Examining Factors that Undermine Privacy Risk Perception and Protective Behaviour Concerning Smart Speakers

Jenny Hapke

Bachelor Thesis

Submitted to the Department of Psychology of Conflict, Risk, and Safety
Faculty of Behavioural Management and Social Sciences
At the University of Twente

1st Supervisor: dr. Nicole Huijts
2nd Supervisor: dr. Iris van Sintemaartensdijk

Abstract

Smart speakers are a novel technology that has become increasingly common in households across the world in recent years. They are popular because of their hands-free, voice-based usability, but as always with innovative technologies they also bring new and particular privacy risks. The goal of this study was to gain insights on antecedents of risk perception and protective behaviour concerning smart speakers by first collecting insights into possible predictors from Protection Motivation Theory and published qualitative studies and developing measures for the variables found. Using a cross-sectional, correlational online survey the relationships between the independent variables perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy with the dependent variables privacy risk perception and protective behaviour, respectively, were examined. The sample consisted of 267 individuals between 18 and 65 years, mainly from Germany, with about equal amounts owning and not owning a smart speaker. The results reveal significant correlations between all variables except privacy self-efficacy and protective behaviour. When looking at the regression analyses, varying factors predicted privacy risk perception and protective behaviour for people who own and do not own a smart speaker. These results imply that interventions promoting privacy-protecting behaviours should be tailored to specific groups and address the individual factors. However, more research is needed to specify interventions further and to investigate protective behaviours.

Keywords. smart speakers, privacy, privacy risk perception, protective behaviour, protection motivation theory

Examining Factors that Undermine Privacy Risk Perception and Protective Behaviour Concerning Smart Speakers

During the past years, smart home appliances have been on the rise. A smart speaker is the most widely adopted smart home device (Smith, 2018). For example, in 2020 about 34.4% of US adults owned a smart speaker (Kinsella, 2020), while the adoption rates in Europe ranged from 14% in France to 22% in the UK in 2018 (McNair, 2019). Given the rise of smart speakers and the fact that most studies examining privacy risk perception of smart speakers were qualitative in nature, the goal of this study is to gain insights on antecedents of privacy risk perception and protective behaviour concerning smart speakers quantitatively. This will be done by first collecting insights into possible predictors from published qualitative studies combined with the Protection Motivation Theory and then developing measures for the found variables.

Literature Review

A smart speaker, such as the Amazon Echo or Google Home is also called a personal voice assistant (PVA). A PVA comprises hardware and software that allows it to record, process, and evaluate sound and give acoustic feedback to the user (Cheng & Roeding, 2022). Thus, the device can comprehend voiced commands and perform the corresponding action. In order to function properly, the device has to constantly record sound to listen for the wake word. After detecting the wake word, the PVA processes the request through automatic speech recognition (ASR) and subsequently carries out the request and responds to the user (Cheng & Roeding, 2022; Lau et al., 2018). These recordings may be stored and used to enhance ASR algorithms or alternative services. Possible requests are to stream music, ask for the weather, or control other smart home appliances such as light bulbs (Lau et al., 2018). These requests are processed mainly in the manufacturer's cloud-based backend, but smart speakers may also perform automation functions like IFTTT (If This Then That; Lau et al., 2018). To further expand these functions users can make use of third-party applications, which are called "skills" for Alexa and "actions" for Google (Lau et al., 2018). Given all these abilities of smart speakers and their corresponding voice assistants, they may make people's lives more comfortable.

However, they also collect a lot of information about users and very few users are aware of the implications of this for their privacy (Emami-Naeini et al., 2019; Lau et al., 2018). While the microphones that smart speakers contain are seen as very privacy-invasive and users are concerned about their privacy few users alter their behaviour around the smart speakers or employ additional privacy measures (Emami-Naeini et al., 2019; Lau et al., 2018). To sum up, while smart speakers and PVAs are on the rise, there should also be a focus on their privacy risks. Some privacy risks of smart speakers were identified by Chalhoub and Flechais (2020). For example, they identified the risk of company monitoring. This means that smart speaker companies have employees listening to users' voice requests to improve the speech recognition technology (Chalhoub & Flechais, 2020). Moreover, the companies collect personal data, like names, IP addresses, locations, addresses, and payment details.

In addition, misinterpretation of the wake word can lead to privacy risks. For instance, there was a case in the US where a private conversation was accidentally recorded and messaged to a random contact because of misinterpretation (Horcher, 2018). Another privacy threat may come from law enforcement, as the huge amount of personal data collected by smart speakers could potentially be used to help them with investigations (Chalhoub & Flechais, 2020). For example, law enforcement could subpoena the audio logs from smart speakers and listen to the conversations to find incriminating evidence. In one instance, Amazon was able to repel the police warrant to protect users' privacy but released the data after the user consented. This and other examples prompt privacy experts to alert people that laws that would allow law enforcement to activate smart speakers and spy on suspects could be passed (Cranz, 2016). These are privacy risks identified by experts in the field, however, regular users of smart speakers may not necessarily be concerned about these risks.

Qualitative research has demonstrated that most users are not overly concerned about their privacy when using smart speakers. The main threat users perceive is being hacked or being vulnerable to cybersecurity breaches (Manikonda et al., 2018). Other prominent themes in Manikonda et al.'s (2018) study were worries about the gathering of personal data, as well as the recording of intimate conversations and the constant listening of the device. Moreover, users were concerned about the device respecting the users' privacy and about how, where, and for how long data is stored (Abdi et al., 2019; Manikonda et al., 2018). These studies show that while some users may be aware of certain privacy risks, there still exists a gap between the risk identified by experts and the perceived risks. Furthermore, not all users may perceive very diverse privacy risks depending on how familiar they are with technology in general (Huang et al., 2020) and as a result, they are not able to respond well to them.

In addition, Emami-Naeini et al. (2019) found that before purchasing a device, users had no or little privacy concerns. The reasons for this are manifold and usually have to do with various beliefs and values regarding technology, specifically smart speakers. The theoretical background for users' privacy risk perceptions and protective actions around smart speakers can be found in the Protection Motivation Theory (PMT). PMT has been successful in explaining people's behaviour around modern technologies, such as the adoption of green electricity, nanotechnology, or hydrogen cars (Hartmann et al., 2013; Montijn-Dorgelo & Midden, 2008; Siegrist et al., 2007) and can also be applied to the smart speaker context. According to PMT individuals shield themselves from a threat when they perceive the threat as severe and likely, and when they think that they can cope with the threat by employing an effective countermeasure (Rogers, 1975). Thus, people's motivation to protect themselves from a specific threat is contingent on a threat and a coping appraisal (Boerman et al., 2021).

The threat appraisal assesses the anticipated severity and vulnerability to the threat, while the coping appraisal focuses on assessing self-efficacy and response efficacy (Boerman et al., 2021; Balaban & Mustățea, 2021). Self-efficacy in this context can be defined as people's belief in their ability to employ measures that protect their privacy, while response efficacy refers to people's belief that these measures are actually successful in protecting their privacy (Boerman et al., 2021). Furthermore, in order for people to be motivated to protect themselves, both the threat and the coping efficacy have to be perceived as high (Patterson et al., 2021; Witte, 1992). In this study, the threat appraisal is measured by people's privacy risk perception of smart speakers, similar to Boerman et al.'s (2021) study, which investigated motivations for protecting online privacy. They found that especially perceived severity to the risk of having their personal data online collected, used, and shared predicted protective behaviour (Boerman et al., 2021). Thus, also in this study, possible protective behaviours around smart speakers are assumed to be preceded by people's risk perception of them. More specifically, the higher people's risk perception, the more likely they are to take protective actions.

Furthermore, previous qualitative research has found that users tend to evaluate the convenience and enjoyableness of a smart speaker very positively and as more important than privacy risks (Abdi et al., 2019; Chalhoub & Flechais, 2020; Ghiglieri, 2017; Kowalczuk, 2018; Lau et al., 2018; Zeng et al., 2017). This means that people perceive fewer privacy risks since smart speakers make their lives much easier because of their hands-free operationality. This is in line with research on the affect heuristic theory, which suggests that people with positive affect are prone to amplify the benefits, as has been shown by Yu et al. (2015) for self-disclosure on social network websites. Furthermore, Kang and Oh (2021) claim that people are inclined to share personal data when the perceived benefits exceed the perceived risks. They found that perceived benefits, which consist of the perceived enjoyableness and the perceived usefulness of a smart speaker, and perceived risks are in direct competition and therefore more perceived benefits correlate with fewer perceived risks. In addition, according to PMT when individuals perceive the benefits of an action as outweighing the associated risks (Kang & Oh, 2021), their assessment of the potential threats will be low, resulting in a decreased likelihood of engaging in protective behaviours. Thus, perceived enjoyableness and perceived usefulness are expected to have a negative relationship with both privacy risk perception and protective behaviour.

Moreover, people have various beliefs regarding smart speakers that shape their privacy perceptions. One reason people often cited for not being too concerned with their privacy was their trust in companies. They believe that big companies like Amazon or Google can be trusted to protect their data properly (Vitak et al., 2021; Zeng et al., 2017). Similarly, Abdi et al., (2019) found that users think it is the responsibility of the company to protect their data. In addition, Lau et al. (2018) argue that people trust these companies as they already have an established, generally positive, relation with them in other contexts. Relatedly, it was found that trust in companies has a positive influence on the intention to use a smart speaker while reducing privacy concerns (Jasper & Pearson, 2022). However, non-users, especially privacy-conscious people, did not trust companies as much as users and cited this as a reason not to own a smart speaker (Jasper & Pearson, 2022; Lau et al., 2018). Hence, trust/distrust in companies seems to be a crucial factor in the decision to own a smart speaker.

The concept of trust can also be incorporated into the PMT, as trust can influence risk perception. The relationship between trust and attitudes is based on the idea of perceived consequences (Triandis, 1979 as cited in Pavlou & Fygenson, 2006), as trust diminishes social uncertainty and thus the possible consequences are viewed more positively (Pavlou & Fygenson, 2006). Additionally, trust involves the assumption that the trustor's interests will be preserved by the trustee (Hosmer, 1995). This way trust in smart speaker companies shapes a favourable attitude towards the intention to use a smart speaker. Another way trust influences behaviour is through control beliefs. Fukuyama (1995 as cited in Pavlou & Fygenson, 2006) argues that while the trustor does not have control over the behaviour of the trustee, trust increases the belief to be able to depend on the trustee.

In addition, previous studies have found that trust affects risk perception, in that as trust in the responsible actors of technology increases, risk perception decreases and the acceptance of these technologies rises (Huijts et al., 2012; Midden & Huijts, 2009; Montijn-Dorgelo & Midden, 2008; Siegrist, 2002; Siegrist, 2006; Siegrist & Cvetkovich, 2002). Adapted to smart speakers, these findings indicate that as consumers already have a trusting relationship with companies, such as Amazon and Google, they believe that these companies will take adequate measures to protect their privacy. This established trust leads customers to feel more secure and less concerned about any potential privacy issues that may arise from using smart speakers. Integrating these insights from the trust literature with PMT, suggests that trust influences the threat appraisal by lowering the levels of perceived severity and following Boerman et al.'s (2021) study people will be less likely to engage in protective behaviours. Thus, trust in smart speaker companies is estimated to decrease protective actions around smart speakers.

In addition, qualitative research revealed that people think they have nothing to hide (Lau et al., 2018; Zeng et al., 2017), meaning that they do not believe that anyone would find something interesting when going through recordings from their smart speaker. So, the perceived severity and vulnerability of privacy risks are low and accordingly, people are not likely to engage in protective behaviours. Another reason people may not take protective action is that they show resignation towards the lack of privacy. They believe there is already so much data about them out there that it does not matter if a smart speaker also collects their data (Lau et al., 2018). Moreover, Meng et al. (2021) found that users feel powerless and not in control of their data but accept this privacy risk nonetheless in the form of digital resignation. This relates to the concept of response efficacy, meaning that people need to believe that their actions to counter the threat will be cost-effective and successful (Patterson et al., 2021). It can thus be expected that, people who demonstrate resignation towards the lack of privacy are less likely to engage in protective behaviours.

Furthermore, PMT (Rogers, 1975) posits that the concept of self-efficacy is an important predictor of whether people engage in protective actions. Research has found that people with a large self-confidence in their privacy management abilities think that they can negate the consequences of privacy breaches and thus disclose more information (Chen & Chen, 2015). In addition, privacy self-efficacy increases strategies of data protection and decreases the effect of perceived privacy risks (Kang & Oh, 2021), so that individuals who exhibit high levels of privacy-self efficacy perceive fewer privacy risks. Similarly, Liao et al. (2019) argue that digital literacy influences the adoption of smart speakers by affecting their risk perception of exposing personal data. While this study examined behaviour, it can be inferred that privacy self-efficacy also influences privacy risk perception. Therefore, people who are noticeably confident in their technical abilities to protect their privacy around smart speakers should perceive fewer privacy risks.

Researchers have identified some privacy-protecting behaviours that users could easily engage in. First, smart speakers have privacy controls, such as a mute button that prevents the device from listening but must be physically pressed (Lau et al., 2018). Another privacy control for users is the possibility to review and delete audio logs through the mobile app to avoid storing their data on the company's servers (Lau et al., 2018). Moreover, qualitative studies such as Brause and Blank (2023) discovered that users protect their privacy by strategic placement of the smart speaker, only sharing non-sensitive information, and muting the device. An additional possibility is to disable certain device features, such as making purchases with the smart speaker (Chalhoub & Flechais, 2020). Furthermore, there is the possibility to set up multiple user profiles, with the aim of keeping features such as calendars, contacts, or purchases private (Chalhoub & Flechais, 2020). Lastly, Chalhoub and Flechais (2020) found that users tried to limit the sharing of data, by not saying their social security number when the device is listening or not sharing contacts with the device.

Those are thus some straightforward ways for users to regain some control of their data, however, research has found that many users are not aware of these possible protective behaviours and hence do not employ them (Abdi et al., 2019; Emami-Naeini et al., 2019; Meng et al., 2021). Consequently, researchers request to increase awareness about the privacy risks of smart devices and ways to mitigate them (Chandrasekaran et al., 2021; Ghiglieri, 2017; Lee & Kobsa, 2019; Lutz & Newlands, 2021; Manikonda et al., 2018), as this is needed to make informed decisions. Similarly, Emami-Naeini et al. (2017) argue that raising users' awareness allows them to define privacy settings that meet their needs. Moreover, Lee and Kobsa (2019) have discovered that people who are conscious of the possible privacy risks of smart devices are more cautious and certain in their decisions. These findings correspond to the concept of self-efficacy in the PMT. Based on previous results from technology acceptance studies (see Boerman et al., 2021; Montijn-Dorgelo & Midden, 2008; Siegrist et al., 2007), it can be assumed that also in the context of smart speakers, higher levels of privacy self-efficacy correlate with higher levels of protective behaviour.

Current Study

Following from these qualitative studies, perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy are considered as antecedents of privacy risk perception and protective behaviour in this study. In addition, privacy risk perception is assumed to precede protective behaviour. Therefore, this paper will use the aforementioned factors to develop and evaluate a model (Figure 1) that explains (lack of) privacy risk perception of smart speakers and protective behaviour, to identify key beliefs and misbeliefs that keep people from taking protective action, and for gaining insights into possible helpful interventions. Furthermore, this model will explore whether privacy risk perceptions and protective behaviours are predicted by varying factors depending on whether people already own a smart speaker, as Emami-Naeini et al. (2019) found that users had few privacy concerns before purchasing a device but developed more privacy worries after the purchase. Thus, the following hypotheses are formulated:

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.

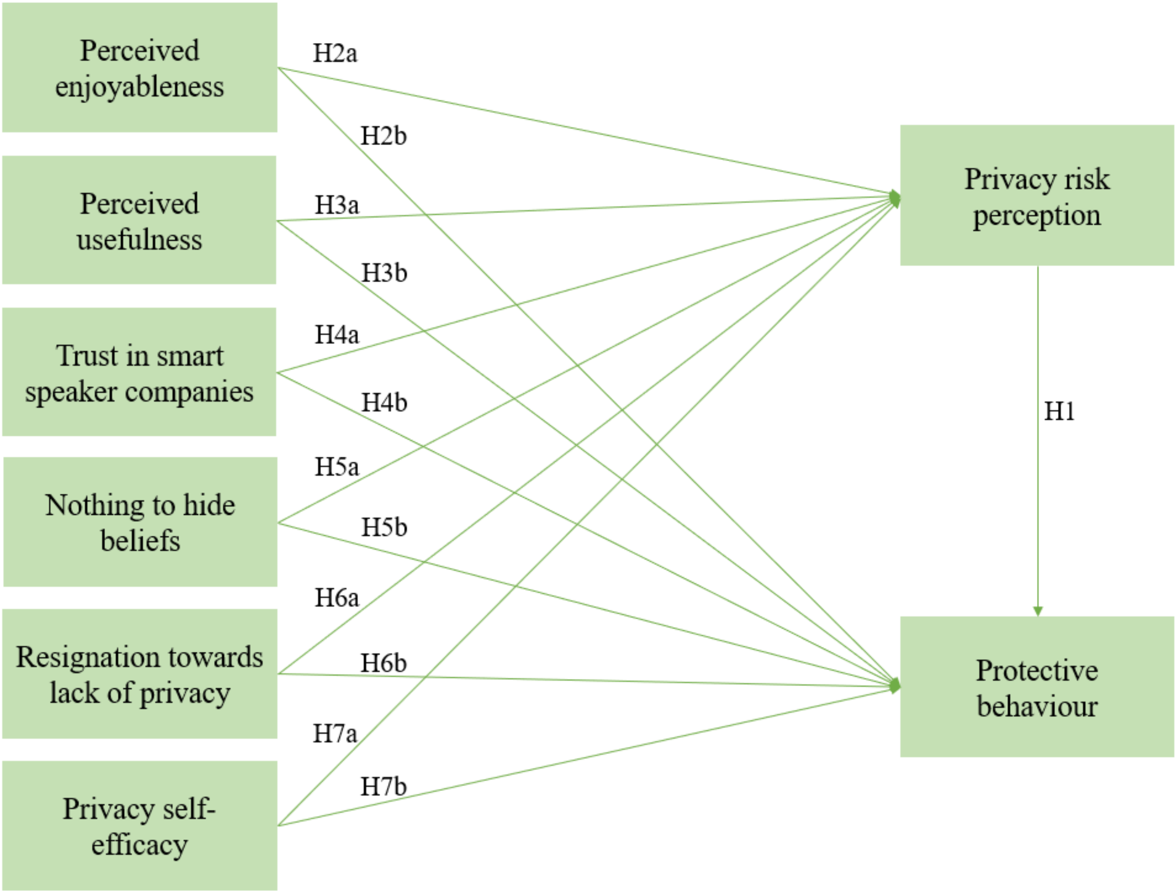
H6b: Resignation towards lack of privacy has a negative effect on protective behaviour.

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

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

Figure 1

Proposed Model Explaining Privacy Risk Perception and Protective Behaviour Regarding Smart Speakers



Methods

Participants

Participants were collected through the online platform SONA, which is a participant recruitment tool used by the University of Twente, social media platforms, such as WhatsApp and Instagram, and the intranet website of Atruvia AG, an IT service provider of the German Cooperative Financial Group. The survey was active from the 6th of April 2023 to the 3rd of May

2023. Participants initially consisted of 393 individuals, from which 126 had to be removed because they did not answer the questions sufficiently, thus the data from 267 participants are subjected to the analyses. 32.6 % of participants are students. 45.7% of participants own a smart speaker, while 54.3 % do not. Out of the 122 participants who own a smart speaker, 80.3% installed it themselves. Participants are aged between 18 and 65 (*M*= 34.2, *SD*= 13.1). The majority of participants are male with 54.7%, 42.7% are female, and 2.6% are non-binary or prefer not to answer this question. Most are from Germany (80.5%) or the Netherlands (10.5%), with other countries including the UK (2.6%) and Spain (0.7%). 1 % of participants completed their primary education and 18% their secondary education; 22 % have completed professional education, 26% have received a bachelor's degree, 24 % a master's degree, and 4% have been awarded a doctorate.

Design and Procedure

The current research used a cross-sectional survey, with a correlational design. An online self-report questionnaire created with Qualtrics was used to gather responses from participants. The entire questionnaire can be found in Appendix A. After agreeing to the informed consent form, participants first answered the control questions, whether they own a smart speaker and if yes installed it themselves, after which they were presented with the corresponding scenario that they have received a smart speaker as a birthday gift and should think about this smart speaker when answering the following questions. Then they completed the items regarding perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, privacy self-efficacy, protective behaviour, and privacy risk perception in random order to minimise any order effects. Afterwards, participants were asked whether they use a smart voice assistant on their phones and their corresponding privacy risk perceptions. Lastly, the demographic data of the participants were measured.

Materials

Some of the items used to measure the various variables were adapted from existing research and others were newly created based on knowledge gained from qualitative research. All items were specified to the context of smart speakers in the home. In addition, the survey had some control items regarding the ownership of a smart speaker and participants' demographic data, such as age, nationality, gender, education, and whether they are a student. The factor loadings for each construct can be found in Appendix B.

Perceived enjoyableness. The items regarding perceived enjoyableness were adapted from the enjoyment scale from Chu (2019). The scale contains four items assessing how enjoyable using a smart speaker would be for participants on a 5-point Likert scale, ranging from 1 "strongly disagree" to 5 "strongly agree". Examples of these items are "I think using a smart speaker that I received as a gift would be enjoyable" and "Using a smart speaker that I received as a gift would not give me pleasure". After reverse coding two of the items, they were averaged (*M*=3.1, *SD*=1.2, α=.91).

Perceived usefulness. Similarly, the items measuring perceived usefulness were taken from Jasper and Pearson (2022) and adapted to the context of smart speakers. This scale consists of five 5-point Likert scale (1 "strongly disagree", 5 "strongly agree") items measuring how a smart speaker would improve the daily life of participants. Examples of items include "Using a smart speaker that I received as a gift would make my life easier" and "Using a smart speaker that I received as a gift would enable me to accomplish my tasks more quickly". The scale consists of the average of these items (*M*=2.5, *SD*=1.0, α=.91).

Trust in smart speaker companies. The concept of trust in smart speaker companies was measured by seven items, four of them were adopted from Jaspers and Pearson (2022) and changed to fit the smart speaker context, while the other three were self-generated. All items were measured on a 5-point Likert scale, with 1 corresponding to "strongly disagree" and 5 being "strongly agree". Examples of the self-generated items are "Smart speaker companies are careful with sharing my personal data with third parties" and "Smart speaker companies care about protecting my data to maintain their positive brand image". All items were averaged (*M*=2.2, *SD*=0.7, α=.85).

Nothing to hide beliefs. The five items belonging to the concept of nothing to hide beliefs were all newly created and measured on a 5-point Likert scale ranging from 1 "strongly disagree" to 5 "strongly agree" but were inspired by the qualitative research done by Lau et al. (2018) and Zeng et al. (2017). For example, the items "I have nothing to hide, so no one would find anything interesting about me in my data" and "I have nothing to hide because I do not do anything criminal in my house" were created. All the items were averaged (*M*=2.6, *SD*=0.8, α=.74). However, the second item "I do not admit to anything that would incriminate me in front of my smart speaker" had an extremely low factor loading of only .01 and was therefore omitted from the analysis, so the final scale consisted of four averaged items (*M*=2.45, *SD*=1.05, α=.83).

Resignation towards lack of privacy. Similarly, the six items regarding resignation towards lack of privacy were self-generated and assessed on a 5-point Likert scale with 1 being "strongly disagree" and 5 "strongly agree" and were influenced by results from qualitative research, such as Lau et al. (2018) and Malkin et al. (2018). Examples of these items include "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" and "Protecting my privacy is so inconvenient that I do not care anymore who has my data". Factor analysis revealed that the items actually measured two distinct constructs (see Table 1), one being indeed resignation towards lack of privacy, consisting of the first three items (*M*=2.55, *SD*=0.95, α=.57), and the other factor relates more to powerlessness and includes the last three items (*M*=3.56, *SD*=0.86, α=.54). Noticeably, both Cronbach's alphas are not very high and below 0.7, which is considered to indicate sufficient reliability of the scale (Tavakol & Dennick, 2011). Consequently, the analyses were carried out for both variables separately, but only the findings of resignation towards lack of privacy are connected to the hypotheses, as no specific hypotheses were formulated for powerlessness.

Table 1

Factor Loadings Resignation towards Lack of Privacy

Construct	Item	Factor loadings	
Resignation towards lack of privacy	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.	.816	-.168
	In order to adopt new technologies, I have to give up my privacy.	.501	.212
	Protecting my privacy is so inconvenient that I do not care anymore who has my data.	.796	
Powerlessness	Consumers have lost all control over how personal information is collected and used by companies.	-.184	.737
	It does not matter what I do regarding the settings of the smart speaker, companies collect loads of information about me anyway.	.466	.578

	I am powerless when it comes to protecting my data from the manufacturer of the smart device.	.121	.784

Privacy self-efficacy. The concept of privacy self-efficacy was measured by nine items on a 5-point Likert scale, ranging from 1 "strongly disagree" to 5 "strongly agree". Four of these items were taken from Kang and Oh's (2021) privacy self-efficacy scale, three were adapted from Schneider and Rahman's (2019) privacy self-efficacy scale, and two items were self-generated to add to Schneider and Rahman's (2019) items. Example items are "I feel in control over the information I provide on my smart speaker" and "I am able to protect my personal information from external threats". Factor analysis revealed that the items actually measured two different constructs (see Table 2). The first one contains the first five items and can be described as privacy self-efficacy (*M*=2.32, *SD*=0.89, α=.84), and the other includes the last four items and can be named security self-efficacy (*M*=2.25, *SD*=0.87, α=.78). Consequently, the analyses were carried out for both variables separately, but only the findings of privacy self-efficacy are connected to the hypotheses, as no specific hypotheses were formulated for security self-efficacy.

Table 2

Factor Loadings Privacy Self-efficacy

Construct	Item	Factor Loading	
Privacy self-efficacy	I feel confident in my ability to protect myself by using the privacy settings of my smart speaker.	.700	.277
	I feel in control over the information I provide to my smart speaker.	.758	.201
	Privacy settings allow me to have full control over the information I would like to provide to my smart speaker.	.835	.167
	I feel in control of who can view my information collected through my smart speaker.	.765	.159
	I am able to protect my personal information from external threats.	.632	.385
Security self-efficacy	I am able to protect the data on my smart speaker from being damaged or altered by external parties.	.457	.629

I am capable of responding well to malicious software such as viruses.	.354	.610
I am able to detect that my smart speaker is hacked.	.197	.824
I am able to erase malicious software from my smart speaker.		.859

Protective behaviour. Regarding protective behaviour, the nine items were measured on a 5-point Likert scale ranging from 1 “extremely unlikely” to 5 “extremely likely”. All the items were self-generated and inspired by previous research, such as Lau et al. (2018), Brause and Blank (2023), Malkin et al. (2019), and Chalhoub and Flechais (2020), as to our knowledge no previous scale assessing protective behaviour concerning smart speakers exists. When constructing the scale, a focus was set on privacy-protecting behaviours, like preventing the device from listening. Example items include “I will regularly spend time reviewing audio logs in the mobile app and delete those that I want to be deleted” and “I will moderate my conversations around the smart speaker so that it does not pick up on very privacy-sensitive conversations”. These nine items were averaged (*M*=2.7, *SD*=1.0, α=.87). Lastly, participants were asked an open question to explore which other behaviours they are likely to conduct around their smart speaker.

Privacy risk perception. The concept of privacy risk perception was measured by three self-generated items, on a 5-point Likert scale, with 1 being “none at all” and 5 being “a great deal”. The items were “To what extent do you think your privacy is at risk now that you installed a smart speaker in your house?”, “How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?”, and “How large do you think the risk is that your privacy is invaded now that you have this smart speaker installed?”. All the items were averaged (*M*=3.2, *SD*=1.0, α=.87). Then participants were asked the same three privacy risk perception questions but adapted to the usage of a smart voice assistant on their phone (averaged: *M*=3.1, *SD*=0.9, α=.89), as initially it was planned to compare privacy risk perception of smart speakers and smartphone voice assistants and whether usage of smartphone voice assistants influences privacy risk perception of smart speakers, but ultimately this was not analysed as it exceeded the scope of this study.

Data Analysis Plan

The data was analysed using IBM SPSS Statistics 28. The demographic data were analysed in terms of frequencies and descriptive statistics. Moreover, descriptive statistics, factor analysis and reliability analysis (Cronbach's alpha) were used to assess the various measurement scales. The hypotheses were assessed with a Pearson correlation analysis and a multiple linear regression analysis was used to evaluate the model. This method section already displayed the descriptive statistics and reliability analysis. The following results section will describe the results from the correlation analysis and the regression analysis.

Results

Hypothesis testing

All Pearson's correlation coefficients and corresponding p-values indicating their significance can be found in Table 3

Table 3

Pearson's Correlation between Privacy Risk Perception and Protective Behaviour with the Dependent Variables

	Privacy risk perception		Protective behaviour	
	r	*p*	*r*	*p*
Privacy risk perception			**.49**	**<.001**
Perceived enjoyableness	**-.47**	**<.001**	**-.49**	**<.001**
Perceived usefulness	**-.35**	**<.001**	**-.36**	**<.001**
Trust in smart speaker companies	**-.54**	**<.001**	**-.33**	**<.001**
Nothing to hide beliefs	**-.38**	**<.001**	**-.29**	**<.001**
Resignation towards lack of privacy	**-.37**	**<.001**	**-.40**	**<.001**
Powerlessness	**.31**	**<.001**	.10	.117
Privacy self-efficacy	**-.55**	**<.001**	**-.21**	**<.001**
Security self-efficacy	**-.22**	**<.001**	.01	.908

Note. All significant correlations are marked in bold.

Hypothesis 1. In line with hypothesis 1, the results show that privacy risk perception has a significant positive relation with protective behaviour. This result suggests that individuals who perceive more privacy risks tend to engage in more protective behaviours regarding smart speakers.

Hypotheses 2a and 2b. In line with hypothesis 2, the analysis revealed that perceived enjoyableness has a significant negative relationship with perceived privacy risks, as well as with protective behaviour. This result suggests that individuals who perceive higher levels of enjoyableness tend to perceive lower levels of privacy risks regarding smart speakers and tend to engage in less protective behaviours around them.

Hypotheses 3a and 3b. In line with hypothesis 3, the results show that perceived usefulness has a significant negative relation with privacy risk perception. This result suggests that individuals who perceive a higher level of usefulness in technology tend to perceive fewer privacy risks of smart speakers. Similarly, there was also a negative correlation found between perceived usefulness and protective behaviour, suggesting that individuals who perceive technology as more useful tend to engage in less protective behaviour.

Hypotheses 4a and 4b. In line with hypothesis 4, the results reveal a significant negative relation between trust in smart speaker companies and privacy risk perception, as well as protective behaviour. This result suggests that individuals who have higher levels of trust in smart speaker companies tend to perceive lower levels of privacy risks of smart speakers and tend to engage in less protective behaviour.

Hypotheses 5a and 5b. In line with hypothesis 5, the analyses showed that nothing to hide beliefs have a significant negative relation with privacy risk perception. This result suggests that individuals who strongly hold the belief of having nothing to hide tend to perceive fewer privacy risks regarding smart speakers. Likewise, the correlation between nothing to hide beliefs and protective behaviour was also negative and significant, indicating that individuals who strongly hold the belief of having nothing to hide tend to engage in less protective behaviour.

Hypotheses 6a and 6b. Since factor analysis revealed that resignation towards lack of privacy actually relies on two different constructs, namely resignation towards lack of privacy and powerlessness, the analyses were performed for both constructs. As the hypotheses were only formulated for resignation towards lack of privacy, the results for powerlessness are considered additional findings and not connected to the hypotheses. In line with hypothesis 6, the results show that resignation towards privacy has a significant negative relation with privacy risk perception and with protective behaviour. These results suggest that people who have a higher tendency to resign themselves towards their perceived lack of privacy tend to perceive fewer privacy risks and engage in less protective behaviour around smart speakers. However, the results revealed a significant positive relation between powerlessness and privacy risk perception, which indicates that the more powerless people feel when it comes to their privacy, the more privacy risks they perceive, as well as a non-significant positive relationship between powerlessness and protective behaviour.

Hypotheses 7a and 7b. Since factor analysis revealed that privacy self-efficacy actually relies on two different constructs, namely privacy self-efficacy and security self-efficacy, the analyses were performed for both constructs. As the hypotheses were only formulated for privacy self-efficacy, the results for security self-efficacy are considered additional findings and not connected to the hypotheses. In line with hypothesis 7, the analyses show a significant positive relationship between privacy self-efficacy and privacy risk perception, suggesting that individuals with higher levels of privacy self-efficacy tend to perceive fewer privacy risks regarding smart speakers. Similarly, the results show that security self-efficacy has a significant negative correlation with privacy risk perception. In contrast, different from the expected result, the analyses demonstrate a significant negative relation between privacy self-efficacy and protective behaviour, indicating that individuals who possess higher levels of privacy self-efficacy tend to engage in slightly fewer protective actions around smart speakers, contradicting hypothesis 7. Lastly, the results also reveal a slightly positive, but non-significant relationship between security self-efficacy and protective behaviour.

Insights into Protective Behaviours

To better understand these unexpected results another Pearson's correlation analysis was performed between privacy-self-efficacy and each of the protective behaviours, as well as between security self-efficacy and every protective behaviour item to see whether there may be individual relationships with the protective measures for example people might engage in one protective behaviour and then do not engage in any other (see Table 4). However, these results also yielded significant negative relationships for the items "I will walk up to the smart speaker and unplug it when I do not want the smart speaker to listen to what I am saying", "I will walk up to the smart speaker and cover it with something of metal when I do not want the smart speaker to hear what I am saying", "I will not place the smart speaker in a privacy-sensitive room like my bedroom", "If I have a visitor, I will inform them that I have a smart speaker", and "If I have a visitor, I will offer to switch the smart speaker off", and non-significant negative correlations for the other items. For security self-efficacy and protective behaviour, the results revealed a significant positive relationship for item 8 “I will set a new difficult password for my smart speaker” but no significant correlations for any of the other items. So, it seems that people with a lot of security self-efficacy are likely to set difficult passwords for their smart speakers and thus probably believe that their privacy is protected sufficiently and do not engage in any other protective behaviours.

Table 4

Pearson’s Correlations Privacy and Security Self-Efficacy with Each Protective Behaviour

	Privacy self-efficacy		Security self-efficacy	
Item	*r*	*p*	*r*	*p*
1) I will walk up to the smart speaker and press the mute button every time I do not want the smart speaker to hear what I am saying.	-.05	.384	-.01	.870
2) I will regularly spend time reviewing audio logs in the mobile app and delete those that I want to be deleted.	-.04	.477	.10	.102
3) I will walk up to the smart speaker and unplug it when I do not want the smart speaker to listen to what I am saying.	**-.22**	**<.001**	-.02	.799
4) I will walk up to the smart speaker and cover it with something of metal when I do not want the smart speaker to hear what I am saying.	**-.15**	**.015**	-.03	.612
5) I will not place the smart speaker in a privacy-sensitive room like my bedroom.	**-.29**	**<.001**	-.07	.248
6) I will moderate my conversations around the smart speaker so that it does not pick up on very privacy-sensitive conversations.	-.11	.067	-.02	.733
7) If I have a visitor, I will inform them that I have a smart speaker.	**-.16**	**.008**	-.04	.548
8) I will set a new difficult password for my smart speaker.	-.11	.070	**.13**	**.032**

9) If I have a visitor, I will offer to switch the smart speaker off.	**-.18**	**.002**	-.03	.596

Note. All significant correlations are marked in bold.

The questionnaire also included an open question that asked participants about other protective behaviours they might take, which were not analysed in depth in this paper but could be points of departure for future research. The behaviours mentioned by participants include non-security solutions, such as only turning it on when it is needed, destroying the microphone, saying contradictory things, not mentioning passwords, or returning the smart speaker. Some participants also mention more technical options like controlling the internet access of the speaker for example by removing wireless hardware and only using cable connection or only using it in the guest WLAN with time/flow control of the traffic.

Regression Analysis

The regression analysis for privacy risk perception and protective behaviour was done for the whole sample and then once more separately for people who own a smart speaker and people who do not own a smart speaker. The independent variables in all cases were perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, powerlessness, privacy self-efficacy, and security self-efficacy. In addition, the regression analysis was done for both privacy risk perception and protective behaviour as the dependent variable, respectively.

Regression Analysis with the Whole Sample. For the complete sample, the regression analysis reveals significant negative effects for perceived enjoyableness, trust in smart speaker companies, resignation towards lack of privacy, and privacy self-efficacy, as well as significant positive effects for powerlessness and security self-efficacy for the dependent variable privacy risk perception (see Table 5). The strongest effect had privacy self-efficacy, followed by perceived enjoyableness and trust in smart speaker companies. Interestingly, the effect of security self-efficacy is positive, while the correlation between those two variables was negative, so it is only positive when the other variables are controlled for. The effects for the variables perceived usefulness and nothing to hide beliefs were not significant. The results from the regression analysis are also in line with the hypotheses for perceived enjoyableness, trust in smart speaker companies, resignation towards lack of privacy, and privacy self-efficacy.

Table 5

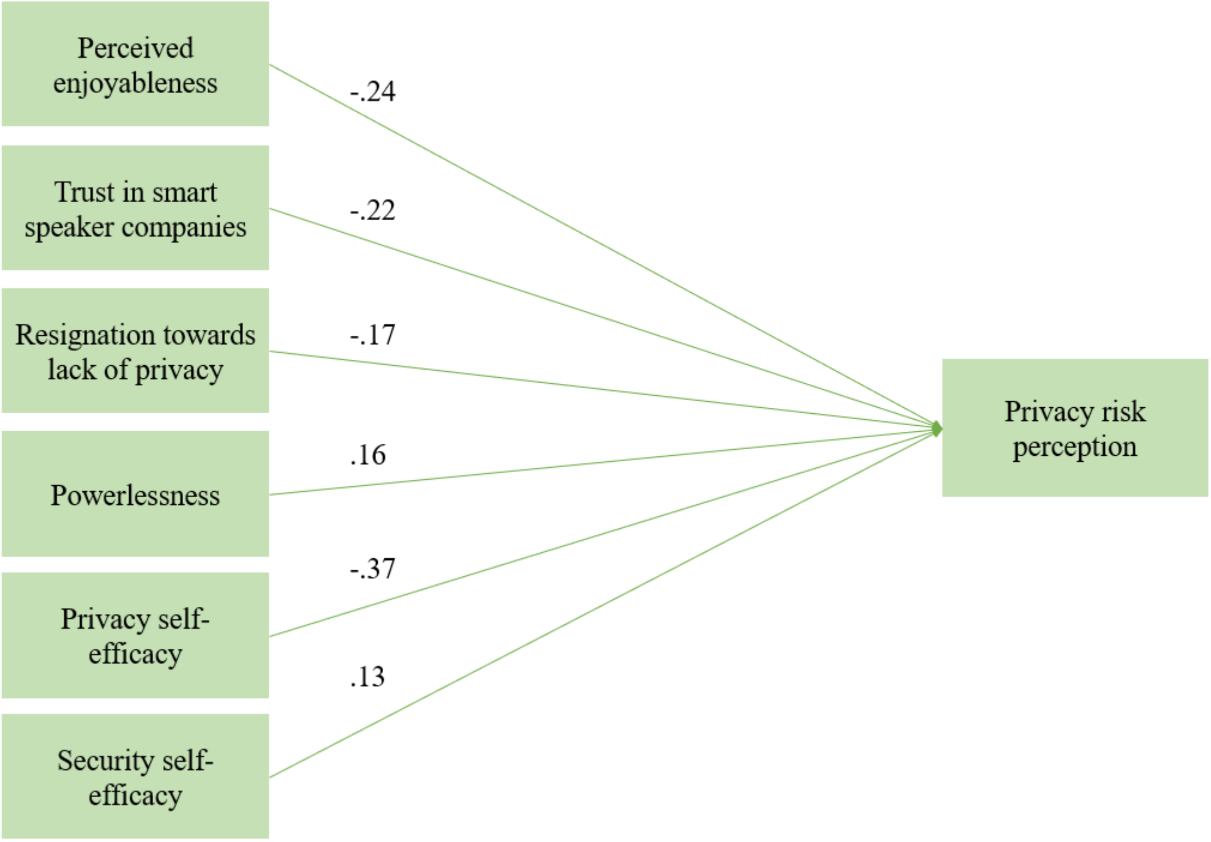
A Model with Privacy Risk Perception as the Dependent Variable of the Complete Sample

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	**-.20**	0.06	-.24	-3.60	**<.001**
Perceived usefulness	.06	0.06	.07	1.06	.292
Trust in smart speaker companies	**-.27**	0.07	-.22	-3.81	**<.001**
Nothing to hide beliefs	-.01	0.05	-.01	-0.23	.819
Resignation towards lack of privacy	**-.17**	0.06	-.17	-2.93	**.004**
Powerlessness	**.17**	0.06	.16	3.07	**.002**
Privacy self-efficacy	**-.39**	0.07	-.37	-5.38	**<.001**
Security self-efficacy	**.14**	0.06	.13	2.23	**.026**

Note. All significant effects are marked in bold. Model Significance: *F*(8,258)=31.76, *p*<.001 R^2=.50

Figure 2

Regression Coefficients with Privacy Risk Perception as the Dependent Variable for Significant Effects



When the dependent variable is protective behaviour, the regression analysis shows significant negative effects for perceived enjoyableness and resignation towards lack of privacy and significant positive effects for powerlessness and security self-efficacy (see Table 6). The negative effects are larger than the positive ones. Interestingly, the effect of security self-efficacy is positive, while the correlation between those two variables was non-significant, so it is only positive when the other variables are controlled for. The other variables had no significant effects on protective behaviour. Overall, this model is less well explained than the previous one on privacy risk perception, as can be seen by the difference in R^2. These results are in line with the hypotheses regarding perceived enjoyableness and resignation towards lack of privacy. Noteworthy is also the positive effect of powerlessness.

Table 6

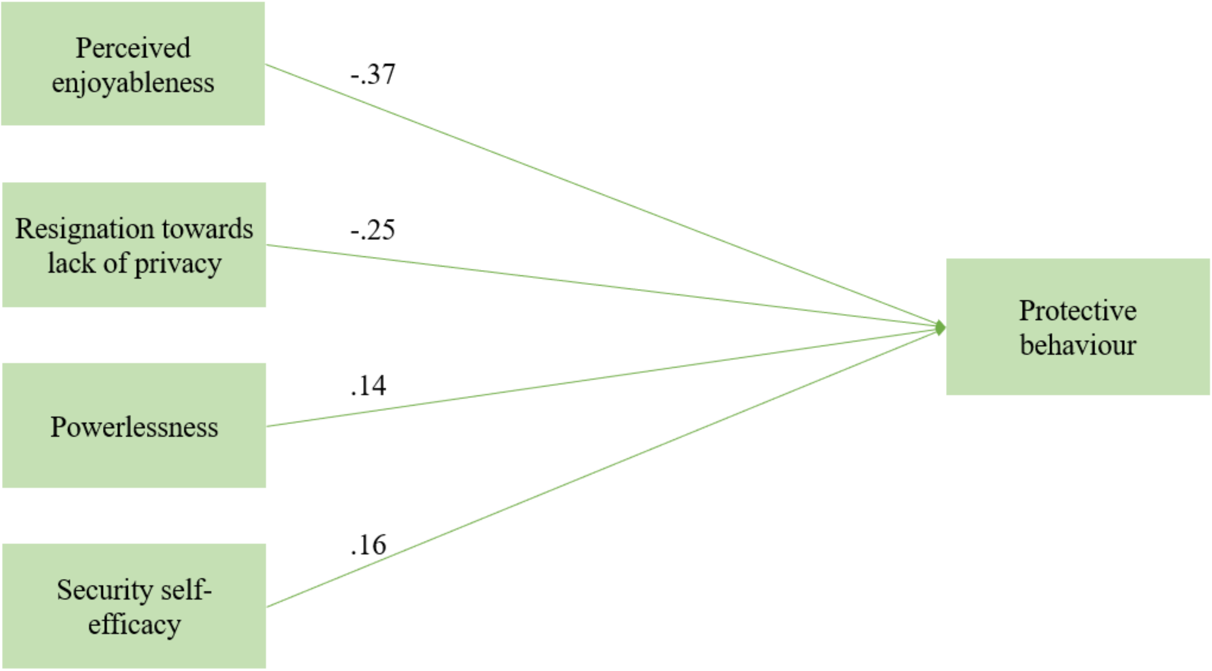
A Model with Protective Behaviour as the Dependent Variable of the Complete Sample

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	**-.32**	0.07	-.37	-4.71	**<.001**
Perceived usefulness	.02	0.07	.02	-0.33	.741
Trust in smart speaker companies	-.12	0.09	-.09	-1.43	.154
Nothing to hide beliefs	.03	0.06	.03	0.42	.678
Resignation towards lack of privacy	**-.25**	0.07	-.24	-3.45	**<.001**
Powerlessness	**.14**	0.07	.13	2.07	**.040**
Privacy self-efficacy	-.06	0.09	-.06	-0.71	.481
Security self-efficacy	**.16**	0.08	.14	2.05	**.042**

Note. All significant effects are marked in bold. Model Significance: $F(8,258)=14.84$, $p<.001$ $R^2=.32$

Figure 3

Regression Coefficients with Protective Behaviour as the Dependent Variable for Significant Effects



3.2.2. Regression Analysis for Privacy Risk Perception.

A comparison was made between people who own and do not own a smart speaker. Here only the *B* and *p*-values are reported, but the complete regression analysis tables can be found in Appendix C. Looking only at the group of people who already own a smart speaker, the regression analysis with privacy risk perception as the dependent variable indicates significant negative effects only for trust in smart speaker companies and privacy self-efficacy (see Table 7). Both effects are similar in size, with trust in smart speaker companies being slightly larger, compared to privacy self-efficacy. The effects for the other variables were not significant. The data is in line with hypotheses concerning trust in smart speaker companies and privacy self-efficacy.

In comparison, when looking at the group of people who do not own a smart speaker, the regression analysis with privacy risk perception as the dependent variable shows significant negative effects for perceived enjoyableness, resignation towards lack of privacy, and privacy self-efficacy, but a significant positive effect for powerlessness (see Table 7). The other variables did not yield significant effects. The strongest effects are found for privacy self-efficacy and perceived enjoyableness. These results are in line with the hypotheses regarding perceived enjoyableness, resignation towards lack of privacy, and privacy self-efficacy. Interestingly, powerlessness has a positive effect on privacy risk perception.

Table 7

Comparison Between People Who Own and Do Not Own a Smart Speaker for Privacy Risk Perception

	People who own a smart speaker		People who do not own a smart speaker	
Variable	*B*	*p*	*B*	*p*
Perceived Enjoyableness	.03	.780	**-.27**	**<.001**
Perceived usefulness	.08	.362	.16	.057
Trust in smart speaker companies	**-.38**	**<.001**	-.09	.385
Nothing to hide beliefs	-.02	.817	-.03	.675
Resignation towards lack of privacy	-.04	.709	**-.23**	**.002**
Powerlessness	.13	.124	**.16**	**.034**
Privacy self-efficacy	**-.28**	**.006**	**-.50**	**<.001**
Security self-efficacy	.17	.056	.13	.134

Note. All significant effects (*p*<.05) are marked in bold.

Regression Analysis for Protective Behaviour.

In contrast, when the regression analysis is done with protective behaviour as the dependent variable for people who own a smart speaker (see Table 8), only security self-efficacy has a significant and positive effect. The other variables (perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, powerlessness, and privacy self-efficacy) had non-significant effects.

To compare, the regression analysis with protective behaviour as the dependent variable for people who do not own a smart speaker reveals significant negative effects for perceived enjoyableness and resignation towards lack of privacy (see Table 8). Perceived enjoyableness has a larger effect compared to resignation towards lack of privacy. The effects of the other variables were not significant. These results are in line with hypotheses regarding perceived enjoyableness and resignation towards lack of privacy.

Table 8

Comparison Between People Who Own and Do Not Own a Smart Speaker for Protective Behaviour

	People who own a smart speaker		People who do not own a smart speaker	
Variable	*B*	*p*	*B*	*p*
Perceived Enjoyableness	-.21	.055	**-.28**	**<.001**
Perceived usefulness	-.12	.239	-.07	.506
Trust in smart speaker companies	-.15	.179	.01	.933
Nothing to hide beliefs	-.01	.898	.04	.651
Resignation towards lack of privacy	-.18	.108	**-.20**	**.034**
Powerlessness	.08	.388	.12	.224
Privacy self-efficacy	-.05	.644	-.01	.948
Security self-efficacy	**.24**	**.017**	.14	.211

Note. All significant effects (*p*<.05) are marked in bold.

Discussion

This study aimed to gain insights into antecedents of privacy risk perception and protective behaviour concerning smart speakers. The results suggest that the variables perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, powerlessness, privacy self-efficacy, and security self-efficacy are negatively correlated with privacy risk perception of smart speakers. Similarly, perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy have a negative correlation with protective behaviours. In contrast, privacy risk perception and protective behaviour have a positive relationship. Moreover, the regression analyses revealed that owners of smart speakers trust in smart speaker companies and privacy self-efficacy undermine privacy risk perception. In comparison for non-owners perceived enjoyableness, resignation towards lack of privacy, and privacy self-efficacy impair privacy risk perception, while powerlessness increases it. Additionally, protective behaviour is encouraged by security self-efficacy for owners of smart speakers, while it is impaired by perceived enjoyableness and resignation towards lack of privacy for non-owners.

Theoretical and Practical Implications

However, there are also a few findings contradicting the expected results. One of these unexpected results is the positive relationship between powerlessness and privacy risk perception, indicating that when people do not feel in control over their privacy with technologies, they still perceive them as very risky. One reason for this result may be that initially the items belonging to the construct of powerlessness were thought to represent resignation towards lack of privacy and thus no concrete hypothesis regarding powerlessness was formulated. The initial variable resignation towards lack of privacy was based on the findings from Lau et al. (2018) and Meng et al. (2021). Lau et al. (2018) had found that people accepted smart speakers out of resignation, as they felt they have to give up their privacy for new technology. In comparison in Meng et al.'s (2021) study, participants reported feeling powerless or helpless as they accept lack of control over their private data when it comes to smart speakers. Similar results were found by Huang et al. (2020), where participants "helplessly accepted the risks" (p. 8). Thus, while the descriptions seemed similar, the results of this study indicate that they should be viewed as two separate constructs and hence should be investigated separately. Considering the results of this study, it seems logical that feeling powerless about protecting one's privacy, does not necessarily mean that one perceives little risks, but that one perceives a lot of privacy risks but feels powerless facing them.

Secondly, the relationship between privacy self-efficacy and protective behaviour is in the opposite direction from the hypothesized one, as the results show a negative correlation, indicating that people with higher privacy self-efficacy tend to engage in less protective behaviours. This finding contrasts with previous technology acceptance studies, such as Boerman et al. (2021) or Montijn-Dorgelo and Midden (2008), which found a positive effect of privacy self-efficacy on protective behaviour When analysing the correlations between privacy self-efficacy and each of the individual behavioural items, the results still mainly show negative and significant correlations. However, the results also show a significant positive relation between security self-efficacy and the item “I will set a new difficult password for my smart speaker”. This finding is quite puzzling and should be researched further. It may be that participants engage in other protective behaviours that were not measured in the questionnaire or they feel sufficiently protected by setting a strong password for their smart speaker. Therefore, future research should use the protective behaviours mentioned in the open question as a point of departure, as they were not measured quantitatively in this study. In that case also a distinction should be made between privacy protecting and security protecting behaviours and how one may influence the other. As in this study the focus was on privacy protecting behaviours, no actions protecting the security of the smart speaker were measured, but the responses to the open question suggest that people first focus on ensuring that the device is secure and then might believe that they are already sufficiently protected and do not need to engage in further privacy protecting behaviours.

The findings of this study indicate that several factors have a negative impact on privacy risk perception, which should be addressed in future research and corresponding interventions, as an increased privacy risk perception correlates with more protective behaviours. Additionally, since the analyses reveal different effects for people who own and do not own a smart speaker, interventions should be tailored to specific groups.

First, research should be done on how to make people more aware of how companies manage their data, so they would be able to have more realistic views on why there are privacy risks when giving your personal data to smart speaker companies. This does not mean that people should not trust these companies at all, but their trust should be well-calibrated. Zheng et al. (2018) for instance, found that people have large levels of trust in the manufacturers of devices, but rarely verify whether companies indeed protect their privacy. This is especially important for people who own a smart speaker, as the results reveal that only for them trust has a significant negative correlation with privacy risk perception. Thus, a campaign aimed at well-calibrated trust in companies should be tailored to individuals who already have a smart speaker.

Moreover, privacy self-efficacy also has a significant negative effect on privacy risk perception for both people who own and do not own a smart speaker. This finding is in line with previous research (see Chen & Chen, 2015; Kang & Oh, 2021) and suggests that people who believe that they are able to protect their privacy, are not very concerned about the privacy risks. This in itself is not necessarily a problem for user's privacy, as long as their confidence in protecting their privacy is accompanied by corresponding protective actions. Thus, interventions should primarily focus on those factors that were found to precede protective behaviour.

For instance, factors that have a negative influence on protective behaviour should be investigated further to create interventions that reduce this effect. One such factor in this study is perceived enjoyableness. This factor only has a significant negative effect for people who do not own a smart speaker. So, an intervention that addresses perceived enjoyableness should be targeted at people who do not have a smart speaker yet. However, such an intervention should not focus on making a smart speaker less enjoyable, but more about putting the perceived enjoyableness and perceived risks into perspective, so that individuals can make informed decisions. For instance, a campaign could promote protective behaviour by saying that when you know it is safe to use a smart speaker, you can relax more and have even more fun with the smart speaker compared to when you do not engage in any protective behaviours. As demonstrated by previous studies, people tend to employ the privacy calculus theory, where they weigh perceived risks against perceived benefits and then form a decision on whether they are willing to accept the risk (Abdi et al., 2019; Chalhoub &Flechais, 2020; Jasper & Pearson, 2022; Ghiglieri, 2017; Kang & Oh, 2021; Kowalczuk, 2018; Lau et al., 2018; Zeng et al., 2017). In addition, the affect heuristic plays a vital role in the relationship between perceived enjoyableness and protective behaviour, as it leads to an overestimation of the benefits of smart speakers (Yu et al., 2015). Thus, an intervention strengthening the perceived risks would lead to more cautious behaviour.

Another factor that has a significant negative effect on protective behaviour for people who do not own a smart speaker is resignation towards lack of privacy. Here, future studies could focus on how to make people less resigned and more interested in defending their privacy again. For example, Lau et al. (2018) propose that smart speaker manufacturers should integrate privacy-friendly defaults, so people do not have to put a lot of extra effort into protecting their privacy. Furthermore, they suggest that the smart speaker itself could explain and clarify privacy-protecting measures (Lau et al., 2018). However, this study found that a campaign focussing on empowering people to regain their privacy should be tailored to individuals who do not own a smart speaker yet. Nevertheless, addressing resignation towards lack of privacy is essential, as it not only concerns the use of smart speakers, but all modern technology and so does not just influence people's private life but also their work (Draper & Turow, 2019; Lee & Kobsa, 2019). Therefore, it is an important challenge to get people interested in protecting their privacy.

In addition, the positive effect of security self-efficacy on protective behaviour in the group of people who own a smart speaker should be noted and researched further. This study showed that there are two types of self-efficacy when it comes to dealing with new technologies, such as smart speakers. First there is privacy self-efficacy, which relates to people's belief that they can protect their data with easy, non-technical measures, like using the privacy settings of a smart speaker. Secondly, security self-efficacy refers more to people's belief in their technical abilities to protect their data, such as recognizing when they are hacked or erasing malicious software. This relates to the results of Chen and Chen (2015) that people who believe they can negate the consequences of privacy breaches provide more information online. Based on these findings, an intervention could be designed that promotes security self-efficacy, for example by teaching about safe passwords or how to deal with malware or viruses. A campaign like this should be focused on people who own a smart speaker. Other interventions could focus more on privacy self-efficacy by educating people about the available privacy controls of smart speakers.

However, to be able to tailor these campaigns even better to people, future research should analyse the socio-demographics further, so target groups can be even smaller and more specific and hence the campaign more successful. For example, there may be gender or age differences, or differences between people of different nationalities. This idea has been explored by Ebbers and Karaboga (2023), who discovered that risk perceptions of smart speakers varied by age, gender, and education. For example, for older people smart speakers may offer increased autonomy, which may outweigh privacy concerns (Lau et al., 2018). Moreover, Ebbers and Karaboga (2023) found that women were significantly more concerned about the security and privacy of smart speakers than men. Interestingly, Ebbers and Karaboga (2023) also found that people who had only used a smart speaker for less than one month perceived fewer privacy risks and consequently took fewer protective measures than people who had it for one year. Then the effect is completely reversed, which could be because, in the beginning, they want to get to know the new device and then increasingly become aware of possible risks. This is something that was not taken into consideration in the present study but would also be interesting to research further to incorporate it into campaigns addressing privacy risks and protective behaviours.

Altogether, the most important next steps are research and campaigns promoting protective behaviours regarding smart speakers, as the technology is advancing and will be present in more households. The starting point for people who do not own a smart speaker yet should be to address the perceived enjoyableness by emphasizing that enjoyableness increases when using a smart speaker safely and their resignation towards a lack of their perceived privacy, as those factors appear to have a negative effect on taking protective actions. For people who already own a smart speaker, campaigns should focus on promoting their security self-efficacy, so users are better able to protect themselves.

Strengths, Limitations, and Future Research

This study has some strong points, but also some limitations. One of the strengths of this study is the sample size (267) and its diversity, as there were about equal numbers of participants who own and do not own a smart speaker (45.7% and 54.3% respectively). There were also about the same number of male and female participants (54.7% and 42.7% respectively). In addition, 32.7% of participants were students, while the others were working population. However, most of the participants were German (80%), so these results may only be representative in Germany and should therefore be replicated with participants from other countries. Moreover, many respondents are from Atruvia AG, an IT service provider, so the study should be repeated with the average population.

In addition, the nature of this study does not allow us to draw inferences about the direction of the relationships. It is very well possible that for example, privacy risk perceptions influence people's trust in companies and not like hypothesized in this study the other way around. For example, Vimalkumar et al. (2021) found that consumers are increasingly concerned about the data gathered by big tech companies about them and so they perceive more privacy risks, which decreased consumers’ trust in innovative technology like voice-based digital assistants. Thus, future research needs to examine the direction of the relationships found in this study, and correspondingly make recommendations for interventions.

Moreover, a limitation of this study was the style of the assessment of protective behaviours of users. The analyses indicate that the closed questions with the limited options that were chosen may not have been the actions users actually take. Even though the protective behaviour options in this study were directly taken from qualitative studies on privacy risk perception of smart speakers like Lau et al. (2018) and Brause and Blank (2023), future studies should improve the assessment of protective behaviours. One option could be to provide them with more options to choose from, like the ones suggested in the open-ended question of this survey or ask if they even would install it, as some participants mentioned that they would just return it. Furthermore, more items that assess whether people protect themselves from cyber attacks, for example if they use a separate router or network for the smart speaker could be aded in future studies. Another item that could be added is whether people would seek advice from someone on how to set up and use a smart speaker safely. It could also be beneficial to ask people what they would do instead of presenting them with options, so they have the opportunity to give answers the researchers do not anticipate but also to avoid biasing them to give socially desirable answers. In addition, future research could make a distinction between primary and secondary users of smart speakers and their privacy risk perceptions, as qualitative research has found that primary users are usually more aware of the functionality and risks of smart speakers (Lau et al., 2018). Furthermore, primary, and secondary users may have diverse privacy concerns, as in a multiple user context there is also the risk of people using the smart speaker to spy on each other (Chalhoub & Flechais, 2020). Moreover, a future study could include factors that may increase privacy risk perception, such as having a technical background or privacy as a value.

Conclusion

Smart speakers easy operationality and life-facilitating functionality makes them increasingly popular. However, their unique privacy risks are concerning when not addressed properly. This study found that protective behaviour is undermined by perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy. Furthermore, it was discovered that protective behaviour is preceded by distinct factors for owners and non-owners of smart speakers, indicating that interventions should make a distinction between those groups. Additionally, future studies should investigate further variations between groups, such as gender, age, or educational differences. That would allow for even better-tailored and more effective interventions. Overall, this study stresses the importance of understanding factors that undermine privacy risk perception and protective behaviour concerning smart speakers and the need to address these factors. Given the rapid adaption-growth of smart speakers and other smart technologies combatting these factors and increasing privacy-protecting behaviours is essential.

References

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. https://www.usenix.org/conference/soups2019/presentation/abdi

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Balaban, D., & Mustățea, M. (2021). Privacy concerns in mobile communication. A user's perspective. *Philobiblon, 26*(1), 101-114. https://doi.org/10.26424/philobib.2021.26.1.06

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

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

Chandrasekaran, V., Banerjee, S., Mutlu, B., & Fawaz, K. (2021). PowerCut and Obfuscator: An Exploration of the Design Space for Privacy-Preserving Interventions for Voice Assistants. *ArXiv:1812.00263 [Cs]*. https://arxiv.org/abs/1812.00263

Chalhoub, G., & Flechais, I. (2020). "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In Moallem, A. (ed) *HCI for Cybersecurity, Privacy and Trust. HCII 2020. Lecture Notes in Computer Science*, (vol 12210). Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_21

Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking 30*(1): 13–19. https://doi.org/10.1089/cyber.2014.0456

Cheng, P., & Roeding, U. (2022). Personal Voice Assistant Security and Privacy – A Survey. *Proceedings of the IEEE, 110*(4), 476-507. https://doi.org/10.1109/JPROC.2022.3153167

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/77187/1/Chu_MSc_BMS.pdf

Cranz, A. (2016, March 15). *Amazon's Alexa Is Not Even Remotely Secure and I Really Don't*

Care. Gizmodo. https://gizmodo.com/alexa-is-not-even-remotely-secure-and-really-i-I-car-1764761117

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New media & society, 21*(8), 1824-1839. https://doi.org/10.1177/1461444819833331

Duezguen, R., Mayer, P., Berens, B., Beckmann, C., Aldag, L., Mossano, M., Volkamer, M., & Strufe, T. (2021). How to Increase Smart Home Security and Privacy Risk. *Proceedings –2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021.* 997-1004. https://doi.org/10.1109/TrustCom53373.2021.00138

Ebbers, F., & Karaboga, M. (2023). Influencing Factors for Users' Privacy and Security Protection Behavior in Smart Speakers: Insights from a Swiss User Study. *Computer Security. ESORICS 2022 International Workshops. ESORICS 2022. Lecture Notes in Computer Science*, (vol 13785, pp. 195–211). Springer, Cham. https://doi.org/10.1007/978-3-031-25460-4_11

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., & Sadeh, N. (2017). Privacy Expectations and Preferences in an IoT World. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).* https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

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

Furey, E., & Blue, J. (2018). She Knows Too Much – Voice Command Devices and Privacy. *29th Irish Signals and Systems Conference (ISSC),* 1-6. https://doi.org/10.1109/ISSC.2018.8585380.

Garun, N. (2019, November 21). *How to hear (and delete) every conversation your Amazon Alexa has recorded*. The Verge. https://www.theverge.com/2018/5/28/17402154/amazon-echo-alexa-conversation-recording-history-listen-how-to

Ghiglieri, M., Volkamer, M., & Renaud, K. (2017). Exploring consumers' attitudes of smart TV related privacy risks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

https://doi.org/10.1007/978-3-319-58460-7_45

Hartmann, P., Apaolaza, V., D'Souza, C., Echebarria, C., & Barrutioa, J. M. (2013). Nuclear power threats, public opposition and green electricity adoption: Effects of threat belief appraisal and fear arousal. *Energy Policy, 62*, 1366-1376. https://doi.org/10.1016/j.enpol.2013.07.058

Horcher, G. (2018, May 25). *Woman says her Amazon device recorded private conversation, Sent it out to random contact*. Kiro7. https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974/

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review, 20*(2), 379-403. https://doi.org/10.5465/amr.1995.9507312923

Huang, Y., Obada-Obieh, B., & Beznosov, K. K. (2020). Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* 1-13. https://doi.org/10.1145/3313831.3376529

Huijts, N., Molin, E., & Steg, L. (2012). Psychological factors influencing sustainable energy technology acceptance: A review-based comprehensive framework. *Renewable and Sustainable Energy Reviews, 16*(1), 525-531. https://doi.org/10.1016/j.rser.2011.08.018

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

Kinsella, B. (2020, April 28). *Nearly 90 Million U.S. Adults Have Smart Speakers, Adoption Now Exceeds One-Third of Consumers*. Voicebot.ai. https://voicebot.ai/2020/04/28/nearly-90-million-u-s-adults-have-smart-speakers-adoption-now-exceeds-one-third-of-consumers/

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., Zimmermann, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on*

Human-Computer Interaction, 2(CSCW). https://doi.org/10.1145/3274371

Lee, H., & Kobsa, A. (2019). Confident Privacy Decision/-Making in IoT Environments. *ACM Transactions on Computer-Human Interaction, 27*(1), 1-39. https://doi.org/10.1145/3364223

Liao, Y., Vitak, J., Kumar, P., Zimmer, M., & Kritikos, K. (2019). Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In Taylor, N., Christian-Lamb, C., Martin, M., Nardi, B. (eds) *Information in Contemporary Society. iConference 2019. Lecture Notes in Computer Science* (vol 11420, pp. 102-113). Springer, Cham. https://doi.org/10.1007/978-3-030-15742-5_9

Lutz, C., & Newlands, G. (2020). Privacy and smart speakers: A multi-dimensional approach. *The Information Society, 37*(3), 147-162. https://doi.org/10.1080/01972243.2021.1897914

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies, 2019*(4), 250-271. https://doi.org/10.2478/popets-2019-0068

Manikonda, L., Deotale, A., & Kambhampati, S. (2018). What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants. *AIES 2018 – Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 229-235. https://doi.org/10.1145/3278721.3278773

McNair, C. (2019, January 2). *Global Smart Speaker Users 2019.* eMarketer. https://www.insiderintelligence.com/content/global-smart-speaker-users-2019

Meng, N., Kekulluoglu, D., & Vainea, K. (2021). Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1). https://doi.org/10.1145/3449119

Midden, C. J. H., & Huijts, N. M. A. (2009). The Role of Trust in the Affective Evaluation of Novel Risks: The Case of CO2 Storage. *Risk Analysis, 29*(5), 743-751. https://doi.org/10.1111/j.1539-6924.2009.01201.x

Montijn-Dorgelo, F. N. H., & Midden, C. J. H. (2008). The role of negative associations and Trust in risk perception of new hydrogen systems. *Journal of Risk Research, 11*(5), 659-671. https://doi.org/10.1080/13669870801967218

Patterson, L., Chard, S., & Welch, I. (2021). Internet of Things (IoT) Privacy and Security: A

User-Focused Study of Aotearoa New Zealand Home Users. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 4404-4412. http://hdl.handle.net/10125/71152

Pavlou, P., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior Qjarteny Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115-143. https://doi.org/10.2307/25148720

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*, 93-114. https://doi.org/10.1080/00223980.1975.9915803

Siegrist, M. (2002). The Influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology. *Risk Analysis, 20*(2), 195-204. https://doi.org/10.1111/0272-4332.202020

Siegrist, M. (2006). A Causal Model Explaining the Perception and Acceptance of Gene Technology. *Journal of Applied Social Psychology, 29*(10), 2093-2106. https://doi.org/10.1111/j.1559-1816.1999.tb02297.x

Siegrist, M., & Cvetkovich, G. (2002). Perception of Hazards: The Role of Social Trust and Knowledge. *Risk Analysis, 20*(5), 713-720. https://doi.org/10.1111/0272-4332.205064

Siegrist, M., Cousin, M., Kastenholz, H., & Wiek, A. (2007). Public acceptance of nanotechnology foods and food packaging: The influence of affect and trust. *Appetite, 49*(2), 459-466. https://doi.org/10.1016/j.appet.2007.03.002

Smith, P. (2018, May 14). *Smart speakers and connected appliances the gateway drug as IoT goes mainstream.* Financial Review. https://www.afr.com/technology/gadgets/home-entertainment/smart-speakers-and-connected-appliances-the-gateway-drug-as-iot-goes-mainstream-20180513-h100i3.

Tavakol, M., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. *International Journal Of Medical Education, 2*, 53-55. https://doi.org/ 10.5116/ijme.4dfb.8dfd

Vimalkumar, M., Sharma, S., Singh, J., & Dwivedi, Y. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behaviour, 120*. https://doi.org/10.1016/j.chb.2021.106763

Vitak, J., Zimmer, M., Lenhart, A., Park, S., Wong, R. Y., & Yao, Y. (2021). Designing for Data Awareness: Addressing Privacy and Security Concerns about "Smart" Technologies.

Conference on Computer Supported Cooperative Work, CSCW, 364-367. https://doi.org/10.1145/3462204.3481724

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59*(4), 329-349. https://doi.org/10.1080/03637759209376276

Yu, J., Hu, P., & Cheng, T. (2015). Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models. *Journal of Management Information Systems, 32*(2), 239-277. https://doi.org/ 10.1080/07421222.2015.1063305

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*. USENIX Association. https://dl.acm.org/citation.cfm?id=3235931

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017). DolphinAttack: inaudible voice commands. *Proceedings of the ACM Conference on Computer and Communications Security*, 103–117. https://doi.org/10.1145/3133956.3134052

Zheng, S., Apthorpe, N., Chetty M., & Feamster, N. (2018). User perceptions of smart home Io privacy. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW). https://doi.org/10.1145/3274469

Appendix A

Questionnaire

Informed Consent

Project Title

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

Researchers

Jenny Hapke (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 last approximately 15 minutes. People who participate via SONA Systems will be compensated with 0.25 credits.

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:

Jenny Hapke: j.hapke@student.utwente.nl,or

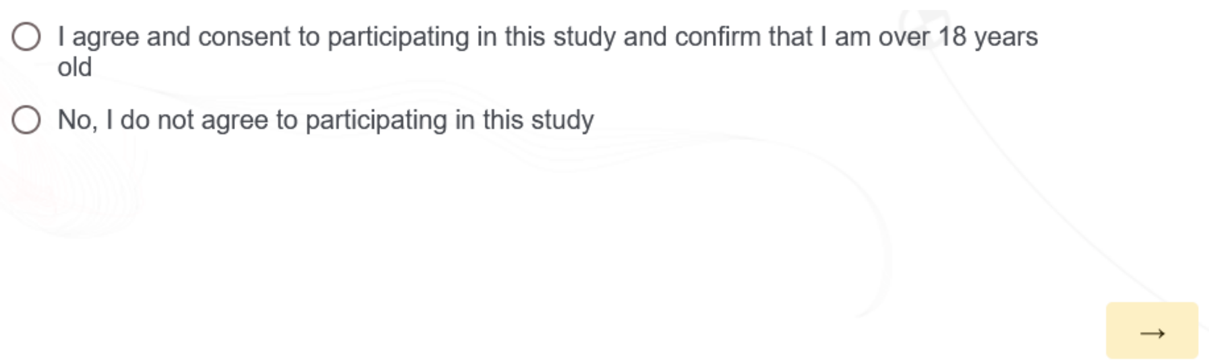
Dr. Nicole Huijts: n.m.a.huijts@utwente.nl

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.**

Consent and Authorization Provisions

In order to continue with this survey, you have to agree with the aforementioned information and consent to participate in the study.

Clicking **“I agree and consent to participating in this study and confirm that I am over 18 years old”** indicates that you have been informed about the nature and method of this research in a manner that is clear to you, you have been given the time to read the page, and that you voluntarily agree to participate in this study.



○ 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

Control questions

- Do you have a smart speaker (also say yes if you are a student and have one in your parent's house)? (Yes/No)
  - If yes: Did you install it yourself? (Yes/No)
  - If yes: For the rest of the survey, please imagine you got a new smart speaker as a present for your birthday and you decide to replace the one you (or your parents when you are a student) already have with the new one. Think about this smart speaker when answering the following questions.
  - If no: For the rest of the survey, please imagine you received a smart speaker as a birthday gift and you installed it in your home. Think about this new smart speaker when answering the following questions.

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

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.
- I think I would have fun using a smart speaker that I received as a gift.
- It would not be interesting to use a smart speaker that I received as a gift.
- Using a smart speaker that I received as a gift would not give me pleasure.

Perceived Usefulness (5-point Likert scale 1= strongly disagree, 5 = strongly agree)

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

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

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

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.
- I trust that smart speaker companies keep my best interests in mind when dealing with the information collected about me by the smart speaker.
- Smart speaker companies are in general predictable and consistent regarding the usage of the information collected about me.
- Smart speaker companies are careful with sharing my personal data with third parties.
- Smart speaker companies are always honest with customers when it comes to using the information that they provide.
- Smart speaker companies intend to protect my data well because they want to keep their market shares.
- Smart speaker companies care about protecting my data to maintain their positive brand image.

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

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

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

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

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

- 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.
- In order to adopt new technologies, I have to give up my privacy.
- Protecting my privacy is so inconvenient that I do not care anymore who has my data.
- Consumers have lost all control over how personal information is collected and used by companies.
- It does not matter what I do regarding the settings of the smart speaker, companies collect loads of information about me anyway.
- I am powerless when it comes to protecting my data from the manufacturer of the smart device.

Privacy self-efficacy (5-point Likert scale 1= strongly disagree, 5= strongly agree)

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.
- I feel in control over the information I provide to my smart speaker.
- Privacy settings allow me to have full control over the information I would like to provide to my smart speaker.
- I feel in control of who can view my information collected through my smart speaker.
- I am able to protect my personal information from external threats.
- I am able to protect the data on my smart speaker from being damaged or altered by external parties.
- I am capable of responding well to malicious software such as viruses.
- I am able to detect that my smart speaker is hacked.
- I am able to erase malicious software from my smart speaker.

Protective behaviour

How likely are you to engage in the following behaviours? (1= extremely unlikely, 5 = extremely likely)

- I will walk up to the smart speaker and press the mute button every time I do not want the smart speaker to hear what I am saying.
- I will regularly spend time reviewing audio logs in the mobile app and delete those that I want to be deleted.
- I will walk up to the smart speaker and unplug it when I do not want the smart speaker to listen to what I am saying.
- I will walk up to the smart speaker and cover it with something of metal when I do not want the smart speaker to hear what I am saying.
- I will not place the smart speaker in a privacy-sensitive room like my bedroom.
- I will moderate my conversations around the smart speaker so that it does not pick up on very privacy-sensitive conversations.
- If I have a visitor, I will inform them that I have a smart speaker.
- I will set a new difficult password for my smart speaker.
- If I have a visitor, I will offer to switch the smart speaker off.
- Which other behaviour(s) not previously listed here are you likely to conduct around your smart speaker?

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

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

Smartphone voice assistants & Privacy Risk Perception (1= none at all, 5 = a great deal)

- Do you use the smart voice assistant on your phone (e.g., Siri, Hey Google) (Yes/No)
- To what extent do you think your privacy is at risk when using a smartphone voice assistant?
- How likely is it that personal information collected about you by the smartphone voice assistant is leaked?
- How large do you think the risk is that your privacy is invaded when using a smartphone voice assistant?

Demographic questions

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

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 Jenny Hapke: j.hapke@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

Factor Loadings

Construct	Items	Factor Loadings
Perceived enjoyableness	I think using a smart speaker that I received as a gift would be enjoyable.	.914
	I think I would have fun using a smart speaker that I received as a gift.	.915
	It would not be interesting to use a smart speaker that I received as a gift.	.864
	Using a smart speaker that I received as a gift would not give me pleasure.	.865
Perceived usefulness	Using a smart speaker that I received as a gift, would improve my productivity in my daily life.	.880
	Using a smart speaker, that I received as a gift, would make my life easier.	.858
	Using a smart speaker, that I received as a gift, would enable me to accomplish my tasks more quickly.	.864
	Using a smart speaker, that I received as a gift, would enhance my effectiveness in daily tasks.	.900
	I would find it useful to use a smart speaker I received as a gift at home.	.801
Trust in smart speaker companies	Smart speaker companies are trustworthy in handling the data the smart speaker collects about me.	.817
	I trust that smart speaker companies keep my best interests in mind when dealing with the information collected about me by the smart speaker.	.739
	Smart speaker companies are in general predictable and consistent regarding the usage of the information collected about me.	.586
	Smart speaker companies are careful with sharing my personal data with third parties.	.791
	Smart speaker companies are always honest with customers when it comes to using the information that they provide.	.713
	Smart speaker companies intend to protect my data well because they want to keep their market shares.	.723
	Smart speaker companies care about protecting my data to maintain their positive brand image.	.746
Nothing to hide beliefs	I have nothing to hide, so no one would find anything interesting about me in my data.	.855
	I do not admit to anything that would incriminate me in front of my smart speaker.	.006

	I have nothing to hide because I do not do anything criminal in my house.	.825	
	I do not do much in my house that I do not want other people to know about.	.722	
	My life is very boring, so the data collected about me is of little interest to others.	.836	
Resignation towards lack of privacy	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.	.816	-.168
	In order to adopt new technologies, I have to give up my privacy.	.501	.212
	Protecting my privacy is so inconvenient that I do not care anymore who has my data.	.796	
Powerlessness	Consumers have lost all control over how personal information is collected and used by companies.	-.184	.737
	It does not matter what I do regarding the settings of the smart speaker, companies collect loads of information about me anyway.	.466	.578
	I am powerless when it comes to protecting my data from the manufacturer of the smart device.	.121	.784
Privacy self-efficacy	I feel confident in my ability to protect myself by using the privacy settings of my smart speaker.	.700	.277
	I feel in control over the information I provide to my smart speaker.	.758	.201
	Privacy settings allow me to have full control over the information I would like to provide to my smart speaker.	.835	.167
	I feel in control of who can view my information collected through my smart speaker.	.765	.159
	I am able to protect my personal information from external threats.	.632	.385
Security self-efficacy	I am able to protect the data on my smart speaker from being damaged or altered by external parties.	.457	.629
	I am capable of responding well to malicious software such as viruses.	.354	.610
	I am able to detect that my smart speaker is hacked.	.197	.824
	I am able to erase malicious software from my smart speaker.		.859
Protective behaviour	I will walk up to the smart speaker and press the mute button every time I do not want the smart speaker to hear what I am saying.	.732	
	I will regularly spend time reviewing audio logs in the mobile app and delete those that I want to be deleted.	.635	

	I will walk up to the smart speaker and unplug it when I do not want the smart speaker to listen to what I am saying.	.775
	I will walk up to the smart speaker and cover it with something of metal when I do not want the smart speaker to hear what I am saying.	.619
	I will not place the smart speaker in a privacy-sensitive room like my bedroom.	.660
	I will moderate my conversations around the smart speaker so that it does not pick up on very privacy-sensitive conversations.	.735
	If I have a visitor, I will inform them that I have a smart speaker.	.780
	I will set a new difficult password for my smart speaker.	.553
	If I have a visitor, I will offer to switch the smart speaker off.	.824
Privacy risk perception	To what extent do you think your privacy is at risk now that you installed a smart speaker in your house?	.927
	How likely is it that personal information collected about you by the smart speaker is leaked to people outside your household?	.830
	How large do you think the risk is that your privacy is invaded now that you have this smart speaker installed?	.910
Smartphone voice assistant risk perception	To what extent do you think your privacy is at risk when using a smartphone voice assistant?	.908
	How likely is it that personal information collected about you by the smartphone voice assistant is leaked?	.881
	How large do you think the risk is that your privacy is invaded when using a smartphone voice assistant?	.931

Appendix C

Complete Regression Analysis Tables

Table C1

Model People Who Own a Smart Speaker with Privacy Risk Perception as the Dependent Variable

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	.03	0.10	.03	0.28	.780
Perceived usefulness	.08	0.09	-.10	-0.92	.362
Trust in smart speaker companies	**-.38**	0.09	-.37	-4.05	**<.001**
Nothing to hide beliefs	-.02	0.07	-.02	-0.23	.817
Resignation towards lack of privacy	-.04	0.10	-.04	-0.37	.709
Powerlessness	.13	0.09	.15	1.55	.124
Privacy self-efficacy	**-.28**	0.10	-.32	-2.82	**.006**
Security self-efficacy	.17	0.09	.19	1.93	.056

Note. All significant effects are marked in bold. Model Significance: $F(8,113)=8.55$, $p<.001$ $R^2=.38$

Table C2

Model People Who Own a Smart Speaker with Protective Behaviour as the Dependent Variable

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	-.21	0.11	-.24	-1.94	.055
Perceived usefulness	.12	0.10	.14	1.18	.239
Trust in smart speaker companies	-.15	0.11	-.14	-1.35	.179
Nothing to hide beliefs	-.01	0.08	-.01	-0.13	.898
Resignation towards lack of privacy	-.18	0.11	-.20	-1.62	.108
Powerlessness	.08	0.10	.09	0.87	.388
Privacy self-efficacy	-.05	0.11	-.06	-0.46	.644
Security self-efficacy	**.24**	0.10	.27	2.43	**.017**

Note. All significant effects are marked in bold. Model Significance: $F(8,113)=3.59$, $p<.001$ $R^2=.20$

Table C3

Model People Who Do Not Own a Smart Speaker with Privacy Risk Perception as the Dependent Variable

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	**-.27**	0.07	-.36	-4.04	**<.001**
Perceived usefulness	.16	0.08	.16	1.92	.057
Trust in smart speaker companies	-.09	0.10	-.07	-0.87	.385
Nothing to hide beliefs	-.03	0.07	-.03	-0.42	.675
Resignation towards lack of privacy	**-.23**	0.07	-.23	-8.09	**.002**
Powerlessness	**.16**	0.08	.15	2.14	**.034**
Privacy self-efficacy	**-.50**	0.11	-.41	-4.49	**<.001**
Security self-efficacy	.13	0.0	.12	1.51	.134

Note. All significant effects are marked in bold. Model Significance: *F*(8,136)= 15.68, *p*<.001 R^2=.48

Table C4

Model People Who Do Not Own a Smart Speaker with Protective Behaviour as the Dependent Variable

Variable	*B*	*SE B*	β	*t*	*p*
Perceived enjoyableness	**-.28**	0.08	-.36	-3.40	**<.001**
Perceived usefulness	-.07	0.10	-.07	-0.67	.506
Trust in smart speaker companies	.01	0.13	.01	0.08	.933
Nothing to hide beliefs	.04	0.09	.04	0.45	.651
Resignation towards lack of privacy	**-.20**	0.09	-.19	-2.14	**.034**
Powerlessness	.12	0.10	.10	1.22	.224
Privacy self-efficacy	-.01	0.14	-.01	-0.07	.948
Security self-efficacy	.14	0.11	.12	1.26	.211

Note. All significant effects are marked in bold. Model Significance: *F*(8, 136)=65.69, *p*<.001 R^2=.25

Appendix D

SPSS codes

Descriptive statistics

```
MEANS VARIABLES = Age
   /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN.

FREQUENCIES VARIABLES=OwnSmartSpeaker InstalledSmartSpeaker Country Gender
Education Student
  /FORMAT=NOTABLE
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN
  /PIECHART PERCENT
  /ORDER=ANALYSIS.
```

Reverse coding items

```
RECODE H3 (1=5) (2=4) (3=3) (4=2) (5=1) INTO H3reversed.
EXECUTE.

RECODE H4 (1=5) (2=4) (3=3) (4=2) (5=1) INTO H4reversed.
EXECUTE.
```

Factor analysis

```
FACTOR
  /VARIABLES H1 H2 H3reversed H4reversed
  /MISSING LISTWISE
  /ANALYSIS H1 H2 H3reversed H4reversed
  /SELECT=Hedonism(1)
  /PRINT INITIAL EXTRACTION ROTATION
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES H1 H2 H3reversed H4reversed
  /MISSING LISTWISE
  /ANALYSIS H1 H2 H3reversed H4reversed
  /SELECT=Hedonism(5)
  /PRINT INITIAL EXTRACTION ROTATION
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES H1 H2 H3reversed H4reversed
  /MISSING LISTWISE
  /ANALYSIS H1 H2 H3reversed H4reversed
  /PRINT INITIAL EXTRACTION ROTATION
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES H1 H2 H3reversed H4reversed
  /MISSING LISTWISE
  /ANALYSIS H1 H2 H3reversed H4reversed
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES H1 H2 H3reversed H4reversed PU1 PU2 PU3 PU4 PU5
  /MISSING LISTWISE
  /ANALYSIS H1 H2 H3reversed H4reversed PU1 PU2 PU3 PU4 PU5
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES PU1 PU2 PU3 PU4 PU5
  /MISSING LISTWISE
  /ANALYSIS PU1 PU2 PU3 PU4 PU5
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.
```

```
FACTOR
  /VARIABLES T1 T2 T3 T4 T5 T6 T7
  /MISSING LISTWISE
  /ANALYSIS T1 T2 T3 T4 T5 T6 T7
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES NTH1 NTH2 NTH3 NTH4 NTH5
  /MISSING LISTWISE
  /ANALYSIS NTH1 NTH2 NTH3 NTH4 NTH5
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES R1 R2 R3 R4 R5 R6
  /MISSING LISTWISE
  /ANALYSIS R1 R2 R3 R4 R5 R6
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES SE1 SE2 SE3 SE4 SE5 SE6 SE7 SE8 SE9
  /MISSING LISTWISE
  /ANALYSIS SE1 SE2 SE3 SE4 SE5 SE6 SE7 SE8 SE9
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES PB1 PB2 PB3 PB4 PB5 PB6 PB7 PB8 PB9
  /MISSING LISTWISE
  /ANALYSIS PB1 PB2 PB3 PB4 PB5 PB6 PB7 PB8 PB9
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES PRP1 PRP2 PRP3
  /MISSING LISTWISE
  /ANALYSIS PRP1 PRP2 PRP3
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES SVA2 SVA3 SVA4
  /MISSING LISTWISE
  /ANALYSIS SVA2 SVA3 SVA4
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.

FACTOR
  /VARIABLES NTH1 NTH3 NTH4 NTH5
  /MISSING LISTWISE
  /ANALYSIS NTH1 NTH3 NTH4 NTH5
  /PRINT INITIAL KMO EXTRACTION ROTATION FSCORE
  /FORMAT SORT BLANK(.10)
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25)
  /ROTATION VARIMAX
  /METHOD=CORRELATION.
```

Reliability analysis

```
RELIABILITY
  /VARIABLES=PU1 PU2 PU3 PU4 PU5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=PerceivedUsefulness
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=T1 T2 T3 T4 T5 T6 T7
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=Trust
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=NTH1 NTH2 NTH3 NTH4 NTH5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.
```

```
DESCRIPTIVES VARIABLES=NothingToHide
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=R1 R2 R3 R4 R5 R6
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=Resignation
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=SE1 SE2 SE3 SE4 SE5 SE6 SE7 SE8 SE9
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=SelfEfficacy
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=PB1 PB2 PB3 PB4 PB5 PB6 PB7 PB8 PB9
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.
```

```
DESCRIPTIVES VARIABLES=ProtectiveBehaviour
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=PRP1 PRP2 PRP3
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=PrivacyRiskPerception
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=SVA2 SVA3 SVA4
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES=SmartphoneVA
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=R1 R2 R3
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES= Inconvenience
```

```
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=R4 R5 R6
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES= Powerlessness
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=SE1 SE2 SE3 SE4 SE5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES= PrivacySelfEfficacy
  /STATISTICS=MEAN STDDEV MIN MAX.

RELIABILITY
  /VARIABLES=SE6 SE7 SE8 SE9
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES= TechnicalSelfEfficacy
  /STATISTICS=MEAN STDDEV MIN MAX.
```

```
RELIABILITY
  /VARIABLES=NTH1 NTH3 NTH4 NTH5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=DESCRIPTIVE SCALE CORR
  /SUMMARY=TOTAL.

DESCRIPTIVES VARIABLES= NothingToHideBeliefs
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Compute scales

```
COMPUTE Hedonism= MEAN (H1 + H2 + H3reversed + H4reversed).
VARIABLE LABELS Hedonism 'Hedonism mean score'.
EXECUTE.

COMPUTE PerceivedUsefulness=MEAN(PU1, PU2, PU3, PU4, PU5).
VARIABLE LABELS PerceivedUsefulness 'Perceived Usefulness mean score'.
EXECUTE.

COMPUTE Trust=MEAN(T1, T2, T3, T4, T5, T6, T7).
VARIABLE LABELS Trust 'Trust in companies mean score'.
EXECUTE.

COMPUTE NothingToHide=MEAN(NTH1, NTH2, NTH3, NTH4, NTH5).
VARIABLE LABELS NothingToHide 'Nothing to hide mean score'.
EXECUTE.

COMPUTE Resignation=MEAN(R1, R2, R3, R4, R5, R6).
VARIABLE LABELS Resignation 'Resignation towards lack of privacy mean score'.
```

```
EXECUTE.

COMPUTE SelfEfficacy=MEAN(SE1, SE2, SE3, SE4, SE5, SE6, SE7, SE8, SE9).
VARIABLE LABELS SelfEfficacy 'Self-efficacy mean score'.
EXECUTE.

COMPUTE ProtectiveBehaviour=MEAN(PB1, PB2, PB3, PB4, PB5, PB6, PB7, PB8, PB9).
VARIABLE LABELS ProtectiveBehaviour 'Protective Behaviour mean score'.
EXECUTE.

COMPUTE PrivacyRiskPerception=MEAN(PRP1, PRP2, PRP3).
VARIABLE LABELS PrivacyRiskPerception 'Privacy Risk Perception mean score'.
EXECUTE.

COMPUTE SmartphoneVA=MEAN(SVA2, SVA3, SVA4).
VARIABLE LABELS SmartphoneVA 'Smartphone Voice Assistant Risk Perception mean score'.
EXECUTE.

COMPUTE Inconvenience=MEAN(R1, R2, R3).
VARIABLE LABELS Inconvenience 'Inconvenience mean score'.
EXECUTE.

COMPUTE Powerlessness=MEAN( R4, R5, R6).
VARIABLE LABELS Powerlessness 'Powerlessness mean score'.
EXECUTE.

COMPUTE PrivacySelfEfficacy=MEAN(SE1, SE2, SE3, SE4, SE5).
VARIABLE LABELS SelfEfficacy 'Self-efficacy mean score'.
EXECUTE.
```

```
COMPUTE TechnicalSelfEfficacy=MEAN(SE6, SE7, SE8, SE9).
VARIABLE LABELS SelfEfficacy 'Self-efficacy mean score'.
EXECUTE.

COMPUTE NothingToHideBeliefs=MEAN(NTH1, NTH3, NTH4, NTH5).
VARIABLE LABELS NothingToHide 'Nothing to hide beliefs mean score'.
EXECUTE.
```

Correlations

```
CORRELATIONS
  /VARIABLES=Hedonism PrivacyRiskPerception
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=Hedonism ProtectiveBehaviour
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=ProtectiveBehaviour PerceivedUsefulness
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=ProtectiveBehaviour Trust
  /PRINT=TWOTAIL NOSIG FULL
```

```
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= ProtectiveBehaviour NothingToHideBeliefs
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= ProtectiveBehaviour Inconvenience
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= ProtectiveBehaviour Powerlessness
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= ProtectiveBehaviour PrivacySelfEfficacy
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= ProtectiveBehaviour TechnicalSelfEfficacy
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
```

```
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception PerceivedUsefulness
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception Trust
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception NothingToHideBeliefs
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception Inconvenience
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception Powerlessness
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.
```

```
CORRELATIONS
  /VARIABLES= PrivacyRiskPerception PrivacySelfEfficacy
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacyRiskPerception TechnicalSelfEfficacy
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES=ProtectiveBehaviour PrivacyRiskPerception
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB1
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB2
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.
```

```
CORRELATIONS
  /VARIABLES=PrivacySelfEfficacy PB3
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB4
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB5
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB6
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
  /VARIABLES= PrivacySelfEfficacy PB7
  /PRINT=TWOTAIL NOSIG FULL
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.

CORRELATIONS
```

```
 /VARIABLES= PrivacySelfEfficacy PB8
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= PrivacySelfEfficacy PB9
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB1
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB2
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES=TechnicalSelfEfficacy PB3
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB4
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB5
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB6
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB7
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB8
 /PRINT=TWOTAIL NOSIG FULL
 /STATISTICS DESCRIPTIVES
 /MISSING=PAIRWISE.

CORRELATIONS
 /VARIABLES= TechnicalSelfEfficacy PB9
 /PRINT=TWOTAIL NOSIG FULL
```

```
  /STATISTICS DESCRIPTIVES
  /MISSING=PAIRWISE.
```

Regression analysis

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT PrivacyRiskPerception
  /METHOD=ENTER Trust NothingToHideBeliefs Inconvenience Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT ProtectiveBehaviour
  /METHOD=ENTER Trust NothingToHideBeliefs Inconvenience Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.

SPSSINC CREATE DUMMIES VARIABLE=OwnSmartSpeaker
ROOTNAME1=OwnSmartSpeakerNo
/OPTIONS ORDER=A USEVALUELABELS=YES USEML=YES OMITFIRST=NO.

USE ALL.
FILTER BY OwnSmartSpeakerNo_1.
EXECUTE.

REGRESSION
```

```
 /MISSING LISTWISE
 /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
 /CRITERIA=PIN(.05) POUT(.10)
 /NOORIGIN
 /DEPENDENT ProtectiveBehaviour
 /METHOD=ENTER Trust Inconvenience NothingToHideBeliefs Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.

REGRESSION
 /MISSING LISTWISE
 /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
 /CRITERIA=PIN(.05) POUT(.10)
 /NOORIGIN
 /DEPENDENT PrivacyRiskPerception
 /METHOD=ENTER Trust NothingToHideBeliefs Inconvenience Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.

USE ALL.
FILTER BY OwnSmartSpeakerNo_2.
EXECUTE.

REGRESSION
 /MISSING LISTWISE
 /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
 /CRITERIA=PIN(.05) POUT(.10)
 /NOORIGIN
 /DEPENDENT ProtectiveBehaviour
 /METHOD=ENTER Trust NothingToHideBeliefs Inconvenience Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.

REGRESSION
```

```
 /MISSING LISTWISE
 /STATISTICS COEFF OUTS CI(95) R ANOVA CHANGE
 /CRITERIA=PIN(.05) POUT(.10)
 /NOORIGIN
 /DEPENDENT PrivacyRiskPerception
 /METHOD=ENTER Trust NothingToHideBeliefs Inconvenience Powerlessness
PrivacySelfEfficacy TechnicalSelfEfficacy Hedonism PerceivedUsefulness.
```