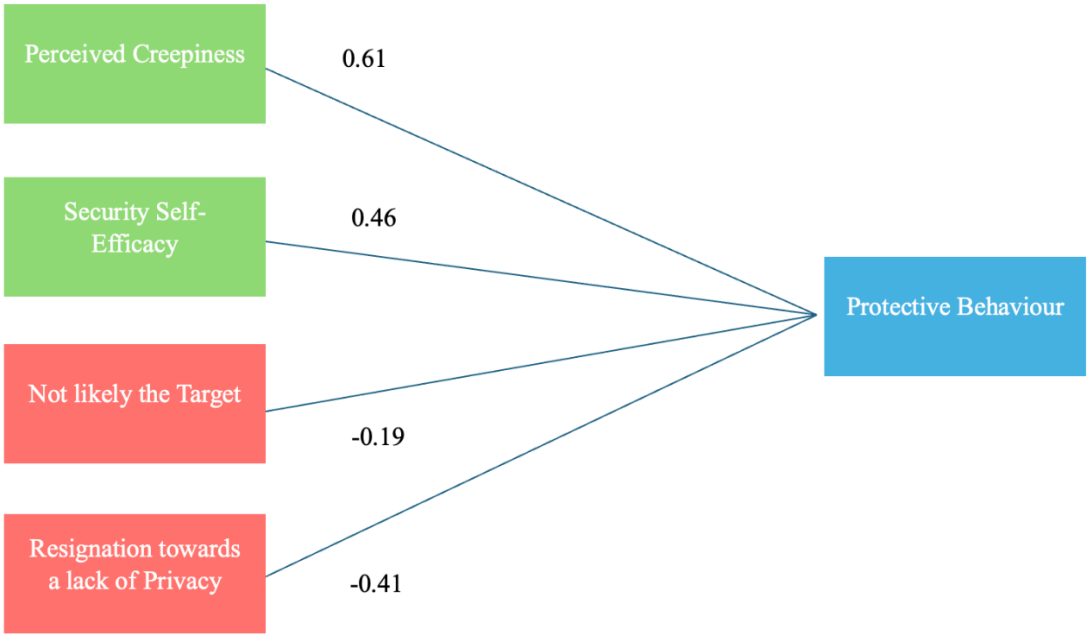
Variable	*B*	*SE*	*t*	*p*
(Intercept)	1.09	0.78	1.39	.168
Perceived enjoyableness	0.03	0.11	0.30	.754
Perceived usefulness	0.01	0.11	0.13	.891
Perceived creepiness	**0.61**	**0.09**	**6.79**	**<.001**
Trust in smart speaker companies	0.12	0.15	0.80	.421
Nothing to hide beliefs	-0.07	0.15	-0.47	.634
Resignation towards lack of privacy	**-0.41**	**0.16**	**-2.47**	**.015**
Not likely the target	-0.19	0.11	-1.63	.102
Powerlessness	0.21	0.13	1.52	.132
Privacy self-efficacy	-0.19	0.1	-1.07	.289
Security self-efficacy	**0.46**	**0.14**	**3.28**	**<.001**
Perceived regulatory protection	-0.02	0.08	-0.24	.806

Note. All significant effects are marked in bold. Model Significance: $F(11, 87) = 5.95$, $p<.001$

R^2=.49 (N = 99)

Figure 1

Significant and marginally significant predictors with effect sizes for the outcome protective behaviour



Note. Positive predictors were displayed on in green and negative predictors in red

Exploratory Analysis

To enhance the understanding of the data, two multiple linear regression analyses were conducted for the divided sample (owners vs. non-owners), focusing on privacy risk perception and protective behaviours. Additionally, a correlational analysis was performed for the sub-variables of protective behaviours (physical and data) and all predictor variables.

Regression Analysis on the Divided Sample

In the following part, a comparison is made between the participants who own a smart speaker and those who do not for the two dependent variables. However, since neither of the two groups are according to the G*Power calculation big enough for conducting a regression analysis, the results must be taken with caution (small effects will unlikely be detected).

A regression table was calculated for the subgroups owning and not owning a smart speaker with privacy risk perception as the dependent variable (see Table 5). For participants owning a smart speaker, none of the variables had a significant effect for privacy risk

perception. The factor powerlessness showed a marginally significant positive effect in the owning condition. For the NOT owning a smart speaker group, perceived creepiness had a significant positive effect. Moreover, trust in smart speaker companies had a significant moderate negative effect in this condition, while only security self-efficacy was marginally significant.

Table 5

Regression models between privacy risk perception and the predictor variables for the subgroups owning and non-owning

	Owning a Smart Speaker *(n=35)*		NOT Owning a Smart Speaker *(n=64)*	
Variable	*B*	*p*	*B*	*p*
Perceived Enjoyableness	-0.05	.890	0.05	.682
Perceived usefulness	-0.03	.889	0.28	.060
Perceived creepiness	-0.09	.760	**0.66**	**<.001**
Trust in smart speaker companies	0.06	.867	**-0.42**	**.013**
Nothing to hide beliefs	0.30	. 376	0.01	.922
Resignation towards lack of privacy	-0.39	.342	-0.10	.542
Not likely the target	-0.10	.629	-0.12	.337
Powerlessness	0.43	.113	-0.06	.667
Privacy self-efficacy	0.16	.609	-0.36	.127
Security self-efficacy	0.006	.989	0.20	.213
Perceived regulatory protection	-0.03	.842	0.02	.807

Note. All significant effects are marked in bold.

Another regression table was calculated for the subgroups owning and not owning a smart speaker with protective as the dependent variable (see Table 6). Regarding people owning a smart speaker under the dependent variable protective behaviours, resignation towards a lack of privacy showed a significant negative effect on protective behaviours, while security self-efficacy had a significant positive effect for the outcome. For the participants who do NOT own a smart speaker, perceived creepiness had a significant moderate effect, while resignation towards a lack of privacy yielded a significant negative effect for protective behaviours. Moreover, perceived usefulness showed a significant negative effect. Finally, powerlessness was marginally significant for a positive effect on the outcome.

Table 6

Regression models between protective behaviours and the predictor variables for the subgroups owning and non-owning

	Owning a Smart Speaker (n=34)		*NOT Owning a Smart Speaker (n=64)*	
Variable	*B*	*p*	*B*	*p*
Perceived Enjoyableness	-0.19	.462	-0.25	.061
Perceived usefulness	0.22	.181	**-0.35**	**.041**
Perceived creepiness	0.02	.905	**0.42**	**<.001**
Trust in smart speaker companies	0.01	.955	0.17	.364
Nothing to hide beliefs	0.25	. 271	0.004	.983
Resignation towards lack of privacy	**-0.88**	**.018**	**-0.49**	**.014**
Not likely the target	0.01	.942	-0.23	.112
Powerlessness	0.27	.146	0.30	.083
Privacy self-efficacy	-0.20	.341	-0.12	.643
Security self-efficacy	**0.43**	**.023**	0.25	.172
Perceived regulatory protection	0.08	.519	0.08	.446

Note. All significant effects are marked in bold.

Correlational Analysis of the Divided Protective Behaviours

For the sub-variables protective physical behaviour and protective data behaviour a further correlational analysis with privacy risk perception and the predictor variables was conducted for the whole sample (see Table 7). The two types of behaviour are both positively correlated with privacy risk perception and are highly correlated with each other. Perceived

creepiness was the only factor that was significantly positive correlated with all the three outcome variables. Perceived usefulness, not likely the target and nothing to hide beliefs were among the only variables negatively predicting all the outcomes. No effect was shown by privacy self-efficacy, powerlessness, and perceived regulatory protection. Yet, privacy self-efficacy was among those, the only one which was close to being marginally significant for privacy risk perception and protective behaviour data. Moreover, perceived trust in companies and security self-efficacy were the only variables which significantly predicted one of the outcomes. Lastly, perceived enjoyableness and resignation towards a lack of privacy showed a significant negative effect on two of the three outcomes. However perceived enjoyableness showed no effect for Protective behaviour data, while resignation towards a lack of privacy did not show more than a marginally significant effect for privacy risk perception. The only major differences between the sub-behaviours were found in perceived enjoyableness and security self-efficacy. Specifically, only the "physical" protective behaviours had a significant effect on perceived enjoyableness, while only the "data" protective behaviours significantly affected security self-efficacy. However, the direction of the effects for the non-significant sub-behaviours was consistent with those that were significant. Additionally, those non-significant sub-behaviours in the other condition were actually marginally or nearly significant.

Table 7

Pearson correlation matrix between the dependent variables privacy risk perception, protective physical behaviour and protective data behaviour and the predictor variables

	Privacy Risk Perception		Protective Physical Behaviours		Protective Data Behaviours	
	r	p	r	p	r	p
Privacy Risk Perception	1	NA	**.41**	**<.001**	**.36**	**<.001**
Protective Physical Behaviour	**.41**	**<.001**	1	NA	**.73**	**<.001**
Protective Data Behaviour	**.36**	**<.001**	**.73**	**<.001**	1	NA
Perceived enjoyableness	**-.27**	**.006**	**-.26**	**.009**	-.12	.232
Perceived usefulness	**-.26**	**.007**	**-.23**	**.029**	**-.21**	**.031**
Perceived creepiness	**.55**	**.001**	**.58**	**<.001**	**.55**	**<.001**
Perceived trust in companies	**-.41**	**.001**	-.14	.169	-.12	.224
Nothing to hide beliefs	**-.29**	**.003**	**-.29**	**.003**	**-.33**	**<.001**
Resignation towards a lack of privacy	-.14	.141	**-.26**	**.008**	**-.37**	**<.001**
Not likely the target	**-.32**	**.001**	**-.34**	**<.001**	**-.34**	**<.001**
Privacy Self-Efficacy	-.15	.113	.06	.518	.13	.167
Security Self-Efficacy	-.09	.338	.16	.106	**.27**	**.007**
Powerlessness	.07	.442	-.07	.476	-.08	.397
Perceived Regulatory Protection	-.18	.0657	-.04	.652	-.10	.306

Note: Significant effects are marked in bold

Discussion

The present study aims to enrich the knowledge about privacy predictors in the use of smart speakers, specifically focusing on factors that influence whether someone takes measures to protect their privacy. It was designed to extend and re-test the model of the

preceding study by Hapke (2023). The identified factors can aid policymakers in understanding the complex process underlying the non-protective behaviour towards personal data in the use of smart speakers. Addressing the non-protective behaviour is crucial, as it has become increasingly common. (Emami-Naeini et al,. 2019).

In the current study, the following additional variables have been proposed as additions to the existing model by Hapke (2023): perceived creepiness, not likely the target, and perceived regulatory protection, resulting in a model with a total of 11 predictors. Perceived creepiness refers to the extent to which someone perceives the smart speaker as creepy or uncomfortable to use or be around. The second factor, not likely the target, considers how much a person feels that they are likely to be a target of cybercrime. Perceived regulatory protection is related to the perceived protection of their smart speaker by government laws and regulations. These variables were identified in qualitative studies in the domain of smart home devices (not solely smart speaker studies).

The results of the study indicated that perceived creepiness and not likely the target had an influence on the privacy risk perception and protective behaviours exhibited by a participant. However, the most consistent predictor for both privacy risk perception and protective behaviours was perceived creepiness, as it yielded support for the association even when controlling for the other factors. Not as consistent throughout the analyses was the factor not likely the target, which had a significant relationship with privacy risk perception and protective behaviour but not when controlling for the other predictors in the model. Perceived regulatory protection did not yield any significant relationships across all analyses but became marginally significant in the correlational analysis with privacy risk perception. Moreover, the factor analysis of the protective behaviours showed two subcategories of the variable: protective physical behaviours and protective data behaviours. The subcategories had roughly the same associations with the predictors. The results also showed that users and

non-users had did not have the same relationships with privacy risk perception and protective behaviours in terms of the predictors (especially perceived creepiness which only influenced non-owners). Moreover, the groups showed high differences in the mean levels of privacy risk perception that are, however, not statistically test. Finally, the original predictors identified by Hapke have proven to be predictive in this study as well. Every factor showed a significant effect on at least one dependent variable (privacy risk perception and protective action) in the full sample and/or in the owner or non-owners subsample, suggesting that it can contribute to developing interventions towards more protective action.

Evaluation of the Additional Factors

As mentioned previously, the first factor, perceived regulatory protection, became marginally significant in the correlational analysis. Given the relatively low sample size, it is appropriate to consider this association as supporting evidence for including the variable as a valuable contribution to the model. However, while it aligns with expectations (H1a), perceived regulatory protection did not significantly affect risk perception when controlling for other predictors. Additionally, it had no significant effect on protective behaviours

This negative association with privacy risk perception indicates that people who felt protected by government laws and regulations perceived less risk when using their smart speakers. The implications of this finding suggest that the factor could influence people's privacy risk perception and likelihood to engage in protective behaviours. This is consistent with the findings of Bombik and colleagues (2022), who also discovered a negative association between these factors. In theory, high levels of perceived regulatory protection could create a false sense of privacy, leading to negligent behaviour. Nevertheless, finding no direct significant effect on protective behaviours suggests that perceived regulatory protection may not make a person more careful in protecting their data. This leaves us with a debate on the implications of these findings that should be clarified in future studies.

The perception of being "not likely the target" had a significant negative association with both privacy risk perception (H2a) and protective behaviour (H2b). However, when controlling for other variables, this perception only yielded a marginally significant effect on protective behaviour and no significant effect on privacy risk perception. Considering the low sample size, accommodating marginally significant findings as acceptable support is reasonable, thus highlighting valuable implications.

A negative association between the perception of "not likely the target" and protective behaviour indicates that individuals who do not see themselves as interesting targets for cybercriminals are less likely to engage in protective actions. This bias in assessing the risk of cybercrime is dangerous because cybercrimes are also opportunistic and not necessarily targeted towards the rich and famous. Hence, also ordinary people should feel at risk of being targeted for their data. Interventions need to address this bias in thinking, as it actively decreases the likelihood of protective action. All things considered, the variable “not likely the target” should be further incorporated into models explaining non-protective behaviour and intervention designers should emphasize educating the public about the opportunistic side of cybercrime.

The last and most promising factor identified in the new model was perceived creepiness. Perceived creepiness was significantly associated with privacy risk perception and protective behaviour with and without controlling for the other predictors. This confirms the notion found in the study by Fruchter and Liccardi (2018), who looked at online ratings of smart speaker’s purchasers, that suspiciousness or creepy feelings towards the smart speaker are a common theme in many reviews. Hence, this study underlines that creepiness or some sort of negative feeling towards the smart speaker can be valuable predictor for privacy risk perception and protective behaviours. Nevertheless, to put these findings into perspective, the comparison between the groups should still be considered to some extent. Here, this paints a

different picture, where perceived creepiness seems to only affect people who do not own a smart speaker. This is also somewhat in line with what the study by Mou and Meng (2023) found. They looked at the non-adopters of smart speakers and found perceived creepiness to be a great predictor for non-adoption. This could suggest, given this study's unequal group size, that this factor may not be relevant for people who own a smart speaker. This is also partly reflected in the mean scores for the two groups, where owners had a mean value approximately substantially than non-owners. Intuitively, it seems logical that people who bought a smart speaker or have a smart speaker in their home for some time lose the feelings of creepiness towards the device due to habituation. The same concept applies to other technology as well, for example, if someone first drives with a self-driving car it may be very strange but if this person keeps on taking rides with it, eventually they will be used to it. The findings, as mentioned already, are to be taken with caution since the sample size is not sufficient for an accurate between group comparison. Still, this finding leaves room for debate over whether this factor is truly helpful for developing interventions, as it may be the case that perceived creepiness deviates in its relevance between groups.

Applying creepiness for interventions is a delicate task. Designers would have to reflect on the appropriateness of using creepiness in order to increase protective behaviours. It could be argued that for users, who seem to score lower on perceived creepiness, increasing creepiness could create fear around the smart speaker which could result in the abandonment of the device. Regarding non-users, who seem to score higher on the variable, increasing perceived creepiness with interventions should according to the findings by Mou and Meng (2023), result in more non-adoption. Both consequences are not much in line with the aim of the study which is to help users to be more privacy responsible. Hence, it should be considered what an optimal amount of creepiness is, that would still allow users to enjoy the device while not making irresponsible privacy decisions. If established, this information

could help intervention designers to develop educational campaigns that address perceived creepiness for users and non-users by providing clear and accurate information about smart speakers, thereby creating a reasonable level of creepiness to reduce unfounded fears and promoting informed protective behaviours.

All in all, this study has provided supporting evidence for perceived regulatory protection, not likely the target and perceived creepiness to be retained for future studies.

Evaluation of the Original Variables

The results of the control variables suggest that every factor from the original study by Hapke (2023) had also an effect on privacy risk perception and protective behaviour in the present study. Moreover, when a predictor was significant in both studies, the direction of the effect was always the same. Yet when looking at the results of correlation analysis in the two studies, one thing becomes apparent; the former study by Hapke (2023) found in total more significant effects on privacy risk perception and protective behaviours than the present one. Furthermore, for the significant predictors the correlation coefficients were almost all higher in the previous study (on average +/ - .10 r). This discrepancy could possibly be explained by the fact that Hapke's earlier study used a single "scenario" where all participants answered questions based on a hypothetically gifted smart speaker, which may have resulted in more uniform responses and higher effect sizes. In contrast, the present study employed a two-way design with tailored questions for both owners and non-owners of smart speakers, potentially introducing greater variability into the data. Additionally, this might have been exaggerated by the addition of more factors, as more factors create more covariance which can lead to lower effect sizes.

This difference in the correlation coefficient was especially high for perceived enjoyableness, with correlations of around twice the size with both privacy risk perception and protective behaviours compared to recent results. This disparity is remarkable since

perceived enjoyableness, was the most reliable predictor in the former study and should therefore also have played a bigger role in the present study. Hapke's results showed that perceived enjoyableness was significant for all analysis except for the regression analysis on the divided group, while here, it did not seem to significantly impact people who already own a smart speaker for neither outcome variable. In the present study the factor did not yield any significant effects for any regression model. Again, this is quite remarkable since the factor served as the strongest predictor for protective behaviour and as the second strongest predictor for privacy risk perception in the regression models of the former study. These differences in effect are difficult to explain but in addition to the explanations in the previous paragraph (study design and covariance due to more factors), it seems important to consider the sample size and the origin of the sample. The study by Hapke (2023) offered a much larger sample size with more than twice as many participants, with several participants originating from the same IT provider company. The larger sample size could have helped to detect even smaller effects in the regressions analyses, while the difference in origin of the two samples might have resulted in different ideas regarding enjoyableness of a smart speaker. Intuitively, a sample with more participants working for an IT company should be more aware and self-efficacious of potential privacy problems with smart speakers than a sample with mostly students (72% indicated to be students). A sample with mostly students could also be considered as more reckless in sacrificing data for the sake of enjoyment. However, this is not reflected here and should be investigated in future studies as the present study could not make sense of these results. This could perhaps be done by comparing different professions in their mean values for smart speaker's enjoyableness, e.g. by comparing student participants with participants working in IT companies. This knowledge could then be used to target specific subpopulations for example by creating interventions that are conducted at university campuses or in companies.

One noteworthy association between factors that aligned with the previous study by Hapke (2023) was between Privacy risk perception and Protective Behaviours. In both studies, the correlation size and direction were approximately the same, confirming previous research that claims that people who perceive more privacy risks, tend to also engage in more protective behaviours (Boerman et al., 2021). Additionally, this also suggests that the revision of the protective behaviours scale had no major influence on the relationship between the outcome variables as they resulted in similar findings.

Furthermore, after the factor analysis of the protective behaviours in the study by Hapke (2023), no extra subfactor was identified. However, in the current study, protective behaviours were separated into protective data and physical behaviours. The only difference between the former measure and the newer two factor measure was a slight differentiation in the correlation sizes. Nonetheless, there were no changes in terms of direction of effect, indicating that both types of behaviour can be influenced by privacy risk perception. Therefore, future studies should consider the present studies measure for protective behaviours as a good alternative.

Ownership

Testing the significance of the differences between owners and non-owners was difficult due to the low sample size, however, some of the evidence suggests that differentiating between these groups is central. One notable fact is the difference in mean scores of privacy risk perception between owners and non-owners. The results showed that, on average, non-owners perceived more than twice the privacy risk compared to owners. This contrast in mean scores indicates that owners exhibit meaningfully fewer concerns about using their devices than non-owners. However, it is important to note that this finding could also be due to inherent differences between the groups (or a combination of both).

Another supporting point is the fact that the predictors for owners and non-owners vary in terms of strength and significance. For instance, the strongest predictor for owners was resignation towards a lack of privacy, which suggests they are less concerned about privacy and more resigned to potential issues. In contrast, this was not the strongest predictor for non-owners, indicating fundamental differences in attitudes. Lau's (2018) study supports this, finding that users accepted smart speakers out of resignation towards new technology. Moreover, as already discussed, perceived creepiness did not yield any effects close to significance in the regression with privacy risk perception and protective behaviours among owners. Consequently, the means for non-owners were substantially higher than for owners, further indicating the groups distinctiveness.

Additionally, only 16 out of 65 non-owners indicated they would install a gifted smart speaker, demonstrating a higher percentage of non-adopters. This implies that non-owners are generally not very interested in becoming owners, suggesting it might be more consistent to compare only those non-owners who would consider owning a smart speaker with current owners for more reliable results.

In summary, the differences between ownership groups should be addressed in future studies and interventions. One claim that this study wants to make is that owners should be prioritized in research, as they are more urgently at risk for data breaches simply because they already possess the device. Another point is that it could add strength to a study if the comparison between owners and non-owners were limited to those who would consider adopting a smart speaker. Nevertheless, results from non-owners, regardless of intention for adoption, are also valuable for informing prevention practices related to the responsible use of smart speakers and preparing potential owners for privacy pitfalls.

Strength Comparison among Predictors

In the present study, some predictors for privacy risk perception and protective behaviour were stronger than others. For privacy risk perception, perceived trust in companies and perceived creepiness were the only significant predictors in both regression and correlational analyses. However, these predictors were not consistently significant for both groups. Only non-owners' risk perception seemed to be influenced by perceived trust in companies and perceived creepiness. For owners, none of the predictors had a significant effect on privacy risk perception when controlling for other predictors, suggesting that interventions targeting trust in smart speaker companies and perceived creepiness would be less useful for them. This conclusion is similar to Hapke's (2023), where owners and non-owners showed differences in significant predictors.

Additionally, the study shows that privacy risk perception and protective behaviours were not predicted by the same variables. This indicates that not every predictor of privacy risk perception is equally valuable for predicting protective behaviours. Practically, this means that a factor highly predictive of privacy risk perception but not of protective behaviour has limited value, as enhancing privacy ultimately requires promoting protective behaviours. Notably, only perceived creepiness showed a significant effect on protective behaviour when controlling for the other variables, reinforcing its importance in the model, though its practical implications are less clear when also looking at ownership status.

When examining the strongest predictors for protective behaviours in both correlational and regression analyses, four variables stand out: perceived creepiness, resignation towards a lack of privacy, not likely the target, and security self-efficacy (see Figure 1). These factors can be primary targets for interventions since they consistently predicted protective behaviours, even when controlling for other predictors. Importantly, they do not need to be associated with privacy risk perception to impact practice, making them crucial components of the model.

The most remarkable negative predictor was resignation towards a lack of privacy, which had the strongest negative impact on protective behaviours for both groups. This contrasts with Hapke (2023), who found this effect only for non-owners. Furthermore, not likely the target was somewhat weaker in strength as it was only marginally significant and seemed to apply mostly for non-owners. These findings highlight the importance of addressing people's resignation towards privacy protection and their biases in estimating their perceived relevance as a target. However, these factors could benefit from more in-depth research in the future.

On the positive side, security self-efficacy and perceived creepiness were positively related to protective behaviours but affected owners and non-owners differently. Perceived creepiness was more important for non-owners, whereas security self-efficacy was significant only among owners. This underscores the need for interventions tailored to the ownership status of the target groups; for example, owners might benefit more from enhancing their security self-efficacy.

Limitations and Recommendations for future Studies

In the process of this study a few limitations became apparent along the way. The first limitation relates to a problem with the length of the survey. The study incorporated about 18 scales in total, with some factors consisting of up to 18 questions (In the case of protective behaviours). The estimated time was set to be around 15 to 20 minutes and was established by conducting three test runs with different people. When collecting the first responses, it became apparent that it took people about 20+ minutes to complete, with some of which who took 45 minutes to complete the survey. This is problematic since according to research (Kost & Rosa, 2018); participants are less likely to complete and reliably respond to longer surveys. In part, this could be due to the fact that most of the participants did not take the survey in the first language and since many participants originated from Germany, a second survey in

German could have increased the reliability of the study. Conclusively, for a future study, a shorter survey is to be recommended with a second language option to increase the studies strength.

Another limitation was already mentioned briefly in the earlier parts. The studies sample size was, according to the G*Power analysis, not sufficient for separately analysing the effects in both groups and could thus, not directly be compared to the results by Hapke (2023). This shortage of participants diminishes an important part of the study which is to analyse the underlying factors of non-protection in people who own a smart speaker. This is likely different from what can be studied with a sample consisting mostly out of non-owners. Here, protection in non-owners may be more likely to result in non-adoption than non-protection. In fact, after data cleaning, in the non-owning group only 34 participants were left which was only about one third of the required sample size for finding medium effect sizes as calculated by G*Power. By having a larger sample, the model could have resulted in more significant effects in the regression analysis and increased power.

Moreover, it is likely that some participants in the non-owning group had no knowledge about the functions of a smart speaker and therefore could not appropriately answer all the questions. This lack of knowledge could have led to increased chances of random responses, particularly in measures like the scale for protective behaviours. For example, participants might not have understood questions such as the necessity of installing a smart speaker app to delete sensitive information. Additionally, the design decision to use forced answers for all questions exacerbates this issue, creating a problematic mixture for the validity of the results. To address these issues, future studies could include preliminary questions to assess participants' familiarity with smart speaker functions and consider avoiding forced answers to reduce the risk of random responses.

Nevertheless, some strengths have also been identified. The study retested and supported the model by Hapke (2023) and could thereby gather support for using the model in future interventions/studies. Moreover, the present work was also able to extend the model with additional variables for a possibly more complete approach. Furthermore, another strength is that it also established a good selection of behaviours for the protective behaviour outcome scale. This revised version of the protective behaviours, now, seems to resemble a more realistic selection of useful behaviours and distinguishes between two types of behaviours and can be seen as strength of the study.

Conclusion

The use of modern technology in today's time is almost always tied to some trade-off between one's personal data on one side and the pleasure and convenience on the other; the smart speaker is no different in that. The downsides of the trade could be diminished by employing appropriate protective behaviours, yet only a small amount of people are doing so. This research tried to shed light on the factors contributing to or undermining someone's privacy risk perception and protective behaviours by enhancing and retesting the previously identified model by Hapke (2023). Among the three added factors of the present study, perceived creepiness and not likely showed the most promising associations with privacy risk perception and protective behaviour, while perceived regulatory protection could be considered the weakest factor. Nevertheless, there is support for incorporating all the added factors to the model for future endeavours. Furthermore, the original variables by Hapke have all proven to be significant predictors at some point of this study's analysis, supporting the value of the model for explaining why or why not people take protective action. The strongest predictors in the entire model can be considered perceived creepiness, resignation towards a lack of privacy, not likely the target, and security self-efficacy. By designing interventions that target these factors, protective action around smart speakers are ought to increase in the

future. Additionally, the present study put great emphasis on revising the protective behaviours for a more sound and coherent measurement. The revision resulted in two subcategories for (physical and data) protective behaviours that did not yield important differences for the predictor variables. Finally, the study found notable differences in terms of owners and non-owners of smart speakers, suggesting a clearer distinction in future studies.

The present study underscores the need for increased awareness of smart speaker privacy. By understanding the factors identified in this study, individuals are not only empowered to take more protective actions, but they are also better equipped to make decisions that prioritize their privacy when using smart speakers.

References

Alam, I., Khusro, S., & Naeem, M. (2017). A review of smart TV: Past, present, and future. *ICOSST 2017 - 2017 International Conference on Open Source Systems and Technologies, Proceedings*, *2018-January*, 35–41. https://doi.org/10.1109/ICOSST.2017.8279002

Bermejo Fernandez, C., Nurmi, P., & Hui, P. (2021). Seeing is Believing?: Effects of Visualization on Smart Device Privacy Perceptions. *MM 2021 - Proceedings of the 29th ACM International Conference on Multimedia*, 4183–4192. https://doi.org/10.1145/3474085.3475552

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bombik, P., Wenzel, T., Grossklags, J., & Patil, S. (2022). A Multi-Region Investigation of the Perceptions and Use of Smart Home Devices. *Proceedings on Privacy Enhancing Technologies*, *2022*(3), 6–32. https://doi.org/10.56553/POPETS-2022-0060

Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., & Hasan, M. (2023). Smart Home System: A Comprehensive Review. *Journal of Electrical and Computer Engineering*, *2023*. https://doi.org/10.1155/2023/7616683

Chesnokova, L. V. (2021). “A Room of One’s Own”: The local aspect of privacy. *Izvestiya of Saratov University. New Series. Series: Philosophy. Psychology. Pedagogy*, *21*(1), 57–61. https://doi.org/10.18500/1819-7671-2021-21-1-57-61

Chhetri, C., & Motti, V. G. (2019). Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11420 LNCS*, 91–101. https://doi.org/10.1007/978-3-030-15742-5_8/TABLES/4

Chu, L. (2019). *Why would I adopt a smart speaker? : Consumers' intention to adopt smart speakers in smart home environment* [Master's Thesis, University of Twente]. https://essay.utwente.nl/77187/

Di Gangi, P. M., Wech, B. A., Hamrick, J. D., Worrell, J. L., Goh, S. H., & Gangi, D. (2023). Risk perceptions about personal Internet-of-Things: Research directions from a multi-panel Delphi study. *Journal of Cybersecurity Education, Research and Practice*, *2022*(2), 5. https://doi.org/10.32727/8.2023.4

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*, *12*(2019). https://doi.org/10.1145/3290605.3300764

Fang, T., & Fu, X. (2020). Development Status and Marketing Strategy of Smart Speakers. *Advances in Intelligent Systems and Computing*, *1209 AISC*, 553–562. https://doi.org/10.1007/978-3-030-50791-6_71/FIGURES/5

Fruchter, N., & Liccardi, I. (2018). Consumer attitudes towards privacy and security in home assistants. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3170427.3188448

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

Haney, J. M., Acar, Y., & Furman, S. M. (2021). *It's the Company, the Government, You and I: User Perceptions of Responsibility for Smart Home Privacy and Security*. https://www.nist.gov/publications/its-company-government-you-and-i-user-perceptions-responsibility-smart-home-privacy-and

Haney, J. M., Furman, S. M., & Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. *Lecture Notes in*

Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), *12210 LNCS*, 393–411. https://doi.org/10.1007/978-3-030-50309-3_26/FIGURES/2

Hapke, J. (2023). *Examining Factors that Undermine Privacy Risk Perception and Protective Behaviour Concerning Smart Speakers*. [Bachelor's Thesis, University of Twente]. https://essay.utwente.nl/77187/ https://essay.utwente.nl/95412/

Ho, C. C., MacDorman, K. F., & Pramono, Z. A. D. D. (2008). Human emotion and the uncanny valley: A GLM, MDS, and Isomap analysis of robot video ratings. *HRI 2008 - Proceedings of the 3rd ACM/IEEE International Conference on Human-Robot Interaction: Living with Robots*, 169–176. https://doi.org/10.1145/1349822.1349845

Huijts, N. M. A., Haans, A., Budimir, S., Fontaine, J. R. J., Loukas, G., Bezemskij, A., Oostveen, A., Filippoupolitis, A., Ras, I., IJsselsteijn, W. A., & Roesch, E. B. (2023). User experiences with simulated cyber-physical attacks on smart home IoT. *Personal and Ubiquitous Computing*, *27*(6), 2243–2266. https://doi.org/10.1007/S00779-023-01774-5/TABLES/3

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2016). *'My Data Just Goes Everywhere:' User Mental Models of the Internet and Implications for Privacy and Security*.

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

Kost, R. G., & Rosa, J. C. da. (2018). Impact of survey length and compensation on validity, reliability, and sample characteristics for Ultrashort-, Short-, and Long-Research Participant Perception Surveys. *Journal of Clinical and Translational Science*, *2*(1), 31. https://doi.org/10.1017/CTS.2018.18

Kowalczuk, P. (2018). Consumer acceptance of smart speakers: a mixed methods approach. *Journal of Research in Interactive Marketing*, *12*(4), 418–431. https://doi.org/10.1108/JRIM-01-2018-0022

Lau, J., Zimmerman, B., & Schaub, F. (2018). 'Alexa, Stop Recording': Mismatches between Smart Speaker Privacy Controls and User Needs. In *USENIX*. 14th Symposium on Usable Privacy and Security. https://www.usenix.org/sites/default/files/soups2018posters-lau.pdf

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media and Society*, *22*(7), 1168–1187. https://doi.org/10.1177/1461444820912544

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *37*(3), 147–162. https://doi.org/10.1080/01972243.2021.1897914

Powell, J. (2023). *Smart speaker trends*. https://www.kantarmedia.com/news-and-resources/smart-speaker-trends

Selinger, E., & Durant, D. (2022). Amazon's Ring: Surveillance as a Slippery Slope Service. *Science as Culture*, *31*(1), 92–106. https://doi.org/10.1080/09505431.2021.1983797

Shaikh, E., Mohiuddin, I., & Manzoor, A. (2019). Internet of Things (IoT): Security and Privacy Threats. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*. https://doi.org/10.1109/CAIS.2019.8769539

Voit, A., Niess, J., Eckerth, C., Ernst, M., Weingärtner, H., & WoÅ°niak, P. W. (2020). It's not a romantic relationship': Stories of Adoption and Abandonment of Smart Speakers at Home. *ACM International Conference Proceeding Series*, 71–82. https://doi.org/10.1145/3428361.3428469

Wozniak, P. W., Karolus, J., Lang, F., Eckerth, C., Schoning, J., Rogers, Y., & Niess, J. (2021). Creepy technology: What is it and how do you measure it? *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445299

Appendix A (Questionnaire)

Introduction

Informed Consent

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

Researchers:
Carl Moritz Pottkamp (B.Sc. student), Antonia Döring (B.Sc. student), 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:

For further information about this study, you may contact:

Carl Pottkamp: c.m.pottkamp@student.utwente.nl

Antonia Döring: a.doring@student.utwente.nl

Jonah Shepherd: j.j.shepherd@student.utwente.nl

Dr. Nicole Huijts: n.m.a.huijts@utwente.nl

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.

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.

- ○ I agree and consent to participating in this study and confirm that I am over 18 years old
- ○ No, I do not agree to participating in this study

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.

- ◯ I agree and consent to participating in this study and confirm that I am over 18 years old
- ◯ No, I do not agree to participating in this study

Demographics

What is your age?

Which country are you from?

- ◯ The Netherlands
- ◯ Germany
- ◯ Other, please indicate:

What is your gender?

- ◯ Male
- ◯ Female
- ◯ Non-binary / non-conforming
- ◯ Prefer not to say

What is your highest completed level of education?

- ◯ Primary school
- ◯ Secondary school
- ◯ Professional education
- ◯ Bachelor
- ◯ Master
- ◯ PhD

Are you a student?

- ◯ No
- ◯ Yes

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.

He wants the state to be strong so it can defend its citizens.

- ◯ Strongly disagree
- ◯ disagree
- ◯ somewhat disagree
- ◯ somewhat agree
- ◯ agree
- ◯ strongly agree

Following his family's customs or the customs of a religion is important to him.

- ◯ Strongly disagree
- ◯ disagree
- ◯ somewhat disagree
- ◯ somewhat agree
- ◯ agree
- ◯ strongly agree

It is important to him to follow rules even when no one is watching.

- ◯ Strongly disagree
- ◯ disagree
- ◯ somewhat disagree

- ○ somewhat agree
- ○ agree
- ○ strongly agree

He thinks it is important never to be annoying to anyone.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to him to be humble.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

He goes out of his way to be a dependable and trustworthy friend.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

Caring for the well-being of people he is close to is important to him.

- ○ Strongly disagree
- ○ disagree

- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

He thinks it is important that every person in the world have equal opportunities in life.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to him to work against threats to the world of nature.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to him to listen to people who are different from him.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to him to have full control over who accesses personal information about him.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

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.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to him to protect his privacy.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

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.

She wants the state to be strong so it can defend its citizens.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

Following her family's customs or the customs of a religion is important to her.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to follow rules even when no one is watching.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

She thinks it is important never to be annoying to anyone.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to be humble.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

She goes out of her way to be a dependable and trustworthy friend.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

Caring for the well-being of people she is close to is important to her.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

She thinks it is important that every person in the world have equal opportunities in life.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree

- ○ strongly agree

It is important to her to work against threats to the world of nature.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to listen to people who are different from her.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to have full control over who accesses personal information about her.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to not share personal information (for example about personal preferences, one's health, or political and religious beliefs) with unknown others.

- ○ Strongly disagree
- ○ disagree

- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

It is important to her to protect her privacy.

- ○ Strongly disagree
- ○ disagree
- ○ somewhat disagree
- ○ somewhat agree
- ○ agree
- ○ strongly agree

Control Questions

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.

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)?

- ○ Yes
- ○ No

Which statement best describes your situation regarding the smart speaker?

- ○ I am the main owner/user
- ○ I use it, but I'm 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
- ◯ more than 2 years

install and use (gifted)

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 don't know

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

- ◯ Yes
- ◯ No
- ◯ I don't know

Protective behaviour (GIFTED)

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.

I will turn off the smart speaker when I am not using it

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will unplug the smart speaker when I am not using it

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will unplug the smart speaker when I am having serious/private conversations

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will turn off the smart speaker when I am having serious/private conversations

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will mute the smart speakers microphone when I am not using it

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will review the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will review which applications/services have access to my smart speaker

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will restrict the amount of data that the device is allowed to collect through the smart speakers settings

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will delete my smart speaker recordings

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

In the app I will delete sensitive information that the smart speaker stored about me.

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will speak very quietly around the smart speaker, in case I don't want to be recorded

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will moderate my language around the smart speaker so that it doesn't record private matters, even if accidentally

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will avoid sensitive/private conversations around the smart speaker

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

If I have a visitor, I will inform them that I have a smart speaker

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

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

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will set a new difficult password for my smart speaker that I don't use for other applications

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

I will not write down the password on a piece of paper or share it otherwise with house members or visitors

- ○ Extremely unlikely
- ○ Somewhat unlikely
- ○ Neither likely nor unlikely
- ○ Somewhat likely
- ○ Extremely likely

Value measures (gifted)

Please indicate to what extent you agree with the following statements:

I think using a smart speaker that I received as a gift would be enjoyable.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I think I would have fun using a smart speaker that I received as a gift.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

It would not be interesting to use a smart speaker that I received as a gift.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

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

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Using a smart speaker that I received as a gift would improve my productivity in my daily life

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Using a smart speaker that I received as a gift would make my life easier

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Using a smart speaker that I received as a gift would enable me to accomplish my tasks more quickly.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Using a smart speaker that I received as a gift would enhance my effectiveness in daily tasks.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I would find it useful to use a smart speaker that I received as a gift at home.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

This smart home assistant, that I received as a gift, would make me feel uncomfortable.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

This smart home assistant, that I received as a gift, would give me an eerie feeling.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

This smart home assistant, that I received as a gift, would creep me out.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I would feel uneasy towards this smart home assistant, that I received as a gift.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Perceived effort needed to adjust privacy settings

Please indicate the extent of effort required for the following statements:

How much effort would it take you to adjust your privacy settings on your smart speaker?

- ◯ it takes very little effort
- ◯ it takes a little effort
- ◯ it takes some effort
- ◯ it takes quite a bit effort
- ◯ it takes a lot of effort

How much effort would it take you to engage in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?

- ◯ it takes very little effort
- ◯ it takes a little effort

- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

How much effort would it take you to continuously keep engaging in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?

- ○ it takes very little effort
- ○ it takes a little effort
- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

How much effort would it take you to find information on how to better protect your privacy from your smart speaker?

- ○ it takes very little effort
- ○ it takes a little effort
- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

How much effort would it take you to seek help or guidance from others to protect your privacy on your smart speaker?

- ○ it takes very little effort
- ○ it takes a little effort
- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

Privacy concern

Please answer the following questions.

To what extent do you think your privacy is at risk now that you installed a smart speaker in your house?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

How large do you think the risk is that your privacy is invaded now that you have this smart speaker installed?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

value measures owning

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

Please indicate to what extent you agree with the following statements:

Using a smart speaker is enjoyable.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I have fun using a smart speaker.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

It is not interesting to use a smart speaker.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Using a smart speaker gives me pleasure.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Using a smart speaker improves my productivity in my daily life

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Using a smart speaker makes my life easier

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Using a smart speaker enables me to accomplish my tasks more quickly.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Using a smart speaker enhances my effectiveness in daily tasks.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I find it useful to use a smart speaker at home.

- ○ Strongly disagree

- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

The smart speaker makes me feel uncomfortable.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

The smart speaker gives me an eerie feeling.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

This smart speaker creeps me out.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I feel uneasy towards my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree

- ◯ Strongly agree

privacy concern owning

Please answer the following questions.

To what extent do you think your privacy is at risk with a smart speaker in your house?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

How large do you think the risk is that your privacy is invaded by your smart speaker?

- ◯ None at all
- ◯ A little
- ◯ A moderate amount
- ◯ A lot
- ◯ A great deal

Perceived effort needed to adjust privacy settings owning

Please indicate the extent of effort required for the following statements:

How much effort does it take you to adjust your privacy settings on your smart speaker?

- ◯ it takes very little effort
- ◯ it takes a little effort
- ◯ it takes some effort
- ◯ it takes quite a bit effort
- ◯ it takes a lot of effort

How much effort does it take you to engage in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?

- ◯ it takes very little effort
- ◯ it takes a little effort
- ◯ it takes some effort
- ◯ it takes quite a bit effort
- ◯ it takes a lot of effort

How much effort does it take you to continuously keep engaging in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?

- ◯ it takes very little effort
- ◯ it takes a little effort
- ◯ it takes some effort
- ◯ it takes quite a bit effort
- ◯ it takes a lot of effort

How much effort does it take you to find information on how to better protect your privacy from your smart speaker?

- ◯ it takes very little effort

- ○ it takes a little effort
- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

How much effort does it take you to seek help or guidance from others to protect your privacy on your smart speaker?

- ○ it takes very little effort
- ○ it takes a little effort
- ○ it takes some effort
- ○ it takes quite a bit effort
- ○ it takes a lot of effort

protective behaviour (owning)

How often in the last 3 month did you engage in the following behaviours?

I turned off the smart speaker when I was not using it

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I unplugged the smart speaker when I was not using it

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I unplugged the smart speaker when I was having serious/private conversations

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I turned off the smart speaker when I was having serious/private conversations

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I muted the smart speakers microphone when I was not using it

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I reviewed which applications/services have access to my smart speaker

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I restricted the amount of data that the device is allowed to collect through the smart speakers settings

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I deleted my smart speaker recordings

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

In the app I deleted sensitive information that the smart speaker stored about me.

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I spoke very quietly around the smart speaker, in case I did not want to be recorded

- ○ never
- ○ almost never

- ○ sometimes
- ○ often
- ○ always

I moderated my language around the smart speaker so that it didn't record private matters, even if accidentally

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

I avoided sensitive/private conversations around the smart speaker

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

When I had a visitor, I informed them that I have a smart speaker

- ○ never
- ○ almost never
- ○ sometimes
- ○ often
- ○ always

When I had a visitor, I offered to switch the smart speaker off

- ○ never
- ○ almost never
- ○ sometimes
- ○ often

- ○ always

When I installed the smart speaker, ...

... I placed the smart speaker so that it was not positioned in areas where I typically engaged in conversations involving sensitive or private information

- ○ Yes
- ○ No

... I set a new difficult password for my smart speaker that I don't use for other applications

- ○ Yes
- ○ No

... I did not write down the smart speakers password on a piece of paper or shared it otherwise with house members or visitors

- ○ Yes
- ○ No

... I changed the password again after using the smart speaker for some time

- ○ Yes
- ○ No

Beliefs 1

Please indicate to what extent you agree with the following statements:

Smart speaker companies are trustworthy in handling the data the smart speaker collects about me.

- ○ Strongly disagree

- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I trust that smart speaker companies keep my best interests in mind when dealing with the information collected about me.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Smart speaker companies are in general predictable and consistent regarding the usage of the information provided by me.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Smart speaker companies are careful with sharing my personal data with third parties.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Smart speaker companies are always honest with customers when it comes to using information that they provide.

- ◯ Strongly disagree

- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Smart speaker companies intend to protect my data well because they want to keep their market shares.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

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

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Please select 'strongly agree' to show you are paying attention to this question

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I have nothing to hide, so no one would find anything interesting about me in my data.

- ◯ Strongly disagree
- ◯ Somewhat disagree

- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I do not admit to anything that would incriminate me in front of my smart speaker.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I have nothing to hide because I do not do anything criminal in my house.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

I am not doing much in my house that I do not want other people to know about.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

My life is very boring, so the data collected about me is of little interest to others.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

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.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

In order to adopt new technologies, I have to give up my privacy.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Protecting my privacy is so inconvenient that I do not care anymore who has my data.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Consumers have lost all control over how personal information is collected and used by companies.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

It does not matter what I do regarding the settings of the smart speaker, companies collect loads of information about me anyway.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am powerless when it comes to protecting my data from the manufacturer of the smart device.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I feel that, because I am not rich or famous, my data is not worth stealing.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that because I am just a normal person, hackers are not interested in accessing my personal data.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that hackers are more likely to target smart speakers of high-profile individuals or organizations rather than individuals like me.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Beliefs 2

Please indicate to what extent you agree with the following statements:

I believe that even if I try to protect my data, I can't prevent others from accessing them.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that in the end, I can't prevent others from accessing my data.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that I don't have the power to protect my personal data effectively from all the possible dangers on the Internet.

- ◯ Strongly disagree
- ◯ Somewhat disagree

- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that it would be naive to think that I can protect my personal data online reliably.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I believe that if someone is determined to access my personal data, there is nothing I can do to stop them.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

The idea that I would be under surveillance by a smart speaker frightens me.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I find it objectionable when I do not know what will be recorded by smart speakers.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree

- ◯ Somewhat agree
- ◯ Strongly agree

It bothers me that others see my activities via the smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

It disturbs me that the smart speaker permanently monitors me.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I worry that my smart device is recording conversations when I talk to my friends.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am concerned that my smart device is capturing information even though I am not actively using it.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I think that people whose opinions I value, would support me using privacy protective behaviour with a smart speaker

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

My family members and friends would recommend me to adjust my smart speaker settings to enhance my privacy

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

People in my immediate surrounding think that privacy protecting behaviour around their smart speaker is important

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

I think people in my surrounding find it important to comply with the privacy recommendations provided by experts when using smart speakers

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree

- ○ strongly agree

People that are important to me generally take privacy protective actions around smart devices

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

My friends and family generally put effort in limiting data-collection from smart devices

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

People close to me generally make sure that their smart devices have restricted privacy settings

- ○ strongly disagree
- ○ somewhat disagree
- ○ neither agree nor disagree
- ○ somewhat agree
- ○ strongly agree

Regulatory Protection

Please indicate to what extent you agree with the following statements.

I feel that current laws and regulations are adequate to protect Smart Speaker data from:

Misuse of data by the smart speaker company itself (e.g. Google or Amazon).

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Unwanted access by third party application developers.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Unwanted access by hackers.

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Unwanted access by government agencies

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Self-efficacy

Please indicate to what extent you agree with the following statements:

I feel confident in my ability to protect myself by using the privacy settings of my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I feel in control over the information I provide on my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Privacy settings allow me to have full control over the information I provide to my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I feel in control of who can view my information collected through my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am able to protect my personal information from external threats.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am able to protect the data on my smart speaker from being damaged or altered by external parties.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am capable of responding well to malicious software such as viruses.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Please select 'strongly agree' to show you are paying attention to this question

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am able to detect that my smart speaker is hacked.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

I am able to erase malicious software from my smart speaker.

- ◯ Strongly disagree
- ◯ Somewhat disagree
- ◯ Neither agree nor disagree
- ◯ Somewhat agree
- ◯ Strongly agree

Experience with CA

Have you ever heard about someone in your social environment (e.g. acquaintances, friends or family) being hacked, or did you personally experience some kind of hack?

- ◯ Yes, I have heard about someone being hacked
- ◯ Yes, I have personally experienced being hacked
- ◯ Yes, I both have heard about someone being hacked and I have personally experienced being hacked
- ◯ No, I have never heard about someone being hacked nor personally experienced being hacked

Debriefing

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.

For further information about this study, you may contact **Carl Pottkamp: c.m.pottkamp@student.utwente.nl Antonia Döring: a.doring@student.utwente.nl Jonah Shepherd: j.j.shepherd@student.utwente.nl**, or Dr. Nicole Huijts: **n.m.a.huijts@utwente.nl**

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

Hypotheses by Hapke (2023)

H1: Privacy risk perception has a positive effect on protective behaviour.

H2a: Perceived enjoyableness has a negative effect on privacy risk perception.

H2b: Perceived enjoyableness has a negative effect on protective behaviour.

H3a: Perceived Usefulness has a negative effect on privacy risk perception.

H3b: Perceived Usefulness has a negative effect on protective behaviour.

H4a: Trust in smart speaker companies has a negative effect on privacy risk perception.

H4b: Trust in smart speaker companies has a negative effect on protective behaviour.

H5a: Nothing to hide beliefs has a negative effect on privacy risk perception.

H5b: Nothing to hide beliefs has a negative effect on protective behaviour.

H6a: Resignation towards lack of privacy has a negative effect on privacy risk perception.

H6b: Resignation towards lack of privacy has a negative effect on protective behaviour.

H7a: Privacy self-efficacy has a negative effect on privacy risk perception.

H7b: Privacy self-efficacy has a positive effect on protective behaviour.

H8a: Powerlessness has a negative effect on privacy risk perception. *

H8b: Powerlessness has a negative effect on protective behaviours. *

H9a: Security self-efficacy has a negative effect on privacy risk perception. *

H9b: Security self-efficacy has a positive effect on protective behaviour. *

**the marked hypotheses are not in Hapke's first Hypotheses however have been tested in her analysis and are therefore also included.*

Appendix C

Factor loadings of the additional and edited factors

Construct	***Items***	***Factor Loadings***
Powerlessness	I believe that even if I try to protect my data, I cant prevent others from accessing them.	*.768*
	I believe that in the end, I cant prevent others from accessing my data.	*.754*
	I believe that I don't have the power to protect my personal data effectively from all the possible dangers on the internet.	*.680*
	I believe that it would be naïve to think that I can protect my personal data online reliably.	*.599*
	I believe that if someone is determined to access my personal data, there is nothing I can do to stop them.	*.671*
Perceived Regulatory Protection	I feel that (…) from misuse of data by the smart speaker company itself (e.g. Google or Amazon).	*.869*
	from unwanted access by third party application developers.	*.819*
	from unwanted access by hackers.	*.869*
	from unwanted access by government agencies	*.684*
Not Likely the target	I feel that, because I am not rich or famous, my data is not worth stealing.	*.844*
	I believe that because I am just a normal person, hackers are not interested in accessing my personal data.	*.824*
	I believe that hackers are more likely to target smart speakers of high-profile individuals or organisations rather than individuals like me	*.573*
Perceived Creepiness (Owning)	The smart speaker makes me feel uncomfortable.	*.654*
	The smart speaker gives me an eerie feeling.	.801
	This smart speaker creeps me out.	.608
	I feel uneasy towards my smart speaker.	.688
Perceived Creepiness (Non-owning)	This smart home assistant, that I received as a gift, would make me feel uncomfortable.	.897
	This smart home assistant, that I received as a gift, would give me an eerie feeling.	.654
	This smart home assistant, that I received as a gift, would creep me out.	.879
	I would feel uneasy towards this smart home assistant, that I received as a gift.	.929

Statements

LLM [1] Statement

During the preparation of this report, I (Carl Pottkamp) utilized Grammarly and ChatGPT 3.5 as editing tools, but not as generative tools. After using these services, I thoroughly reviewed and edited the content, ensuring I took full responsibility for the final outcome.

[1]Large Language Model