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

Antonia Döring

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. Mariëlle Stel

Abstract

Smart homes, and especially smart speakers, have become more and more popular during the last years, bringing many advantages. Whereas, they also have some disadvantages including privacy risks for the user. The goal of this study was to gain more insight into antecedents of privacy risk perception and protective behaviours around smart speakers. For this, the study retested the factors of Hapke's (2023) study and extended the proposed model with the new factors, from looking at the Protection Motivation Theory (PMT) and the Theory of Planned Behaviour, for which new measures were developed. To identify the relationship between the variables an online survey was conducted that included Hapke's independent variables perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy and the dependent variable privacy risk perception. Additionally, the new independent variables, possession period of a smart speaker, injunctive norm, descriptive norm, and perceived effort needed to adjust privacy settings, as well as the dependent variable protective behaviours, were included. The sample consisted of 99 individuals between 18 and 65 years, mainly from Germany. The results reveal the strongest predictor for undermining privacy risk perception was trust in smart speaker companies. The strongest predictor diminishing protective behaviours was nothing to hide beliefs, while the strongest predictor increasing protective behaviours was social norm. These results can serve for more insight into the antecedents of privacy risk perception and protective behaviours while more research is needed to investigate protective behaviours more and develop interventions.

Keywords. smart speaker, privacy risk perception, protective behaviours

Introduction

During the past years, smart homes have been becoming more and more popular around the world. A smart home refers to devices and appliances in the home that are interconnected through the internet. It allows the user to access these devices through a smartphone or other devices (Hayes, 2023). Some examples of devices in smart homes are a smart thermostat, smart door locks, smart light bulbs, or a smart speaker. These devices can also learn the owner's schedule and make needed adjustments, such as control the light to reduce the electricity use. These devices are part of the internet of things (IoT) technology, which is a network of physical objects that collects and shares information (Hayes, 2023).

A smart speaker is a smart home device that has already been broadly adopted. In 2023, 40% of households in Germany, 23% of households in Spain, and 18% of households in France owned such a device (Borgeaud, 2023). Despite the popularity of smart speakers, owning such a device also poses a threat to privacy, including access to personal data, like bank details, or the collection of data, such as online activities by companies. Besides that, individuals often fail to take preventative actions. The goal of this present study is therefore to build further on the work of Hapke (2023) and try to understand factors that undermine privacy risk perception and protective behaviour concerning smart speakers. This present study retests and extends the proposed model by Hapke with additional factors from looking at the Protection Motivation Theory and the Theory of Planned Behaviour.

Theoretical Background

A smart speaker, also known as a personal voice assistant (PVA), has an integrated microphone that enables voice interaction with a virtual assistant, which is a piece of software that listens to the user speech, recognizes commands, and questions, and communicates with other services or the user, when needed. Some other functions a smart speaker has are playing music, making phone calls, conducting online searches, like the weather forecast, or features for managing lists. If a third-party software is installed, additional features might be enabled. If a household, for example, uses a smart speaker and smart bulbs, the smart speaker can be used to turn the lights on and off via a voice command. To activate a smart speaker like Amazon Echo or Google Home a wake-up phrase is needed. In order to recognize the wake-up phrase the speaker's microphone is always on and listening (Lareo, 2019).

Despite these aforementioned advantages the always-on feature threatens the user's privacy and raises concerns about the information that is gathered, how it might be used, and how to protect it (Lau et al., 2018). Information gathered by the smart speaker include information about the user's contacts, calendars, voice searches, browsing history, and past online purchases (Gardiner, 2018). In addition, about 50% of smart device owners that participated in a study around privacy expressed mistrust in their digital assistant and felt like it jeopardized their privacy, through their passive listening (Charlton & Charlton, 2018). Next to that, companies like Amazon or Google can use the stored information and voice recordings for more targeted advertisement through creating user profiles. This is a concern because consumers may worry about other ways in which their data is used, and it may be viewed as intrusive and uncomfortable, or give a feeling of being watched all the time (Lutz & Newlands, 2021). Another concern for privacy risk are hackers, or other third parties, that can access the stored information of the speaker and purchase things online, use it for surveillance, or use other stored information. Additionally, the government can use the recordings from smart speakers in court, as in the US for example, the recorded and saved data is subject to subpoena (Lutz & Newlands, 2021).

Nevertheless, studies have indicated that consumers often fail to recognise the privacy risks. According to Lau et al. (2018), while consumers think a smart speaker is useful, they know very little about the scope of data colleting and its potential for abuse. Thus, while consumers are only slightly concerned about accidental activations of the smart speaker, eavesdropping, or data misuse (Marks, 2022), experts perceive these risks as greater and emphasize the policy related aspects of these risks, like lack of transparency (the user does not know the extent to which their data is collected by the companies) and control from manufacturers (privacy controls from the manufacturer are not tailored to the need of the users) (Ahmed, 2023). Another study by McReynolds et al. (2017) found that users often trust a brand without understanding the full privacy consequences of their interactions with the device. Furthermore, according to Zeng et al. (2017) lack of concern about privacy and security issues can also be attributed to feeling like the users are not a meaningful target, have nothing to hide, and users think they have taken enough privacy securing steps.

The study of Hapke (2023) aimed to gain insights on antecedents of risk perception and protective behaviour concerning smart speakers, while mostly relying on insights from interview studies. The six factors used in that study were, *perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy.* Whereas, during the factor analysis two additional factors were found. First, the analysis revealed that the measure *resignation towards lack of privacy* consists of two subdimensions. Where one mostly reflects resignation towards lack of privacy and another, labelled *powerlessness*. Secondly, *privacy self-efficacy* also consists of two subdimension. One being privacy self-efficacy and the second, labelled *security self-efficacy*.

In line with the expected findings of Hapke's (2023) study, the results of Hapke's Pearson's correlation show a positive relationship between *privacy risk perception* and *protective behaviour*, which means smart speaker users that have a higher privacy risk perception engage in more protective behaviours around their smart speaker. Next to that, also in line with the expected results, a negative relationship between the dependent factor privacy risk perception and each of the independent factors *perceived usefulness, perceived enjoyableness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy*, and *privacy self-efficacy,* was found. This indicates, the more useful and enjoyable user's think their smart speaker is, the more trust they have in the smart speaker company, the more they think they have nothing to hide, resign towards their perceived lack of privacy, and have high levels of privacy self-efficacy, the fewer privacy risks they perceive. There was also a negative relationship between the dependent factor protective behaviour and the independent factors *perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide belief,* and *resignation towards lack of privacy*. These relationships with protective behaviour all indicate less engagement in protective behaviours, if the user perceives high usefulness and enjoyableness, the more trust they have in the smart speaker company, the more they think they have nothing to hide, and resign towards their perceived lack of privacy. Different from the expected results was the negative relationship *between privacy self-efficacy* and *protective behaviours*. This also indicates less engagement in protective behaviours if the user has high *privacy self-efficacy*. Furthermore, the measure for the factor *resignation towards lack of privacy* was found to also measure a second distinct factor, labelled *powerlessness*. The factor *powerlessness* was then additionally tested. It revealed a significant positive relation between *powerlessness* and *privacy risk perception*, however a non-significant relation between *powerlessness* and *protective behaviour.* Moreover, the factor *privacy self-efficacy* was also found to measure a second distinct construct, which was labelled *security self-efficacy*. *Security self-efficacy* revealed a significant negative correlation towards *privacy risk perception* and a non-significant relationship towards *protective behaviour*.

In addition, Hapke distinguished between smart speaker owners and non-owners during the regression analysis. The results showed that for owners of a smart speaker *trust in smart speaker companies* and *privacy self-efficacy* undermine privacy risk perception. Next to that, *protective behaviours* are supported by *security self-efficacy.* In contrast, for non-owners of a smart speaker the privacy risk perception increased with the factor *powerlessness,* while it is diminished by the factors *perceived enjoyableness, resignation towards lack of privacy,* and *privacy self-efficacy.* Also, engagement in protective behaviours for non-smart speaker owners was impaired by *resignation towards lack of privacy* and *perceived enjoyableness.*

Building further on Hapke (2023), this present study is trying to understand factors that undermine privacy risk perception and protective behaviour concerning smart speakers. While the work by Hapke was very insightful, it only included factors that were identified through reviewing qualitative literature. The current study extends the number of predictors by looking at important theories in relation to privacy risk perception and protective behaviours. These theories include the Protection Motivation Theory (PMT) and the Theory of Planned Behaviour (TPB), from which it became apparent that four factors were missing. At the same time this present study retests Hapke's work, including the eight factors that were found.

The first framework used within this current study for understanding how people assess dangers and choose to take preventative actions, offers the Protection Motivation Theory (PMT). PMT states that how a person defends themselves against perceived danger is based on threat appraisal and coping appraisal. Threat appraisal includes the components perceived severity and perceived vulnerability. Coping appraisal includes perceived response efficacy and perceived self-efficacy (Rogers, 1975). That means, the individual is likely to adopt protective behaviours if they think the threat is serious enough and when they think they are capable of handling the actions to reduce the threat. That means, both threat appraisal and coping appraisal are high (Hedayati et al., 2023). In the study by Hapke (2023) it is already explained that threat appraisal is measured by the user's privacy risk perception of smart speakers and precedes possible protective behaviours, which is also true for this current study. However, what was not included is that, according to literature around threat appraisal in the context of smart speakers, users' privacy risk perception and engagement in protective behaviours may be influenced by the length of time they own a smart speaker (Ebbers & Karaboga, 2023). A short possession period of a smart speaker could influence threat appraisal, specifically perceived severity and vulnerability, as individuals are more aware and think more about the potential threats when the time, they have owned a smart speaker, is short. This would also promote protective behaviour. As the possession period of the smart speaker increases, the user becomes more familiar and comfortable with their smart speaker. Hence, their perceived vulnerability decreases and their perceived control (coping appraisal) increases. Thus, their protective measures might decrease (Dupuis & Ebenezer, 2018). On the other hand, as the possession period of a smart speaker increases, the user might also learn more about privacy measures and threats about their device, which could further increase their perceived severity and perceived vulnerability. This in turn could help them in taking more action around protective behaviours (Ebbers & Karaboga, 2023). Thus, the *possession period* of a smart speaker seems to be an important factor in privacy risk perception and protective behaviour and might therefore be a good extension to the model of Hapke (2023).

Next to that, the Theory of Planned Behaviour (TPB) predicts a person's intention to engage in an action which is determined by their attitude, their subjective norm, and their perceived behavioural control. The goal of this theory is to be able to explain the behaviours that a person can control themselves (Ajzen, 1987). Social norms in the context of TPB are a part of subjective norms. Social norms are actual expectations for the appropriate behaviour and influence subjective norm (Klein, 2005). Social norms can be divided into injunctive norms and descriptive norms. Injunctive norms are what people think is accepted or rejected by others, whereas descriptive norms are what people think others actually do or not do (Hedeman, 2021). With respect to smart speakers, social norms might have an effect on how people perceive and engage in protective behaviours. If people perceive other people to take protective action and to find protective action around smart speakers important, then it is more likely that they take on more protective actions oneself. Whereas if users think others do not take precautionary actions, they are also less inclined to do so (Lutz & Newlands, 2021). The study by Ebbers and Karaboga (2023) found that smart speaker users' adoption of privacy protective behaviours depends on social norms. This present study wants to therefore find out if the users' engagement in protective behaviours may be influenced by separating social norms into injunctive norms and descriptive norms as both motivate behaviour in a different way. Therefore, *injunctive*, and *descriptive norms* seem to be a good extension to the model of Hapke (2023).

Furthermore, perceived behavioural control means that the person assesses how easy or difficult it is to carry out the specific behaviour based on different situations and circumstances. Their perceived control is based on external factors, such as resources available to them and obstacles, and also on internal factors, such as skills and knowledge (Ajzen, 2002). The more a person perceives control over the situation and the intended behaviour they would like to follow, the more likely it is for them to actually carry out this behaviour. One factor for control includes effort and the less effort a person perceives a behaviour to be, the more control they think they have over this behaviour. This in turn means they are more likely to carry out this behaviour (Sommer, 2011). In the context of this present study, the factor *perceived effort needed to adjust privacy settings* can be used and described as the work a smart speaker user must put in, to carry out privacy protective behaviours. To engage in more protective behaviour around smart speakers, a person needs to think the effort it takes to delete their voice recordings, change privacy settings, or muting the device, is low (Kang, & Oh, 2021). However, if they see these actions as effortful, they are less likely to engage in protective behaviour (Liu et al., 2021). Hence, the variable *perceived effort needed to adjust privacy settings* seems to have an influence on the users' engagement in privacy protective behaviour towards a smart speaker and is thus also a good extension to the model of Hapke (2023).

To mitigate the privacy risks, experts have identified some risk protecting behaviours users should engage in. Some of these are muting the smart speaker before talking about sensitive information while in the same room as the device or deleting the recordings. Hapke also already included various behaviours in the study, including muting, unplugging, or covering the smart speaker, moderating conversations around it, reviewing audio logs, and not placing the smart speaker in privacy sensitive rooms. Next to these, more behaviours seem to be relevant. The study by Lutz and Newland (2021) identified additional protective behaviours, which seem to be relevant for this present study as well. These include, for example, reviewing which applications have access to the smart speaker, restrict the amount of data the device is allowed to collect, and deleting the smart speaker recordings.

However, research has shown that some users are unaware of existing protection features, do not know how to access these features, or avoid them on purpose even though they might express some worry about their privacy (Huang et al., 2020). Thus, it is important to identify underlying factors that undermine or influence privacy risk perception and the engagement in protective behaviours. This in turn is beneficial to develop interventions that are better targeted at individuals to raise awareness of the privacy risks and increase engagement in protective behaviours.

Current Study

Following from the literature review and insights in PMT and TPB the factors, *perceived effort needed to adjust privacy settings, injunctive norm*, *descriptive norm,* and *possession period* were identified and suggested as additional antecedents of privacy risk perception and protective behaviour in regard to smart speakers. Thus, the goal of this study is to retest the factors of Hapke (2023), to investigate if similar findings are found when using the same factors and to extend the proposed model by including the factors *powerlessness* and *security self-efficacy* based on Hapke's findings. Furthermore, the model is extended by the newly suggested factors, from this present study, to gain insights in the relationship with perceived risk and protective behaviour (see Figure 1). Similar findings regarding the factors that Hapke already used in her study are expected because the effects are assumed to be consistent across different samples. Next to that, the same hypotheses as in Hapke's study are used, with a difference of an expected relationship in the self-efficacy hypotheses regarding protective behaviour, after the findings in Hapke's study revealed a negative correlation. These following hypotheses are formulated:

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

H2: Perceived enjoyableness has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H3: Perceived Usefulness has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H4: Trust in smart speaker companies has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H5: Nothing to hide beliefs has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H6: Resignation towards lack of privacy has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H7: Powerlessness has a positive effect on (a) privacy risk perception and (b) protective behaviours.

H8: Privacy self-efficacy has a negative effect on (a) privacy risk perception and (b) protective behaviour.

H9: Security self-efficacy has a negative effect on (a) privacy risk perception and a positive effect on (b) protective behaviour.

H10: Possession period of smart speaker owners has a negative effect on (a) risk perception (b)protective behaviour.

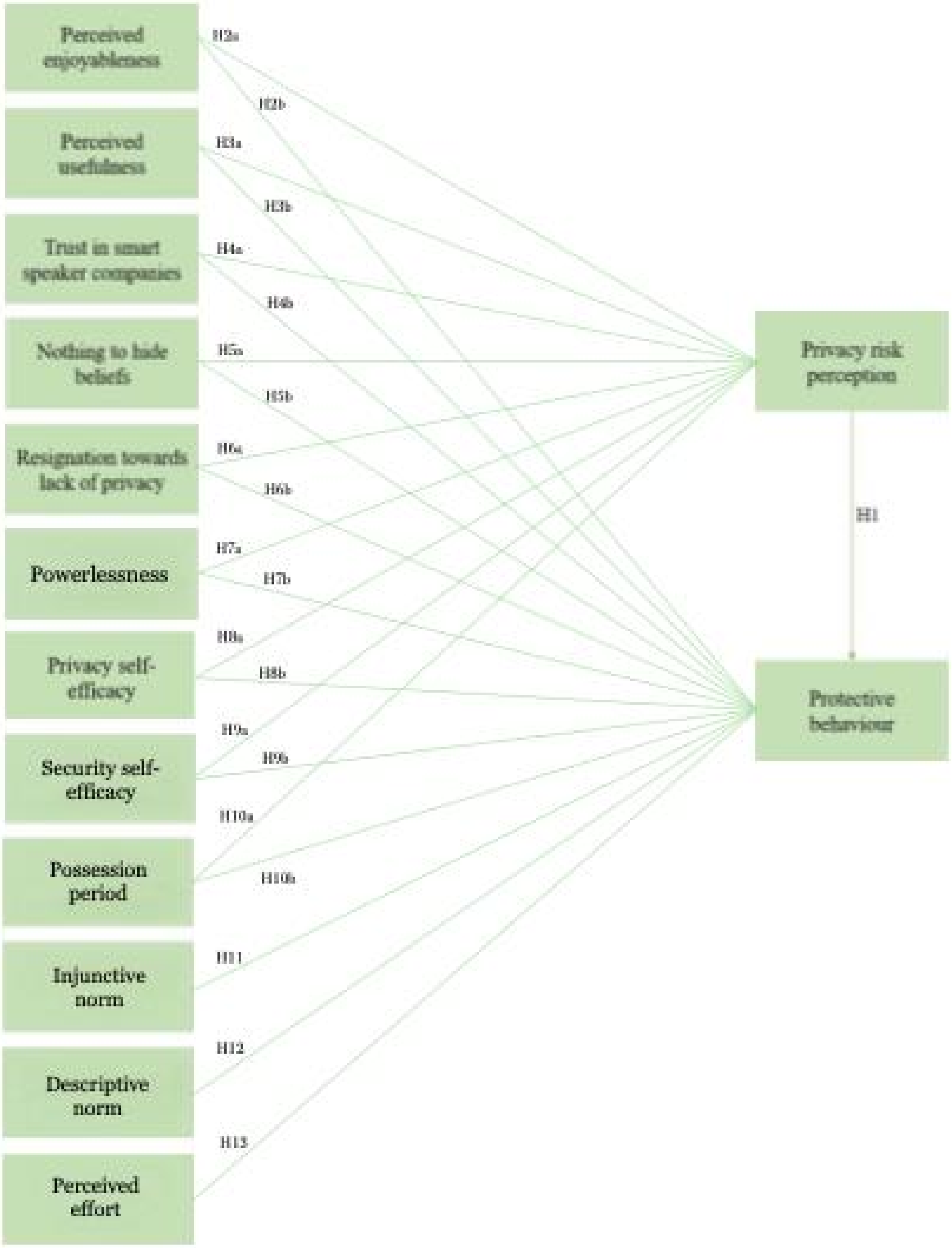
H11: Injunctive social norm has a positive effect on protective behaviour.

H12: Descriptive social norm has a positive effect on protective behaviour.

H13: Perceived effort needed to adjust privacy settings has a negative effect on protective behaviour.

Figure 1

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



Method

Participants

Participants could enter the study via the online platform SONA, which is a participant recruitment tool for students used by the University of Twente and through social media platforms, such as WhatsApp and Instagram. The survey was active from the 19th of April

2024 until the 10th of May 2024 and was initially comprised of a sample of 119 participants. However, 20 participants were excluded from the study because they did not pass the attention checks. The final sample was comprised of 99 participants between the ages of 18 and 65 (*M* =29.5, *SD* = 12.4), 34 participants owned a smart speaker and 65 did not. From the participants that did not own a smart speaker, 33 would install a smart speaker if it was gifted to them however, only 28 would use it. The majority of participants was female including 60 participants, 37 participants were male, one non-binary, and one preferred not to say. The nationalities in this sample were mostly German (80), some Dutch (7), Spanish (3), Mexican (2), Indian (2), Italian (1), Turkish (1), Ukrainian (1), Lithuanian (1), and Lebanese (1). Moreover, 36 participants highest completed educational level was secondary school, 24 had completed a bachelor's degree, 24 participants already had professional education, 13 had already obtained a master's degree and 1 participant had a PhD. The study was approved by the Behavioural Management and Social Sciences Ethics Committee, and all participants were informed about the procedure and the use of their data. They gave informed consent online prior to taking part in the study and participated voluntarily.

Design and Procedure

For creating the online study, the online survey tool Qualtrics was used. To make sure that people with different languages could participate, the study was conducted in English. The questionnaire included different questions depending on whether participants owned a smart speaker or did not. If the participants owned a smart speaker, they were asked to answer the questionnaire while thinking about their behaviour towards it in the past three months. If participants did not own a smart speaker, they were asked to imagine their behaviour towards a smart speaker that was gifted to them. Depending on this they were directed to differently formulated questions, fitting the scenario. The entire questionnaire can be found in Appendix A. At the start of the study, the participants were welcomed, and the purpose of the study was briefly explained. This was followed by an informed consent sheet they had to fill out. It included a short description of the purpose and procedure of the study, participant rights, risks and benefits, and information about anonymity and confidentiality. Following that, the participants had to complete questions that included general demographics such as gender, age, and nationality. Next, they answered questions regarding their values, which was followed by a definition of a smart speaker and the control question, whether the participants own a smart speaker or not. This question served as basis for the comparison between smart speaker owners and non-owners and to be directed to the right type of questions in the questionnaire. After that, 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, perceived effort needed to adjust privacy settings, injunctive and descriptive norms, possession period, protective behaviour, and privacy risk perception in random order to minimise any order effects. During the questionnaire two attention checks were used. For these the task was that participants had to select the answer "Strongly Agree" to see if they were still mindfully reading and answering the questions. At the end of the survey, the participants were debriefed and thanked for their participation.

Materials

Existing Items

The items used to measure the variables *perceived enjoyableness* (*M*= 3.04, *SD*=0.94, *α=.81), perceived usefulness* (*M*= 2.55, *SD*=0.98, *α=.89), trust in smart speaker companies* (*M*= 2.26, *SD*=0.73, *α=.84), nothing to hide beliefs* (*M*= 2.92, *SD*=0.79, *α=.67), resignation towards lack of privacy* (*M*= 2.82, *SD*=0.76, *α=.56), powerlessness (M*= 3.45, *SD*=0.79, *α=.55), privacy self-efficacy* (*M*= 2.35, *SD*=0.76, *α=.81)*, security self-efficacy (*M*= 2.24, *SD*=0.87, *α=.79*), and *privacy risk perception* (*M*= 3.21, *SD*=0.98, *α* =.88) were taken from Hapke's study (2023). Those items were either taken from already existing questionnaires and adapted to fit the context of smart speakers, or self-generated by Hapke, based on literature findings (see Hapke's study, method section, for a more detailed explanation). However, in this present study, for some items the formulation had to be changed to the past tense, to fit the context of the scenario for smart speaker owners (see precise formulation in Appendix A). Most items were measured on a 5-point Likert scale, ranging from 1 "strongly disagree" to 5 "strongly agree" (for perceived enjoyableness, perceived usefulness, trust in smart speaker companies, nothing to hide beliefs, resignation towards lack of privacy, and privacy self-efficacy), or 1 "none at all" to 5 "being a great deal" (for privacy risk perception).

Newly created Items

The newly added variables, *perceived effort needed to adjust privacy settings, injunctive social norm, descriptive social norm, and possession period,* in this current study, were measured by items that were adapted from existing research and some newly created, based on knowledge from qualitative studies. Moreover, the items measuring privacy protective behaviour from Hapke's (2023) study were changed, to be able to measure this factor in more depth.

Perceived Effort needed to adjust privacy settings. The five items regarding effortfulness were inspired by the effortful control scale for adults (Allan & Lonigan, 2011) and then self-generated. The items assess how effortful smart speaker users find engaging in risk protective behaviour. Examples of these items are “How much effort does it take you to adjust your privacy settings on your smart speaker?” and "How much effort does it take you to seek help or guidance from others to protect your privacy on your smart speaker?”. All items were measured on a 5-point Likert scale, ranging from 1 “it takes a little effort” to 5 “it takes a lot of effort”. The scale consists of the average of these items (*M*=3.08, *SD*=0.87, *α*=0.80). The complete factor loadings for the independent variables can be found in appendix B.

Social norm. The items of social norm were measured with injunctive norm (four items) and descriptive norm (three items) and adapted from Venkatesh (2012). One examples for injunctive social norm is “I think that people whose opinions I value, would support me using privacy protective behaviours with a smart speaker”. An example for descriptive social norm is “People that are important to me generally take privacy protective actions around smart devices”. See table 1 for the formulations of the other items. All items were measured on a 5-point Likert scale, ranging from 1 “strongly disagree” to 5 “strongly agree”.

The factor analysis revealed *injunctive* and *descriptive norm* were on the same dimension, which led to the combination of these factors into one, called social norm. The factor loadings can be seen in table 1. The scale for social norm consists of the average of these items (*M*= 2.91, *SD*=0.76, *α*=0.81). However, item one revealed a very low factor loading of .23 and was therefore omitted from the analysis, the final scale consisted of the remaining six items (*M*= 2.77, *SD*=0.83, *α*=0.83).

Table 1

The Items Measuring Social Norms and Their Factor Loadings

Item	Factor Loading
“I think that people whose opinions I value, would support me using privacy protective behaviour with a smart speaker”.	.23
“My family members and friends would recommend me to adjust my smart speaker settings to enhance my privacy”.	.54
“People in my immediate surrounding think that privacy protecting behaviour around their smart speaker is important”.	.82
"I think people in my surrounding find it important to comply with the privacy recommendations provided by experts when using smart speakers".	.56

“People that are important to me generally take privacy protective actions around smart devices”.	.81
“My friends and family generally put effort in limiting data-collection from smart devices”.	.67
“People close to me generally put make sure that their smart devices have restricted privacy settings”.	.65

Possession period. To measure the influence of the possession period the one item “For how long have you been using your smart speaker device?” is used. This item was self-generated and measured with a scale from “less than 1 month”, “2-3 months”, “4 months to 1 year”, “1-2 years”, and “more that 2 years”.

Privacy Protective Behaviours. To measure the variable privacy protective behaviour the items were taken from Lutz and Newland (2021) while the following items have been omitted. First, the item covering the smart speaker microphone. This is not an effective way to protect one’s privacy. While it might interfere with the functionality of the smart speaker, it does not create a faraday cage. Hence, the smart speaker might still be able to pick up what has been said (Ebbers & Karaboga, 2023). Secondly, giving misleading information to the smart speaker. This is unrealistic because it reduces the usefulness of the smart speaker and is impractical for the user. They have to continuously change the context and information they are talking about (Ebbers & Karaboga, 2023). Lastly, restricting guest access to the smart speaker. It is unclear for whom it is a privacy risk, as it does not give the owner any benefits or improves privacy protection, besides limiting the use of the smart speaker for guests. Hence, smart speaker would still be able to listen to everything that is said and therefore does not give any protection (Ebbers & Karaboga, 2023). The measure for privacy protective behaviours also included the non-overlapping items from Hapke (2023). In total this measure had 19 items which were measured on a 5-point Likert scale, ranging from 1 “extremely unlikely” to 5 “extremely likely”. Additionally, these items had different formulations for smart speaker owners and non-owners to fit each scenario. An example item is” I turned off the smart speaker when I was having serious/private conversations”. For the factor analysis only item one to 14 were used from the smart speaker owner and non-owner scenario. This was done to be able to combine these items and do one factor analysis together, with both scenarios. The factor analysis revealed two underlying dimensions for protective behaviours. This was based on the criterion of eigenvalues being over one which showed two components were greater than one and the scree plot which showed a drop of eigenvalues after the second factor. This indicated two factors contributed to the variance of items (Table 2 and Appendix

C). One factor relates more to the meaning of physical protective behaviours, consisting of item one to five and 11 to 14. While the second factor relates more to the meaning of online data handling as protective behaviour, including item six to ten. To decide which item belongs to which factor the relative strengths of each item was used. The items were put with the underlying factor for which their factor loading was highest, as this means it better predicts the underlying factor. Next to that, because all these items measure some kind of protective behaviour, the results are still called connected to the hypotheses, as the hypotheses were extended to both factors. To sum this up, the overall protective behaviour variable was calculated by averaging all 14 items (*M*=2.56, *SD*=1.20, *α*=0.95). Then the subscales were calculated by averaging the items for physical protective behaviour (*M*=2.34, *SD*=1.20, *α*=0.94) and averaging the items for online data handling protective behaviour (*M*=2.96, *SD*=1.38, *α*=0.93).

Table 2

The Items Measuring Protective Behaviours and Their Factor Loadings

Item	Factor Loading	
1. I turned off the smart speaker when I was not using it	.73	.29
2. I unplugged the smart speaker when I was not using it	.74	.30
3. I unplugged the smart speaker when I was having serious/private conversations	.81	.30
4. I turned off the smart speaker when I was having serious/private conversations	.82	.42
5. I muted the smart speakers microphone when I was not using it	.74	.48
6. I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account	.34	.81
7. I reviewed which applications/services have access to my smart speaker	.35	.72
8. I restricted the amount of data that the device is allowed to collect through the smart speaker settings	.27	.83
9. I deleted my smart speaker recordings	.49	.71
10. In the app I deleted sensitive information that the smart speaker stored about me.	.55	.72
11. I spoke very quietly around the smart speaker in case I did not want to be recorded	.56	.31

12. I moderated my language around the smart speaker so that it didn't record private matters, even if accidentally	.71	.39
13. I avoided sensitive/private conversations around the smart speaker	.74	.48
14. When I had a visitor, I informed them that I have a smart speaker	.51	.42

Data Analysis

The statistical software RStudio (version 1.4.1717) was used to analyse the data. The demographic data was analysed in terms of descriptive statistics and frequencies. Furthermore, to assess the newly created measurement scales, *social norm, perceived effort needed to adjust privacy settings*, and *protective behaviours*, the data of the smart speaker owner and non-owner scenario was first merged, for each scale separately. After that, descriptive statistics, factor analysis, and reliability analysis (Cronbach's alpha) were used for each scale. This was also done with the existing measures from Hapke (2023), to check their reliability again. The results of this were already shown in the method section. To measure the different hypotheses first composite scores were calculated for every factor, also including the factors of Hapke (2023). This was done by averaging the item scores belonging to each scale. The composite scores were then used for Pearson correlation. Moreover, for the multiple regression analysis the composite scores of the smart speaker owner and non-owner scenario were merged to create one combined dataset. The multiple regression analysis was then used for hypothesis one to seven and nine to eleven. Hypothesis eight was measured with an Analysis of Variance (ANOVA). The complete code can be found in appendix F.

Results

Hypothesis Testing

To calculate the Pearson's correlation first the assumptions were checked, and then Pearson's Correlation was done with each predictor. The coefficients with their related p-values, for the whole sample, can be found in Table 3, also indicating their significance. Next to that, an explorative analysis was done separating between smart speaker owners and non-owners.

Table 3

Pearson's Correlation with the whole sample, between Privacy Risk Perception, Physical Protective Behaviour, and Online Data Handling Behaviour with the Independent Variables

	Privacy Risk Perception		Physical Protective Behaviour		Online Data Handling Protective Behaviours	
	r	*p*	*r*	*p*	*r*	*p*
Privacy Risk Perception			**.42**	**<.001**	**.38**	**<.001**
Perceived Enjoyableness	**-.32**	**<.001**	**-.35**	**<.001**	**-.29**	**.003**
Perceived Usefulness	**-.26**	**.007**	**-.23**	**.021**	**-.23**	**.021**
Trust in Companies	**-.41**	**<.001**	-.13	.173	-.13	.169
Nothing to Hide	**-.29**	**.003**	**-.30**	**.002**	**-.33**	**<.001**
Resignation Towards Lack of Privacy	-.17	.086	**-.31**	**<.001**	**-.42**	**<.001**
Powerlessness	.05	.572	-.09	.355	-.15	.117
Privacy Self-Efficacy	-.13	.117	.08	.397	.14	.161
Security Self-Efficacy	-.09	.339	.16	.098	**.26**	**.008**
Social Norm			**.36**	**<.001**	**.37**	**<.001**
Perceived Effort Needed to Adjust Privacy Settings			-.02	.786	-.05	.623

Note. All significant correlations are marked in bold. (*n* = 99)

Hypothesis 1. In line with hypothesis 1, the analysis showed a positive and significant correlation between privacy risk perception and physical protective behaviours as well as online data handling for protective behaviours.

Hypothesis 2. In line with hypothesis 2a and 2b, the analysis showed a negative and significant correlation between perceived enjoyableness and privacy risk perception as well as between perceived enjoyableness and physical protective behaviours and online data handling protective behaviours.

Hypothesis 3. In line with hypothesis 3a and 3b, the analysis showed a negative and significant correlation between perceived usefulness and privacy risk perception as well as physical and online data handling protective behaviours.

Hypothesis 4. In line with hypothesis 4a, the analysis showed a negative and significant correlation between trust in companies and privacy risk perception. Also, in line with hypothesis 4b the analysis showed a negative but non-significant correlation between trust in companies and physical protective behaviours as well as online data handling protective behaviours.

Hypothesis 5. In line with hypothesis 5a and 5b, the analysis showed a significant negative correlation for nothing to hide beliefs with privacy risk perception as well as physical and online data handling protective behaviours.

Hypothesis 6. In line with hypothesis 6a, a marginally significant negative correlation was found between resignation towards lack of privacy and privacy risk perception. Furthermore, in line with hypothesis 6b, a significant negative correlation was found between resignation towards lack of privacy and physical protective behaviours, as well as online data handling protective behaviours.

Hypothesis 7. In line with hypothesis 7a, the analysis revealed a positive but non-significant correlation was found between powerlessness and privacy risk perception. In contrast to hypothesis 7b, a negative but non-significant correlation was found between powerlessness and physical protective behaviours as well as online data handling protective behaviours.

Hypothesis 8. In line with hypothesis 8a, the analysis showed a negative but non-significant correlation between privacy self-efficacy and privacy risk perception. Unlike hypothesis 7b, the analysis revealed a positive but non-significant correlation between privacy self-efficacy and physical as well as online data handling protective behaviours.

Hypothesis 9. In line with hypothesis 9a, the analysis revealed a negative but non-significant correlation between security self-efficacy and privacy risk perception. Also, in line with hypothesis 9b the analysis revealed a marginally significant positive correlation between security self-efficacy and physical protective behaviours as well as a significant correlation with online data handling protective behaviours.

Hypothesis 11 & 12. Injunctive and Descriptive norm were analysed together as one factor. In line with hypothesis 10 and 11, the analysis revealed a positive and significant correlation between social norm and physical as well as online data handling protective behaviours. This result indicates that the more individuals think certain protective behaviours are accepted and used by others the more likely they will practice them.

Hypothesis 13. In line with hypothesis 13, the analysis showed a negative but non-significant correlation between perceived effort needed to adjust privacy settings and physical as well as online data handling protective behaviours.

Explorative Analysis Hypothesis Testing

To see if the Pearson's Correlation would show any differences when calculated separately for smart speaker owners and non-owners, the analysis was calculated a second time. The complete results including the correlation table can be found in appendix D.

When looking at smart speaker owners none of the predictor variables had a significant effect on privacy risk perception. However, when looking at smart speaker non-owners the analysis revealed a significant negative effect for privacy risk perception with the independent variables perceived enjoyableness, trust in smart speaker companies, and nothing to hide beliefs. When looking at smart speaker owners and the two protective behavioural factors the variable resignation towards lack of privacy had a significant negative effect on both with a larger effect size for online data handling protective behaviours. Next to that, powerlessness and security self-efficacy showed a significant effect only for online data handling protective behaviours. Compared to the non-owner condition, nothing to hide beliefs and social norm significantly explained the two behavioural factors, with a larger effect size for physical protective behaviours. Next to that, privacy risk perception, and resignation towards lack of privacy also explained the two behavioural factors, with a larger effect size for online data handling protective behaviours. Furthermore, perceived enjoyableness showed a significant negative effect for physical protective behaviours. Moreover, security self-efficacy showed a significant positive effect for online data handling protective behaviours. Finally, privacy self-efficacy and perceived effort needed to adjust privacy settings showed a marginally significant positive effect for online data handling protective behaviours.

Analysis of Variance (ANOVA)

An analysis of variance was conducted to assess the effect of possession period on privacy risk perception, physical protective behaviours, and online data handling protective behaviours. 34 participants of this study owned a smart speaker. From these two owned it less than a month, one owned it two to three month, three owned it for 4 months to one year, six owned it for one to two years, and 22 owned it for more than two years. The results in table 4 indicate that the variable possession period did not have a significant effect on privacy risk perception. Next to that, Figure 2 shows the average risk perception by how long a smart speaker user has owned their smart speaker.

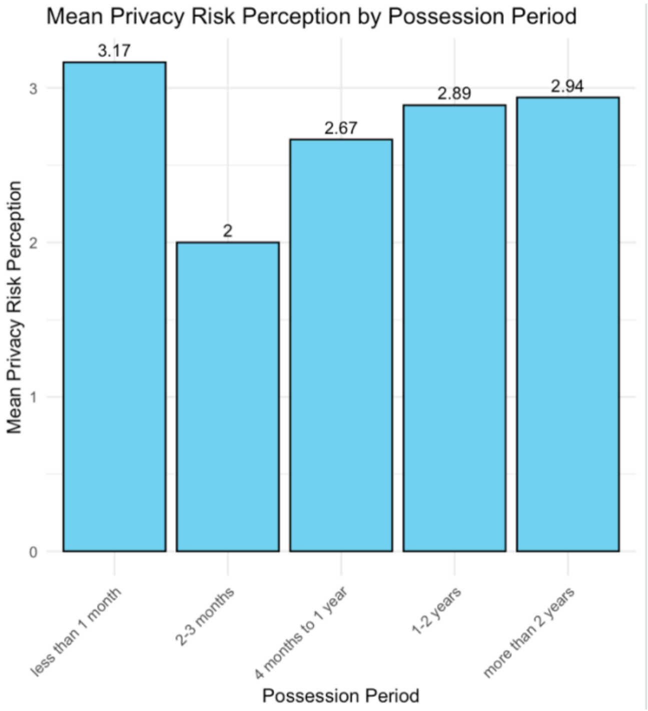
Table 4

ANOVA Results for Possession Period with Privacy Risk Perception

	df	*SS*	*MS*	*F*	*p*
Possession Period	4	1.14	.28	.41	.794
Residuals	29	19.9	.68	N/A	N/A

Figure 2

Mean Privacy Risk Perception by Possession Period



Similarly, table 5 shows that possession period did not have a significant effect on protective behaviours. Figure 3 shows the average engagement in physical protective behaviours by how long a smart speaker user has owned their smart speaker.

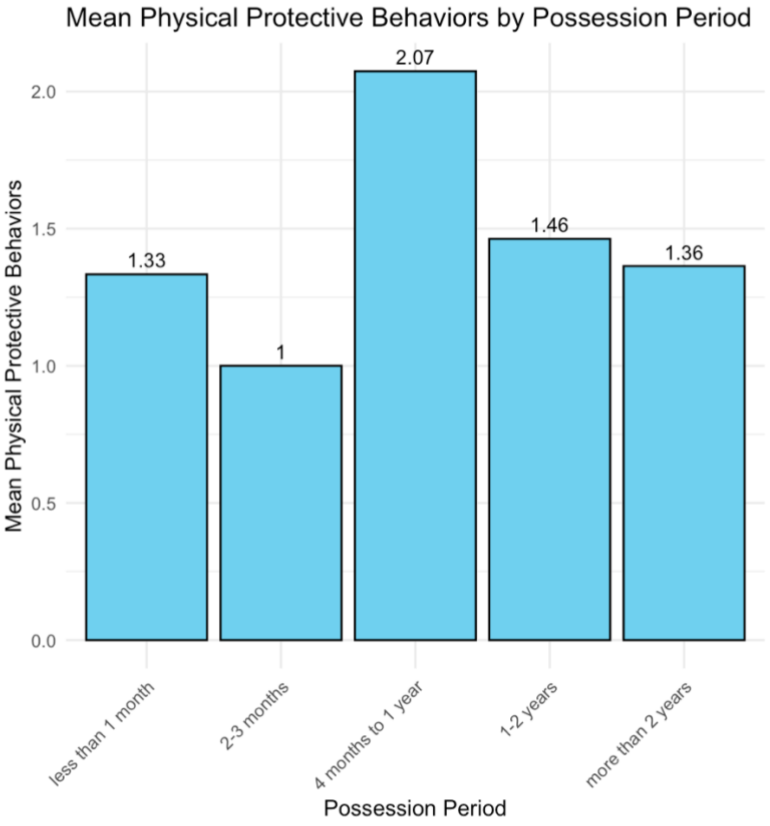
Table 5

ANOVA Results for Possession Period with Physical Protective Behaviours

	df	*SS*	*MS*	*F*	*p*
Possession Period	4	1.55	.38	.70	.596
Residuals	29	15.99	.55	N/A	N/A

Figure 3

Mean Physical Protective Behaviour by Possession Period



Lastly, table 6 shows that possession period does not have a significant effect on online data handling protective behaviours. Furthermore, figure 4 shows the average engagement in online data handling protective behaviours by how long a smart speaker user has owned their smart speaker.

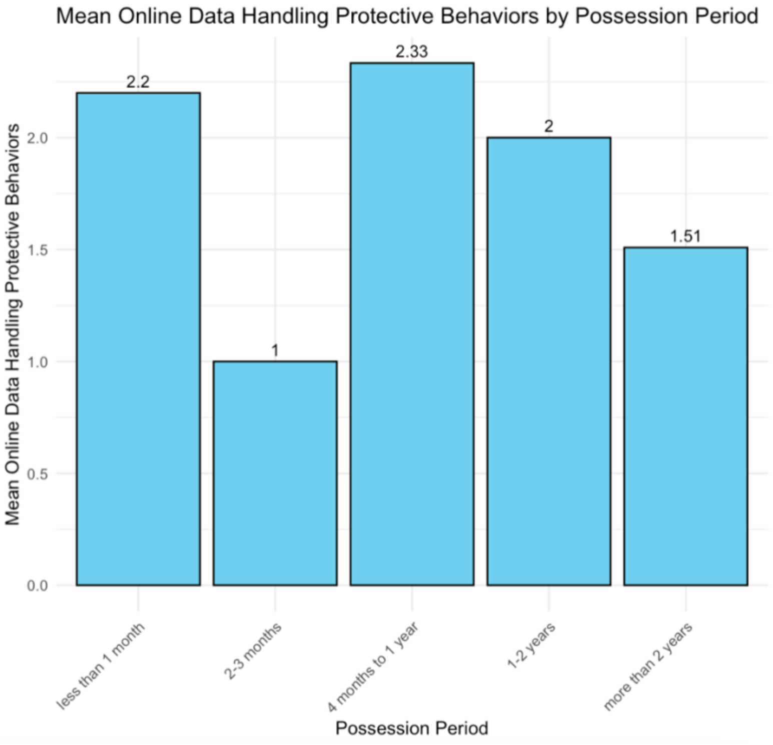
Table 6

ANOVA Results for Possession Period with Online Data Handling Protective Behaviours

	df	*SS*	*MS*	*F*	*p*
Possession Period	4	3.54	.88	1.0	.423
Residuals	29	25.61	.88	N/A	N/A

Figure 4

Mean Online Data Handling Protective Behaviour by Possession Period



Regression Analysis

The regression analysis for privacy risk perception and each protective behaviour was done with the whole sample including all factors. After that, the regression analysis was done a second time, only using the significant factors from the correlation analysis, to see if it would show any differences. The results were similar to the analysis with the whole sample and can be found in Appendix E.

Regression Analysis with all Factors. The regression analysis with privacy risk perception as dependent variable showed one significant negative effect for trust in smart speaker companies (Table 8). This result is in line with the correlation and hypothesis 4a for trust in smart speaker companies. The effects for the variables perceived enjoyableness, perceived usefulness, nothing to hide, resignation towards lack of privacy, powerlessness, privacy risk perception, and security risk perception were not significant.

Table 8

A Regression Model with Privacy Risk Perception as the Dependent Variable for the whole Sample

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	-.18	.12	-.19	-1.49	.137
Perceived Usefulness	-.03	.12	-.03	-.25	.802

Trust in Smart Speaker Companies	**-.39**	.15	-.53	-2.53	**<.01**
Nothing to Hide Beliefs	-.21	.13	-.26	-1.58	.117
Resignation Towards Lack of Privacy	-.00	.11	.00	-.07	.941
Powerlessness	-.04	.12	-.06	-.38	.698
Privacy Self-Efficacy	.01	.18	.01	.07	.938
Security Self-Efficacy	-.03	.14	-.04	-.25	.798

Note. All significant effects are marked in bold. Model Significance: *F*(8,90)=3.59, p=<0.01, R^2=.24

When the dependent variable was physical protective behaviours, the regression analysis showed a significant negative effect for perceived enjoyableness, and nothing to hide beliefs and a significant positive effect for social norm (Table 9). These results are also in line with the correlation analysis and hypothesis 2b and hypothesis 5b. The variables perceived usefulness, trust in smart speaker companies, resignation towards lack of privacy, powerlessness, privacy self-efficacy, security self-efficacy, and perceived effort needed to adjust privacy settings, had no significant effects on physical protective behaviours. Furthermore, the dependent variable, physical protective behaviours, has slightly more variance explained than the dependent variable privacy risk perception, which can be seen in the difference of R^2.

Table 9

A Regression Model with Physical Protective Behaviour as the Dependent Variable for the whole Sample

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	**-.29**	.14	-.31	-1.95	**.051**
Perceived Usefulness	-.10	.15	-.10	-.67	.501
Trust in Smart Speaker Companies	.02	.18	.03	.13	.891
Nothing to Hide Beliefs	**-.31**	.15	-.39	-1.97	**.050**
Resignation Towards Lack of Privacy	-.16	.14	-.17	-1.14	.253
Powerlessness	.02	.14	.03	.16	.871
Privacy Self-Efficacy	-.01	.21	-.01	-.06	.951
Security Self-Efficacy	.16	.17	.18	.91	.362
Social Norm	**.40**	.13	.48	3.00	**<.01**

Perceived Effort Needed to Adjust Privacy Settings	-.06	.12	-.07	-.51	.611

Note. All significant effects are marked in bold. Model Significance *F*(10,88)=4.14, p=<0.01, R^2=.32

Moreover, when the dependent variable was online data handling protective behaviours, the regression analysis showed a negative and significant effect for nothing to hide beliefs and resignation towards lack of privacy (table 10). Furthermore, a positive and significant effect was found for security self-efficacy, and social norm (Table 10). The variables perceived enjoyableness, perceived usefulness, trust in smart speaker companies, powerlessness, privacy self-efficacy, and perceived effort needed to adjust privacy settings did not show a significant effect. In addition, the dependent variable, online data handling protective behaviours, has slightly more variance explained than the dependent variables privacy risk perception and physical protective behaviours, which can be seen in the difference of R^2.

Table 10

A Regression Model with Online Data Handling Protective Behaviour as the Dependent Variable for the whole Sample

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	-.17	.16	-.18	-1.07	.285
Perceived Usefulness	-.22	.16	-.22	-1.33	.184
Trust in Smart Speaker Companies	.05	.20	.06	.24	.816
Nothing to Hide Beliefs	**-.36**	.17	-.46	-2.11	**.038**
Resignation Towards Lack of Privacy	**-.33**	.15	-.37	-2.16	**.033**
Powerlessness	-.03	.16	-.04	-.20	.841
Privacy Self-Efficacy	-.10	.24	-.13	-.14	.677
Security Self-Efficacy	**.38**	.19	.43	1.92	**.051**
Social Norm	**.45**	.14	.54	3.03	**<.001**
Perceived Effort Needed to Adjust Privacy Settings	-.07	.14	-.08	-.51	.613

Note. All significant effects are marked in bold. Model Significance *F* (10,88) =5.67, p=<0.01, R^2=.39

Discussion

The goal of this study was to retest factors, as well as include newly suggested factors to the proposed model by Hapke (2023), that underlie privacy risk perception and protective behaviours of smart speaker users and non-users. Firstly, privacy risk perception was positively correlated with physical protective behaviours as well as data handling protective behaviours. Next, the results of the regression analysis showed that trust in smart speaker companies undermines privacy risk perception. This result is also in line with the result of Hapke. The factors perceived enjoyableness, perceived usefulness, and nothing to hide beliefs correlated significantly, however, the effects were not significant when other variables were controlled for. Moreover, a marginally significant correlation was found between resignation toward lack of privacy and privacy risk perception.

Furthermore, perceived enjoyableness diminishes physical protective behaviours, which is in line with Hapke's results. However, different from Hapke's results, is the finding that nothing to hide beliefs had a significant effect on diminishing physical protective behaviours as well as data handling protective behaviours, whereas Hapke did not find a significant effect for nothing to hide beliefs with protective behaviours. In addition, perceived usefulness, and resignation towards lack of privacy, showed a significant negative relationship with physical protective behaviours, were however not significant when other variables were controlled for. Similarly, a positive marginally significant correlation between security self-efficacy and physical protective behaviours was found, however the effect was not significant when other variables were controlled for.

The regression analysis also revealed that nothing to hide beliefs, and resignation towards lack of privacy impair online data handling protective behaviours, whereas security self-efficacy increases it. Thus, the results are in line with the results of Hapke's (2023) study, which shows consistency across time and a different sample, which indicates the factors are reliable. The effect for perceived enjoyableness and perceived usefulness however were not significant when other variables were controlled for, while they did correlate significantly.

Similarly, the newly suggested factor, social norm, increased physical protective behaviours as well as data handling protective behaviours. This finding is in line with the expected results. The initial hypothesis belonged to the separate constructs of injunctive and descriptive norm, both hypothesized with a positive relationship towards protective behaviour. Thus, while the initial descriptions of the constructs seemed to be different, the analysis revealed they should be seen as one construct and therefore analysed together. Besides that, the factor perceived effort needed to adjust privacy settings was not significant when other variables were controlled for, while it did positively correlate marginally significant with online data handling protective behaviours. This, however, was only for smart speaker non-owners, when the correlation was tested separately for smart speaker owners and non-owners. This result contrasts with the hypothesis. The effect might have been marginally significant due to the small sample size but may possibly have had a significant effect in a larger sample size. This result seems to indicate that users engage in protective behaviours that take less effort and are easy to achieve.

Theoretical and Practical Implications

The distinction between the two protective behaviours, physical protective behaviour, and online data handling protective behaviour, that was found indicates individuals perceive different types of protective behaviours. Physical protective behaviours are typically physical actions for which the user needs to be in direct contact with the smart speaker. Online data handling protective behaviours, on the other hand, are digital actions, which can be performed remotely from another device connected to the smart speaker. Secondly, these two dependent variables, showed a different effect on the various independent variables in this present study. The analysis showed a significant effect for resignation towards lack of privacy and powerlessness, on online data handling protective behaviours, which were non-significant for physical protective behaviours. This suggests that experiencing a lack of control affects online data handling behaviours but not physical protective behaviours. This lack or abundance of control in turn seems to influence if and in which type of protective behaviour someone engages in, around their smart speaker, which should be researched further.

Furthermore, the results of the factor social norm suggests that individuals would engage in more privacy protective behaviours around their smart speaker when they think others in their environment also engage in protective behaviours around their smart speaker. Next to that, the results suggests that individuals engage in more privacy protective behaviours if they feel like others in their surrounding think, it is acceptable and recommended to engage in privacy protective behaviours around a smart speaker. This is in line with expected results as well as the TPB. Furthermore, these results are also in line with the study of Ebbers and Karaboga (2023), who found that the context in which individuals use their smart speaker, and with that the social norms they are exposed to, influences the adoption of protective behaviours. Subsequently, future research should aim to better and in more detail understand how the social, cultural, and environmental context, influences the engagement or lack of engagement in privacy protective behaviours around smart speakers. It has been shown that these influence the social norms of an individual. The cultural context could have an influence in so far that some cultures value privacy more than others which would result in higher engagement in privacy protective behaviours. Next to that, can the environmental context have an influence on the use of the smart speaker. Individuals who live in shared homes may have different privacy needs than individuals who live on their own (Mcleod, 2023).

Next to that, contradicting the hypothesis and findings by Liu et al. (2021), was the marginally positive relationship between perceived effort needed to adjust privacy settings and online data handling protective behaviours, for smart speaker non-owners. Liu et al. (2021) found that individuals are less likely to engage in protective behaviour if they see actions as effortful, due to their low perceived behavioural control. To explain the positive relation, it could be that individuals who perceive protective behaviours as more effortful also perceive these behaviours as more helpful. Hence, individuals might associate more effort with higher efficacy and therefore engage in protective behaviours even though they require more effort. The finding however, should be researched further and compared to smart speaker owners, also with a higher sample size, as it might also be that individuals who do not own a smart speaker lack practical experience with a smart speaker and therefore perceive a different amount of effort it would take them to engage in protective behaviours than it would a smart speaker owner (Malkin et al., 2019). This could subsequently help in understanding factors and needs for smart speaker users to engage in more privacy protective behaviours. Furthermore, it could be researched if individuals perceive a different amount of effort and control for physical protective behaviour than for online data handling protective behaviour and how this influences the engagement in each type of protective behaviour.

Moreover, as additional explorative analysis, the correlation analysis was calculated separately for smart speaker owners and non-owners. The results revealed different significant results when the sample was tested separately for smart speaker owners and non-owners (Appendix D). The strongest predictor for privacy risk perception in the smart speaker non-owner group was trust in smart speaker companies. The strongest predictor for both protective behaviours in the smart speaker owner group was resignation towards lack of privacy. For the group smart speaker non-owners, the strongest predictor was social norm in regard to physical protective behaviours. In regard to online data handling protective behaviours, resignation towards lack of privacy was the strongest predictor. Hence, the different significant correlations for smart speaker owners and non-owners suggest that the two groups are influenced differently by the variables. This can be attributed to different characteristics such as age, education level, or being an early or late adopter of technology. It can furthermore be attributed to preferences or needs, such as perceiving a smart speaker to be more convenient, automating tasks, or to use it for home security with connected cameras and alarms (Malkin et al., 2019). Lastly it can be attributed to behaviours which divides these two groups in the first place. However, the sample size for the two subgroups was too small for the analysis and therefore insufficient to make meaningful claims based on the results. These subgroups should be researched further in future studies, with a larger sample size. Additionally, it is also important to understand the differences and needs of these two groups, to better tailor specific interventions, and products that help in privacy risk perception and to engage in more protective behaviours.

Strengths, Limitations, and Future Research

A strong point of this study is the high Cronbach's alpha for the newly suggested factors social norm, perceived effort needed to adjust privacy settings, and each protective behaviour. With an alpha of 0.8 or higher this indicates high internal consistency between the items which means they reliably measure the intended constructs which in turn strengthens the validity of the findings. Another strong point of this study is to have measured many different variables at once, while also among different subgroups. This provides a more complete understanding of the antecedents that undermine privacy risk perception and protective behaviours around smart speakers at once. Having these variables measured with different subgroups also allows to find out how these subgroups effect the variables differently, which can be used for future research.

On the contrary, this study also has some limitations. Firstly, the low sample size (99) and low diversity, as the majority of participants did not own a smart speaker (65). As a result, only 33 of these participants would install a smart speaker if it would be gifted to them, and 28 would use it. Thus, a particularly small group owned a smart speaker (34). Also, there were more female (60) than male (37) participants in the study and the majority of the participants came from Germany (80), which might indicate that these results are only representative of the German population. Next to that, due to the low sample size and many predictors in the regression analysis only very large effects were found. Thus, non-significant effects in this study might show a different result when tested with a larger sample size. Furthermore, the low diversity of the sample could potentially lead to bias in the results, not giving an accurate representation. This study should therefore be replicated with a larger sample size as well as more diversity in the sample. Moreover, the low Cronbach's alpha for nothing to hide beliefs, resignation towards lack of privacy, and powerlessness, being under 0.7, might have the limited reliability, which should be improved in future studies to guarantee a reliable measure for the variables.

Another point for future research would be to find out if smart speaker users, that see privacy protective behaviours as effortful while thinking they are capable of overcoming the effort needed, might be more inclined to engage in privacy protective behaviours around their smart speaker. Additionally, future studies could investigate how to develop helpful interventions or adapt existing interventions that addresses the adoption of protective behaviours around smart speakers using social norms. As research has already shown social norms successfully increase the adoption of protective behaviour through making the protective behaviour seem normal, socially approved, common, and valued (McDonald & Crandall, 2015). Interventions using social norms to engage individuals in more protective behaviours, for example, around health behaviours or pro environmental behaviours have been very effective (Terry & Mathews, 2022, Yamin et al., 2019). These interventions include campaigns highlighting the percentage of vaccinated individuals, how many neighbourhoods participate in recycling programmes, or reports showing how to reduce the energy consumption. To transfer these interventions to the smart speaker context, campaigns could share information about the number of users that already engage in protective behaviours around their smart speaker, which could be shown in the accompanying app. Next to that, a feature could be added to the app that lets users compare their privacy settings to those of their friends and family. Lastly, publicly advertising and demonstrating engagement in protective behaviours, through social media platforms, could help individuals see these behaviours as normal and socially approved. As a result, individuals would change their perception of social norms around smart speakers, to engage in more privacy protective behaviours as they see others are doing the same, which, this study has shown, to be a strong predictor of privacy protective behaviours. Lastly, future research should engage more in convincing people they do have something to hide from their smart speaker, as the strongest predictor of this study diminishing protective behaviour was the factor nothing to hide beliefs. Some aspects every individual should hide or be mindful about when sharing this information with their smart speaker are things such as addresses and locations, appointments and schedules, confidential information, and bank details. This information can be accessed and used by third parties which increases a privacy risk. It is therefore important individuals understand they do have something to hide from their smart speaker and engage in more privacy protective behaviours.

Conclusion

To conclude, this study was used to gain more insight into the antecedents of privacy risk perception and protective behaviours around smart speakers as well as retesting the results of Hapke (2023). The results show some similarities to the previous study, indicating the strongest predictor for undermining privacy risk perception was trust in smart speaker companies. The strongest predictor diminishing protective behaviours was nothing to hide beliefs, while the strongest predictor increasing protective behaviours was social norm. This study therefore provides additional support for earlier findings by Hapke while also giving new insights into antecedents of privacy risk perception and protective behaviours. Future studies should take the results into account and investigate in retesting and finding further antecedents that could potentially extent the model. Lastly, a distinction should be made in protective behaviours, which could help develop better targeted interventions.

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

Ahmed, A. (2023, January 21). Uncovering the dark side of Amazon Alexa: How intelligent speakers jeopardize your privacy. *Digital Information World*. https://www.digitalinformationworld.com/2023/01/uncovering-dark-side-of-amazon-alexa.html?m=1

Allan, N. P., & Lonigan, C. J. (2011). Examining the dimensionality of effortful control in preschool children and its relation to academic and socioemotional indicators. *Developmental Psychology*, *47*(4), 905–915. https://doi.org/10.1037/a0023748

Ajzen, I. (1987). Attitudes, Traits, and Actions: Dispositional Prediction of Behavior in Personality and Social Psychology. In *Advances in Experimental Social Psychology* (pp. 1–63). https://doi.org/10.1016/s0065-2601(08)60411-6

Ajzen, I. (2002). Perceived behavioral control, Self-Efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psycholog*, *32*(4), 665–683. https://people.umass.edu/aizen/pubs/pbc.pdf

Borgeaud, A. (2023, December 19). *Smart speaker ownership in France, Germany, and Spain 2023 | Statista*. Statista. https://www.statista.com/statistics/1422961/smart-speakers-ownership-france-germany-spain/

Brooke, J. (1996). SUS—A Quick and Dirty Usability Scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & I. L. McClelland (Eds.), Usability Evaluation in Industry (pp. 189-194). London: Taylor & Francis.

Charlton, A., & Charlton, A. (2018, July 12). *Half of US adults believe smart home devices record conversations to send targeted ads*. Gearbrain. https://www.gearbrain.com/smart-home-device-trust-fragile-2580279907.html

Dupuis, M., & Ebenezer, M. E. D. (2018). Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. *Research Gate*. https://doi.org/10.1145/3241815.3241869

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

Gardiner, B. (2018, June 5). *Private Smarts: Can Digital Assistants Work without Prying into Our Lives?* Scientific American. https://www.scientificamerican.com/article/private-smarts-can-digital-assistants-work-without-prying-into-our-lives/

Hayes, A. (2023, September 29). *Smart Home: definition, how they work, pros and cons*. Investopedia. https://www.investopedia.com/terms/s/smart-home.asp

Hapke, J. (2023). *Examining Factors that Undermine Privacy Risk Perception and Protective Behaviour Concerning Smart Speakers* [BA thesis, University of Twente]. http://essay.utwente.nl/95412/1/Hapke_BA_BMS.pdf

Hedayati, S., Hossein, D., Farhadinejad, M., & Rastgar, A. A. (2023). Meta-analysis on application of Protection Motivation Theory in preventive behaviors against COVID-19. *International Journal of Disaster Risk Reduction*, *94*, 103758. https://doi.org/10.1016/j.ijdrr.2023.103758

Hedeman, J. (2021). *Hey Siri, let's go shopping! A study into the factors influencing Dutch consumers' intention to use a voice assistant for online shopping* [MA thesis, University of Twente]. http://essay.utwente.nl/85619/1/Hedeman_MA_BMS.pdf

Huang, Y., Obada-Obieh, B., & Beznosov, 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*. https://doi.org/10.1145/3313831.3376529

Kang, H., & Oh, J. (2021). Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society*, *25*(5), 1153–1175. https://doi.org/10.1177/14614448211026611

Klein, K.-A. (2005). *Subjective, descriptive, and injunctive norms: three separate constructs* [PhD dissertation, Michigan State University]. https://www.proquest.com/openview/8bdfc4094f3cc2d585190fa806048963/1?pq-origsite=gscholar&cbl=18750&diss=y#:~:text=In%20other%20words%2C%20social%20norms,Trafimow%20%26%20Fishbein%2C%201994).

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

Lareo, X. (2019). Technodispatch Smart Speakers and Virtual Assistants. In *European Data Protection Supervisor* (QT-AD-19-001-EN-N). Publications Office of the European Union. https://doi.org/10.2804/755512

Lau, J., Zimmerman, B. G., & Schaub, F. (2018). Alexa, are you listening? *Proceedings of the ACM on Human-computer Interaction*, *2*(CSCW), 1–31. https://doi.org/10.1145/3274371

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

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

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

Marks, T. (2022, May 13). *The privacy risks of your smart speaker*. VPNOverview.com. https://vpnoverview.com/privacy/devices/privacy-risks-smart-speaker/

Masur, P. K., Bazarova, N. N., & DiFranzo, D. (2023). The impact of what others do, approve of, and expect you to do: An In-Depth Analysis of Social Norms and Self-Disclosure on Social media. *Social Media + Society*, *9*(1), 205630512311564. https://doi.org/10.1177/20563051231156401

McDonald, R. I., & Crandall, C. S. (2015). Social norms and social influence. *Current Opinion in Behavioral Sciences*, *3*, 147–151. https://doi.org/10.1016/j.cobeha.2015.04.006

Mcleod, S., PhD. (2023). Social roles and Social norms in Psychology. *Simply Psychology*. https://www.simplypsychology.org/social-roles.html

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M. & Roesner. F., 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In Proceedings of the 2017 CHI Conference on Human FactorsinComputingSystems(CHI'17).ACM,NewYork,NY,USA,5197–5207. https://doi.org/10.1145/3025453.3025735

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

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

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

Rosenstock, I. M. (1974). The health belief model and Preventive health behavior. *Health Education Monographs*, *2*(4), 354–386. https://doi.org/10.1177/109019817400200405

Savadori, L., & Lauriola, M. (2021). Risk perception and protective behaviors during the rise of the COVID-19 outbreak in Italy. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.577331

Sommer, L. (2011). The theory of planned behaviour and the impact of past behaviour. *International Business & Economics Research Journal*, *10*(1). https://doi.org/10.19030/iber.v10i1.930

Terry, D. L., & Mathews, D. P. (2022). Social norms and engagement in protective health behaviors among rural health providers. *Journal of Clinical Psychology in Medical Settings*, *29*(2), 384–390. https://doi.org/10.1007/s10880-022-09845-0

Venkatesh, N., Thong, N., & Xu, N. (2012). Consumer Acceptance and use of Information technology: Extending the unified theory of acceptance and use of technology. *Management Information Systems Quarterly*, *36*(1), 157. https://doi.org/10.2307/41410412

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

Yamin, P., Fei, M., Lahlou, S., & Levy, S. (2019). Using social norms to change behavior and increase sustainability in the real world: A Systematic Review of the literature. *Sustainability*, *11*(20), 5847. https://doi.org/10.3390/su11205847

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

Appendix A: Questionnaire

Informed Consent

Project Title

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

Researchers

Antonia Döring (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 the researcher 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 20 minutes.

Participant Rights

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

Risks and Benefits

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

Confidentiality

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

Anonymity and Confidentiality

Your responses will be strictly anonymous; we will not be collecting or retaining any information about your identity. The information you provide will not be disclosed to third parties, and it will be aggregated with the responses of other participants and examined for hypothesized patterns. Data from this study will be stored in an online repository and shared publicly to adhere to best practices in scientific transparency.

Questions

For further information about this study, you may contact:

Antonia Döring: a.doring@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.

Demographic questions

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

Values male (if gender male, or randomized for non-binary & prefer not to say)

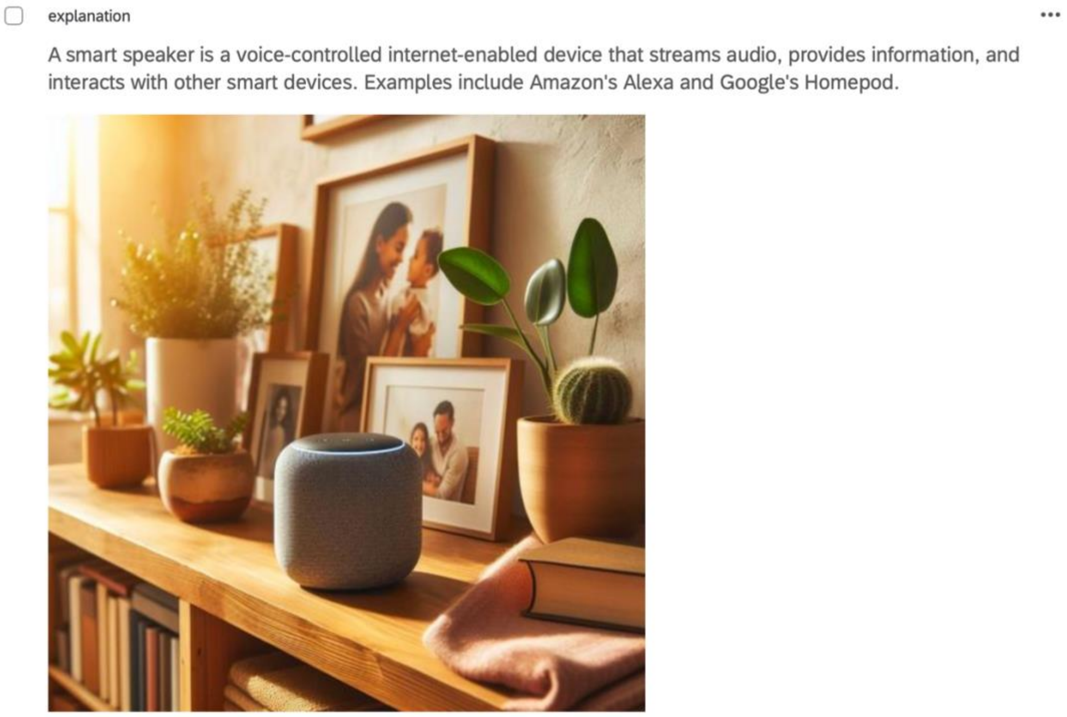
- He wants the state to be strong, so it can defend its citizens.
- Following his family's customs or the custom of a religion is important to him.

- It’s important to him to follow rules even when no one is watching.
- He thinks it is important to never be annoying to anyone.
- It is important to him to be humble.
- He goes out of his way to be a dependable and trustworthy friend.
- Caring for the well-being of people he is close to is important to him.
- He thinks it is important that every person in the world has equal opportunities in life.
- It is important to him to work against threats to the world of nature.
- It is important to him to listen to people who are different from him.
- It is important to him to have full control over who accesses personal information about him.
- It is important to him to not share personal information (for example about personal preferences, one’s health, or political religious beliefs) with unknown others.
- It is important to him to protect his privacy.

Values female (if gender female, or randomized for non-binary & prefer not to say)

- She wants the state to be strong, so it can defend its citizens.
- Following her family’s customs or the custom of a religion is important to her.
- It’s important to her to follow rules even when no one is watching.
- She thinks it is important to never be annoying to anyone.
- It is important to her to be humble.
- She goes out of her way to be a dependable and trustworthy friend.
- Caring for the well-being of people she is close to is important to her.
- She thinks it is important that every person in the world has equal opportunities in life.
- It is important to her to work against threats to the world of nature.
- It is important to her to listen to people who are different from her.
- It is important to her to have full control over who accesses personal information about her.
- It is important to her to not share personal information (for example about personal preferences, one’s health, or political religious beliefs) with unknown others.
- It is important to her to protect her privacy.

Control questions



□ explanation

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

- Is there a smart speaker in your household? (please also answer 'yes' if you are a student and there is one in your parent's house)? (Yes/No)
  - If yes: Which statement best describes your situation regarding the smart speaker? (I am the owner/ user or I use it, but I am not the owner)
  - If yes: Did you install it yourself? (Yes/No)
  - If yes: ***Possession period***
    - "For how long have you been using your smart speaker device?"
      - Less than 1 month
      - 2-3 months
      - 4 months to 1 year
      - 1-2 years
      - More than 2 years
  - 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.

    - If no: Keeping in mind that you have been gifted a smart speaker, what would you do?
        - I will install the smart speaker that has been gifted to me (yes/No/I don’t know)
        - I will use the smart speaker that has been gifted to me (yes/no/I don’t know)

Gifted Scenario:

Protective behaviour (Gifted)

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

- I will turn off the smart speaker when I am not using it
- I will unplug the smart speaker when I am not using it
- I will unplug the smart speaker when I am having serious/private conversations
- I will turn off the smart speaker when I am having serious/private conversations
- I will mute the smart speakers microphone when I am not using it
- I will review the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account
- I will review which applications/services have access to my smart speaker
- I will restrict the amount of data that the device is allowed to collect through the smart speakers settings
- I will delete my smart speaker recordings
- In the app I will delete sensitive information that the smart speaker stored about me.
- I will speak very quietly around the smart speaker, in case I don’t want to be recorded
- I will moderate my language around the smart speaker so that it doesn’t record private matters, even if accidentally
- I will avoid sensitive/private conversations around the smart speaker
- If I have a visitor, I will inform them that I have a smart speaker
- I will consider where to place the smart speaker so that it is not positioned in areas where I typically engage in conversations involving sensitive or private information
- I will set a new difficult password for my smart speaker that I don’t use for other applications
- I will not write down the password on a piece of paper or share it otherwise with house members or visitors

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.

Perceived Effort needed to adjust privacy settings

*(*5-point Likert scale 1= it takes very little effort, 5= it takes a lot of effort)

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

- “How much effort would it take you to adjust your privacy settings on your smart speaker?”
- “How much effort would it take you to engage in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?”
- “How much effort would it take you to continuously keep engaging in privacy protecting measures (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?”
- “How much effort would it take you to find information on how to better protect your privacy from your smart speaker?”

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

Owning scenario

Protective Behaviour (Owning)

How often in the last month did you engage in the following behaviours (1 = never, 5 = always) ?

- I turned off the smart speaker when I was not using it
- I unplugged the smart speaker when I was not using it
- I unplugged the smart speaker when I was having serious/private conversations
- I turned off the smart speaker when I was having serious/private conversations
- I muted the smart speakers microphone when I was not using it
- I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account
- I reviewed which applications/services have access to my smart speaker
- I restricted the amount of data that the device is allowed to collect through the smart speakers settings
- I deleted my smart speaker recordings
- In the app I deleted sensitive information that the smart speaker stored about me.
- I spoke very quietly around the smart speaker, in case I did not want to be recorded
- I moderated my language around the smart speaker so that it didn’t record private matters, even if accidentally
- I avoided sensitive/private conversations around the smart speaker
- When I had a visitor, I informed them that I have a smart speaker
- When I had a visitor, I offered to switch the smart speaker off

- When I installed the smart speaker,...
  - ... I placed the smart speaker so that it was not positioned in areas where I typically engaged in conversations involving sensitive or private information
  - ... I set a new difficult password for my smart speaker that I don't use for other applications.
  - ... I did not write down the smart speakers password on a piece of paper or shared it otherwise with house members or visitors
  - ...I changed the password again after using the smart speaker for some time

Perceived enjoyableness

(5-point Likert scale 1= strongly disagree, 5 = strongly agree) *Please indicate to what extent you agree with the following statements:*

- Using a smart speaker is enjoyable.
- I have fun using a smart speaker.
- It is not interesting to use a smart speaker.
- Using a smart speaker gives 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 improves my productivity in my daily life.
- Using a smart speaker makes my life easier.
- Using a smart speaker enables me to accomplish my tasks more quickly.
- Using a smart speaker enhances my effectiveness in daily tasks.
- I find it useful to use a smart speaker at home.

Perceived Effort needed to adjust privacy settings

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

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

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

- “How much effort does it take you to continuously keep engaging in privacy protecting measures (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?”
- “How much effort does it take you to find information on how to better protect your privacy from your smart speaker?”
- "How much effort does it take you to seek help or guidance from others to protect your privacy on 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 with 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 by your smart speaker?

Questions that are the same for the gifted and the owning scenario

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.

Social norm/subjective norm

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

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

Injunctive social norm

- “I think that people whose opinions I value, would support me using privacy protective behaviour with a smart speaker”.
- “My family members and friends would recommend me to adjust my smart speaker settings to enhance my privacy”.
- “People in my immediate surrounding think that privacy protecting behaviour around their smart speaker is important”.

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

Descriptive social norm

- “People that are important to me generally take privacy protective actions around smart devices”.
- “My friends and family generally put effort in limiting data-collection from smart devices”.
- “People close to me generally make sure that their smart devices have restricted privacy settings”.

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.

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 Antonia Döring: a.doring@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 for Independent Variables

Construct	Item	Factor Loading
Social Norm	“I think that people whose opinions I value, would support me using privacy protective behaviour with a smart speaker”.	.231
	“My family members and friends would recommend me to adjust my smart speaker settings to enhance my privacy”.	.543
	“People in my immediate surrounding think that privacy protecting behaviour around their smart speaker is important”.	.821
	"I think people in my surrounding find it important to comply with the privacy recommendations provided by experts when using smart speakers".	.568
	“People that are important to me generally take privacy protective actions around smart devices”.	.807
	“My friends and family generally put effort in limiting data-collection from smart devices”.	.679
	“People close to me generally put make sure that their smart devices have restricted privacy settings”.	.652
Perceived Effort needed to adjust privacy settings	“How much effort would it take you to adjust your privacy settings on your smart speaker?”	.764
	“How much effort would it take you to engage in privacy protective behaviours (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?”	.643

“How much effort would it take you to continuously keep engaging in privacy protecting measures (like muting the microphone, unplugging the smart speaker when it is not used) around your smart speaker?”	.659
“How much effort would it take you to find information on how to better protect your privacy from your smart speaker?”	.655
"How much effort would it take you to seek help or guidance from others to protect your privacy on your smart speaker?”	.654

Appendix C: Factor Loadings for the Dependent Variable

Construct	Item	Factor Loading	
Physical Protective Behaviours	I turned off the smart speaker when I was not using it	.734	.296
	I unplugged the smart speaker when I was not using it	.741	.302
	I unplugged the smart speaker when I was having serious/private conversations	.816	.303
	I turned off the smart speaker when I was having serious/private conversations	.823	.421
	I muted the smart speakers microphone when I was not using it	.743	.488
Data Handling Protective Behaviours	I reviewed the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account	.341	.811
	I reviewed which applications/services have access to my smart speaker	.358	.728
	I restricted the amount of data that the device is allowed to collect through the smart speaker's settings	.276	.832
	I deleted my smart speaker recordings	.492	.711
	In the app I deleted sensitive information that the smart speaker stored about me.	.558	.724
Physical Protective Behaviours	I spoke very quietly around the smart speaker in case I did not want to be recorded	.569	.312

	I moderated my language around the smart speaker so that it didn’t record private matters, even if accidentally	.719	.394
	I avoided sensitive/private conversations around the smart speaker	.748	.481
	When I had a visitor, I informed them that I have a smart speaker	.519	.421

Appendix D: Hypothesis Testing for Smart Speaker Owners and Non-Owners

Privacy Risk Perception

Pearson's Correlation between Privacy Risk Perception with the Independent Variables for Smart Speaker Owners and Non-Owners.

	Owners		Non-Owners	
	r	*p*	*r*	*p*
Perceived Enjoyableness	-.13	.446	**-.31**	**.012**
Perceived Usefulness	-.16	.354	-.21	.078
Trust in Companies	-.12	.498	**-.45**	**<.001**
Nothing to Hide	.18	.291	**-.41**	**<.001**
Resignation Towards Lack of Privacy	-.06	.724	-.22	.077
Powerlessness	-.11	.518	-.04	.696
Privacy Self-Efficacy	-.03	.854	-.22	.074
Security Self-Efficacy	-.08	.630	-.12	.309

Note. All significant correlations are marked in bold.

When looking at smart speaker owners none of the predictor variables had a significant effect on privacy risk perception. However, when looking at smart speaker non-owners the analysis revealed a significant negative effect for privacy risk perception with the independent variables perceived enjoyableness, trust in smart speaker companies, and nothing to hide beliefs.

Protective Behaviours

Pearson's Correlation with both Protective Behaviours and the Independent Variables for Smart Speaker Owners and Non-Owners.

	Owners Physical Protective Behaviour		Owners Online Protective Behaviour		Non-Owners Physical Protective Behaviour		Non-Owners Online Protective Behaviour	
	r	*p*	*r*	*p*	*r*	*p*	*r*	*p*
Privacy Risk Perception	.20	.238	-.03	.846	**.39**	**<.001**	**.43**	**<.001**

Perceived Enjoyableness	.21	.212	.10	.555	**-.29**	**.016**	-.16	.178
Perceived Usefulness	.03	.839	.16	.342	-.06	.631	-.05	.667
Trust in Companies	-.04	.784	.17	.308	-.02	.831	-.06	.596
Nothing to Hide	.01	.928	-.21	.234	**-.27**	**.029**	**-.24**	**.052**
Resignation Towards Lack of Privacy	**-.36**	**.032**	**-.55**	**<.001**	**-.25**	**.042**	**-.37**	**<.001**
Powerlessness	-.18	.303	**-.39**	**.021**	-.11	.352	-.17	.167
Privacy Self-Efficacy	.00	.979	.12	.469	.14	.251	.21	.081
Security Self-Efficacy	.23	.171	**.33**	**.050**	.13	.284	**.27**	**.025**
Social Norm	-.02	.900	.27	.111	**.34**	**.004**	**.25**	**.043**
Perceived Effort Needed to Adjust Privacy Settings	-.08	.644	-.23	.19	-.19	.122	.23	.063

When looking at smart speaker owners and the two protective behavioural factors the variable resignation towards lack of privacy had a significant negative effect on both with a larger effect size for online data handling protective behaviours. Next to that, powerlessness and security self-efficacy showed a significant effect only for online data handling protective behaviours.

Compared to the non-owner condition, nothing to hide beliefs and social norm significantly explained the two behavioural factors, with a larger effect size for physical protective behaviours. Next to that, privacy risk perception, and resignation towards lack of privacy also explained the two behavioural factors, with a larger effect size for online data handling protective behaviours. Furthermore, perceived enjoyableness showed a significant negative effect for physical protective behaviours. Moreover, security self-efficacy showed a significant positive effect for online data handling protective behaviours. Finally, privacy self-efficacy and perceived effort needed to adjust privacy settings showed a marginally significant positive effect for online data handling protective behaviours.

Appendix E: Regression Analysis for Significant Factors

The regression analysis with privacy risk perception as dependent variable showed one significant negative effect for trust in smart speaker companies, which is in line with hypothesis 4a. Additionally, one marginally significant negative effect for nothing to hide beliefs (Table 11) was found, which is in line with hypothesis 5a. The independent variables perceived enjoyableness, perceived usefulness, and resignation towards lack of privacy did not show any significant effects towards privacy risk perception.

Table 11

A Model with Privacy Risk Perception as the Dependent Variable including the Significant Independent Variables from the Correlation Analysis

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	-.18	.12	-.19	-1.51	.13
Perceived Usefulness	-.03	.12	-.03	-.29	.76
Trust in Smart Speaker Companies	**-.38**	.13	-.52	-2.79	**<0.05**
Nothing to Hide Beliefs	-.22	.12	-.28	.02	.08
Resignation Towards Lack of Privacy	.00	.11	.00	.02	.97

Note. All significant effects are marked in bold. Model Significance *F*(5,93)=5.88, p=<0.01, R^2=.24

When the dependent variable was physical protective behaviours the analysis showed a negative significant effect for perceived enjoyableness, nothing to hide beliefs, and social norm (table 12). These results are in line with hypothesis 2b and 5b. For the variables perceived usefulness, resignation towards lack of privacy, and security self-efficacy, no significant effect was found.

Table 12

A Model with Physical Protective Behaviour as the Dependent Variable including the Significant Independent Variables from the Correlation Analysis

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	**-.29**	.14	-.31	-2.01	**<.05**
Perceived Usefulness	-.08	.14	-.09	-.62	.53
Nothing to Hide Beliefs	**-.29**	.14	-.37	-2.01	**<.05**

Resignation Towards Lack of Privacy	-.16	.13	-.18	-1.27	.21
Security Self-Efficacy	.16	.12	.19	1.34	.18
Social Norm	**.39**	.13	.47	3.07	**<.05**

Note. All significant effects are marked in bold. Model Significance *F*(6,92)=7.13, p=<0.01, R^2=.31

Furthermore, when the dependent variable was online data handling protective behaviours the regression analysis showed a negative significant effect for nothing to hide beliefs and resignation towards lack of privacy and a positive significant effect for security self-efficacy and social norm (Table 12). Next to that, no significant effect was found for the independent variables perceived enjoyableness and perceived usefulness. Additionally, the dependent variable online data handling protective behaviours has slightly more variance explained than the dependent variables privacy risk perception and physical protective behaviours, which can be seen in the difference of R^2.

Table 13

A Model with Online Data Handling Protective Behaviour as the Dependent Variable including the Significant Independent Variables from the Correlation Analysis

Variable	*B*	*SE B*	*β*	*t*	*p*
Perceived Enjoyableness	-.17	.16	-.34	-1.09	.27
Perceived Usefulness	-.21	.15	-.09	-1.35	.18
Nothing to Hide Beliefs	**-.36**	.16	-.43	-2.22	**<.05**
Resignation Towards Lack of Privacy	**-.34**	.14	-.42	-2.39	**<.05**
Security Self-Efficacy	**.34**	.13	.02	2.45	**<.05**
Social Norm	**.44**	.14	.21	3.11	**<.05**

Note. All significant effects are marked in bold. Model Significance *F*(6,92)=9.76, p=<0.01, R^2=.38

Appendix F: R script

```
#load packages
library(tidyverse)
library(tidyr)
library(nlme)
library(readxl)
library(dplyr)
library(nlme)
library(lmerTest)
library(psych)
library(janitor)
library(CTT)
library(carData)
library(lmtest)
library(ggplot2)
library(broom)
library(foreign)

#load dataset
dataset <- read.csv("datathesis.csv", sep = ",")

# Create a new column to mark participants who didn't pass both attention checks
dataset$exclude <- ifelse(dataset$attention.check.1. != "Strongly agree" |
dataset$attention.check.2.. != "Strongly agree", TRUE, FALSE)

# View the dataset to verify the new column
View(dataset)

# Exclude rows where "exclude" is TRUE from analysis
cleaned_dataset <- dataset[dataset$exclude == FALSE, ]

# Create the subset of data without the excluded variables
cleaned_dataset_novalues <- cleaned_dataset[, !names(cleaned_dataset) %in% c("Q255",
"Q256", "Q257", "Q258", "Q259", "Q260", "Q261", "Q262", "Q263", "Q264",
                                            "PAV1.female.", "PAV2.female.",
"PAV3.female.",
                                            "SES1.", "TR1.", "COR1.", "COI1", "HUI1",
"BED1", "BEC1", "UNC1", "UNN1", "UNT1",
                                            "PAV1", "PAV2", "PAV3.")]

########################################
# Subset for participants who own a smart speaker
smart_speaker_subset_owning <-
cleaned_dataset_novalues[cleaned_dataset_novalues$control1 == "Yes", ]
```

```
#remove the questions that belong to the other condition
smart_speaker_subset_owning <- subset(smart_speaker_subset_owning, select = -c(UaI1.,
UaI2, PBg1:PBg17, H1:H4, PU1:PU5, Q88, Q90, Q91, Q92, PE1.:PE5., PRP1:PRP3))

# Subset for participants who do not own a smart speaker (No gifted questions)
smart_speaker_subset_gifted <-
cleaned_dataset_novalues[cleaned_dataset_novalues$control1 == "No", ]

#remove the questions belonging to the other condition (No owning questions)
smart_speaker_subset_gifted <- subset(smart_speaker_subset_gifted, select = -
c(primaryOsecondaryU, control2, possession.period., Ho1:Ho4, PUo1:PUo5, PCo1:PCo4,
prpO1:prpO3, Q210:Q214, PBo1:PBo18, PBo19.))

###########################################################################
####Descriptive Statistics######
#demographics
#make age as numeric
cleaned_dataset_novalues$Age <- as.numeric(cleaned_dataset_novalues$Age)
summary(cleaned_dataset_novalues$Age)
sd(cleaned_dataset_novalues$Age)

#country
# Combine counts from both 'Country' and 'Country_3_TEXT' columns
combined_counts <- table(c(cleaned_dataset_novalues$Country,
cleaned_dataset_novalues$Country_3_TEXT))
print(combined_counts)

#education
combined_counts_education <- table(c(cleaned_dataset_novalues$Education))
print(combined_counts_education)

#gender
combined_counts_gender <- table(c(cleaned_dataset_novalues$Gender))
print(combined_counts_gender)

#student
combined_counts_student <- table(c(cleaned_dataset_novalues$Student))
print(combined_counts_student)

# Count the number of TRUE and FALSE values in the exclude variable
(ATTENTIONCHECK)
exclude_counts <- table(dataset$exclude)
print(exclude_counts)
```

```
#General Means
summary(smart_speaker_subset_gifted)
describe(smart_speaker_subset_gifted)

summary(smart_speaker_subset_owning)
describe(smart_speaker_subset_owning)


#smart speaker user or not
table(cleaned_dataset_novalues$control1)

#installed smart speaker by themselves
table(cleaned_dataset_novalues$control2)

#are users primary or secondary users
table(cleaned_dataset_novalues$primaryOsecondaryU)

#possession period
table(cleaned_dataset_novalues$possession.period.)

#gifted install and use
table(smart_speaker_subset_gifted$UaI1.)
table(smart_speaker_subset_gifted$UaI2)

###########################################################################
###Put likert scales in numeric values####
############################################
#below Gifted Privacy Risk Perception and Protective Behaviours

# Convert Likert scale responses to numeric values for Privacy Risk Perception Gifted
(Package dplyr)
smart_speaker_subset_gifted$PRP1 <- recode(smart_speaker_subset_gifted$PRP1, "None at
all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)
smart_speaker_subset_gifted$PRP2 <- recode(smart_speaker_subset_gifted$PRP2, "None at
all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)
smart_speaker_subset_gifted$PRP3 <- recode(smart_speaker_subset_gifted$PRP3, "None at
all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)

#converting prp for the owning condition
smart_speaker_subset_owning$prpO1 <- recode(smart_speaker_subset_owning$prpO1,
"None at all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)
smart_speaker_subset_owning$prpO2 <- recode(smart_speaker_subset_owning$prpO2,
"None at all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)
smart_speaker_subset_owning$prpO3 <- recode(smart_speaker_subset_owning$prpO3,
"None at all" = 1, "A little" = 2, "A moderate amount" = 3, "A lot" = 4, "A great deal" = 5)
```

```
# Define mapping from Likert scale responses to numeric values
likert_mapping_likeliness <- c("Extremely unlikely" = 1, "Somewhat unlikely" = 2, "Neither
likely nor unlikely" = 3, "Somewhat likely" = 4, "Extremely likely" = 5)

# Define mapping from Likert scale responses to numeric values for protective behavior
likert_mapping_engagement <- c("never" = 1, "almost never" = 2, "sometimes" = 3, "often" =
4, "always" = 5)

# Define Likert scale mapping agreement
likert_mapping_agreement <- c("Strongly disagree" = 1, "Somewhat disagree" = 2,
                          "Neither agree nor disagree" = 3, "Somewhat agree" = 4,
                          "Strongly agree" = 5)

#define likert mapping for klein
likert_mapping_agreement_klein <- c("strongly disagree" = 1, "somewhat disagree" = 2,
                              "neither agree nor disagree" = 3, "somewhat agree" = 4,
                              "strongly agree" = 5)

#define likert mapping for perceived effort
likert_mapping_effort <- c("it takes very little effort" = 1,
                       "it takes a little effort" = 2,
                       "it takes some effort" = 3,
                       "it takes quite a bit effort" = 4,
                       "it takes a lot of effort" = 5)

#define liekt mapping yes no questions protective behaviour
likert_mapping_yesno <- c("Yes" = 1,
                      "No" = 2)

#GIFTED#Hedonism (peceived enjoyableness) reverse code H3 and H4 and likert scale into
numeric
# Convert Likert scale responses to numeric values for hedonism factor
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(H1:H4),
~recode(., !!!likert_mapping_agreement))

#reverse coding
smart_speaker_subset_gifted$H3 <- 6 - smart_speaker_subset_gifted$H3
smart_speaker_subset_gifted$H4 <- 6 - smart_speaker_subset_gifted$H4

# Convert Likert scale responses to numeric values for hedonism factor
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning, vars(Ho1:Ho4),
~recode(., !!!likert_mapping_agreement))

#reverse coding
```

```
smart_speaker_subset_owning$Ho3 <- 6 - smart_speaker_subset_owning$Ho3
smart_speaker_subset_owning$Ho4 <- 6 - smart_speaker_subset_owning$Ho4

###########
###FOR GIFTED ALL QUESTIONS TRANSFORMED FORM LIKERT TO NUMERIC
NOW WITH MAPPINGS
# Convert Likert scale responses to numeric values for gifted subset
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(PBg1:PBg17),
~recode(., !!!likert_mapping_likeliness))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(PU1:PU5),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(Q88:Q92),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(T1:T7),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(NTH1:NTH5),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(R1:R6),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(NLT1:NLT3),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted,
vars(Powerlessness.1.:Powerlessness.5.), ~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(SA.1..:SA.6),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(RP1:SE7),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(SE8:SE9),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted,
vars(Injunctive.norm.1..:IN4), ~recode(., !!!likert_mapping_agreement_klein))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted,
vars(Descriptive.norm.1:DN3.), ~recode(., !!!likert_mapping_agreement_klein))
smart_speaker_subset_gifted <- mutate_at(smart_speaker_subset_gifted, vars(PE1.:PE5.),
~recode(., !!!likert_mapping_effort))

###FOR OWNING ALL QUESTIONS TRANSFORMED FORM LIKERT TO NUMERIC
NOW WITH MAPPINGS
# Convert Likert scale responses to numeric values for owning condition
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(PBo1:PBo15), ~recode(tolower(.), !!!likert_mapping_engagement))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(PUo1:PCo4), ~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning, vars(T1:T7),
~recode(., !!!likert_mapping_agreement))
```

```
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(NTH1:SA.6), ~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning, vars(RP1:SE7),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning, vars(SE8:SE9),
~recode(., !!!likert_mapping_agreement))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(Injunctive.norm.1..:IN4), ~recode(., !!!likert_mapping_agreement_klein))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(Descriptive.norm.1:DN3.), ~recode(., !!!likert_mapping_agreement_klein))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(Q210:Q214), ~recode(., !!!likert_mapping_effort))
smart_speaker_subset_owning <- mutate_at(smart_speaker_subset_owning,
vars(PBo16:PBo19.), ~recode(., !!!likert_mapping_yesno))

################################################################################
##############COMPOSITE SCORES########

# Calculate composite scores for gifted condition
smart_speaker_subset_gifted$privacy_risk_perception <-
rowMeans(smart_speaker_subset_gifted[, c("PRP1", "PRP2", "PRP3")], na.rm = TRUE)
smart_speaker_subset_gifted$protective_behaviors_physical <-
rowMeans(smart_speaker_subset_gifted[, c("PBg1", "PBg2", "PBg3", "PBg4", "PBg5",
"PBg11", "PBg12", "PBg13", "PBg14")], na.rm = TRUE)
smart_speaker_subset_gifted$protective_behaviors_data <-
rowMeans(smart_speaker_subset_gifted[, c("PBg6", "PBg6", "PBg8", "PBg9", "PBg10")],
na.rm = TRUE)

#composite score for hedonism (perceived enjoyaleness)
smart_speaker_subset_gifted$perceived_enjoyableness <-
rowMeans(smart_speaker_subset_gifted[, c("H1", "H2", "H3","H4")], na.rm = TRUE)

#perceived usefulness
smart_speaker_subset_gifted$perceived_usefulness <-
rowMeans(smart_speaker_subset_gifted[, c("PU1", "PU2", "PU3","PU4","PU5")], na.rm =
TRUE)

#perceived effort
smart_speaker_subset_gifted$perceived_effort <- rowMeans(smart_speaker_subset_gifted[,
c("PE1.", "PE2.", "PE3.","PE4.","PE5.")], na.rm = TRUE)

#trust in smart speaker companies
smart_speaker_subset_gifted$perceived_trust_companies <-
rowMeans(smart_speaker_subset_gifted[, c("T1", "T2", "T3","T4","T5","T6","T7")], na.rm =
TRUE)
```

```
#nothing to hide beliefs
smart_speaker_subset_gifted$nothing_to_hide <- rowMeans(smart_speaker_subset_gifted[,
c("NTH1", "NTH2", "NTH3","NTH4","NTH5")], na.rm = TRUE)

#resignation towards lack of privacy
smart_speaker_subset_gifted$resignation <- rowMeans(smart_speaker_subset_gifted[,
c("R1", "R2", "R3","R4","R5","R6")], na.rm = TRUE)

#resignation towards lack of privacy 2
smart_speaker_subset_gifted$resignation_2 <- rowMeans(smart_speaker_subset_gifted[,
c("R1", "R2", "R3")], na.rm = TRUE)

#powerlessness 2
smart_speaker_subset_gifted$powerlessness_2 <- rowMeans(smart_speaker_subset_gifted[,
c("R4","R5","R6")], na.rm = TRUE)

#injunctive norm
smart_speaker_subset_gifted$injunctive_norm <- rowMeans(smart_speaker_subset_gifted[,
c("Injunctive.norm.1..", "IN2.", "IN3.","IN4")], na.rm = TRUE)

#descriptive norm
smart_speaker_subset_gifted$descriptive_norm <- rowMeans(smart_speaker_subset_gifted[,
c("Descriptive.norm.1", "DN2", "DN3.")], na.rm = TRUE)

#self-efficacy
smart_speaker_subset_gifted$self_efficacy <- rowMeans(smart_speaker_subset_gifted[,
c("SE1", "SE2", "SE3", "SE4", "SE5")], na.rm = TRUE)

#security-efficacy
smart_speaker_subset_gifted$security_efficacy <- rowMeans(smart_speaker_subset_gifted[,
c("SE6", "SE7", "SE8", "SE9")], na.rm = TRUE)

#social norm
smart_speaker_subset_gifted$social_norm <- rowMeans(smart_speaker_subset_gifted[,
c("Injunctive.norm.1..", "IN2.", "IN3.","IN4", "Descriptive.norm.1", "DN2", "DN3.")], na.rm
= TRUE)

#social norm 2
smart_speaker_subset_gifted$social_norm_2 <- rowMeans(smart_speaker_subset_gifted[,
c("IN2.", "IN3.","IN4", "Descriptive.norm.1", "DN2", "DN3.")], na.rm = TRUE)

###########
####OWNING COMPOSITE SCORES

# Calculate composite scores of the dependent variables (PRP and PB) for owning condition
```

```
smart_speaker_subset_owning$privacy_risk_perception <-
rowMeans(smart_speaker_subset_owning[, c("prpO1", "prpO2", "prpO3")], na.rm = TRUE)
smart_speaker_subset_owning$protective_behaviors_physical <-
rowMeans(smart_speaker_subset_owning[, c("PBo1", "PBo2", "PBo3", "PBo4", "PBo5",
"PBo11", "PBo12", "PBo13", "PBo14")], na.rm = TRUE)
smart_speaker_subset_owning$protective_behaviors_data <-
rowMeans(smart_speaker_subset_owning[, c("PBo6", "PBo7", "PBo8", "PBo9", "PBo10")],
na.rm = TRUE)

#######COMPESITE SCORES FRO ALL OWNING##############
#composite score for hedonism (perceived enjoyaleness)
smart_speaker_subset_owning$perceived_enjoyableness <-
rowMeans(smart_speaker_subset_owning[, c("Ho1", "Ho2", "Ho3","Ho4")], na.rm = TRUE)

#perceived usefulness
smart_speaker_subset_owning$perceived_usefulness <-
rowMeans(smart_speaker_subset_owning[, c("PUo1", "PUo2", "PUo3","PUo4","PUo5")],
na.rm = TRUE)

#perceived effort
smart_speaker_subset_owning$perceived_effort <-
rowMeans(smart_speaker_subset_owning[, c("Q210", "Q211", "Q212","Q213","Q214")],
na.rm = TRUE)

#trust in smart speaker companies
smart_speaker_subset_owning$perceived_trust_companies <-
rowMeans(smart_speaker_subset_owning[, c("T1", "T2", "T3","T4","T5","T6","T7")], na.rm
= TRUE)

#nothing to hide beliefs
smart_speaker_subset_owning$nothing_to_hide <-
rowMeans(smart_speaker_subset_owning[, c("NTH1", "NTH2", "NTH3","NTH4","NTH5")],
na.rm = TRUE)

#resignation towards lack of privacy
smart_speaker_subset_owning$resignation <- rowMeans(smart_speaker_subset_owning[,
c("R1", "R2", "R3","R4","R5","R6")], na.rm = TRUE)

#resignation towards lack of privacy 2
smart_speaker_subset_owning$resignation_2 <- rowMeans(smart_speaker_subset_owning[,
c("R1", "R2", "R3")], na.rm = TRUE)

#powerlessness
smart_speaker_subset_owning$powerlessness_2 <-
rowMeans(smart_speaker_subset_owning[, c("R4","R5","R6")], na.rm = TRUE)
```

```
#injunctive norm
smart_speaker_subset_owning$injunctive_norm <-
rowMeans(smart_speaker_subset_owning[, c("Injunctive.norm.1..", "IN2.", "IN3.","IN4")],
na.rm = TRUE)

#descriptive norm
smart_speaker_subset_owning$descriptive_norm <-
rowMeans(smart_speaker_subset_owning[, c("Descriptive.norm.1", "DN2", "DN3.")], na.rm
= TRUE)

#self-efficacy
smart_speaker_subset_owning$self_efficacy <- rowMeans(smart_speaker_subset_owning[,
c("SE1", "SE2", "SE3", "SE4", "SE5")], na.rm = TRUE)

#security-efficacy
smart_speaker_subset_owning$security_efficacy <-
rowMeans(smart_speaker_subset_owning[, c("SE6", "SE7", "SE8", "SE9")], na.rm = TRUE)

#social norm
smart_speaker_subset_owning$social_norm <- rowMeans(smart_speaker_subset_owning[,
c("Injunctive.norm.1..", "IN2.", "IN3.","IN4", "Descriptive.norm.1", "DN2", "DN3.")], na.rm
= TRUE)

#social norm 2
smart_speaker_subset_owning$social_norm_2 <- rowMeans(smart_speaker_subset_owning[,
c("IN2.", "IN3.","IN4", "Descriptive.norm.1", "DN2", "DN3.")], na.rm = TRUE)

######################################################################
####### all protective behaviours into one subset ############
protective_behaviors_gifted <- subset(smart_speaker_subset_gifted, select = c(PBg1, PBg2,
PBg3, PBg4, PBg5, PBg6, PBg7, PBg8, PBg9, PBg10, PBg11, PBg12, PBg13, PBg14))
protective_behaviors_owning <- subset(smart_speaker_subset_owning, select = c(PBo1,
PBo2, PBo3, PBo4, PBo5, PBo6, PBo7, PBo8, PBo9, PBo10, PBo11, PBo12, PBo13,
PBo14))

# rename columns
names(protective_behaviors_gifted) <- c("PB1", "PB2", "PB3", "PB4", "PB5", "PB6", "PB7",
"PB8", "PB9", "PB10", "PB11", "PB12", "PB13", "PB14")
names(protective_behaviors_owning) <- c("PB1", "PB2", "PB3", "PB4", "PB5", "PB6",
"PB7", "PB8", "PB9", "PB10", "PB11", "PB12", "PB13", "PB14")

#combine datasets
combined_dataset <- rbind(protective_behaviors_gifted, protective_behaviors_owning)

##################################
```

```
####### all social norms into one subset ############
socialnorm_gifted <- subset(smart_speaker_subset_gifted, select = c("IN2.", "IN3.", "IN4",
"Descriptive.norm.1", "DN2", "DN3."))
socialnorm_owning <- subset(smart_speaker_subset_owning, select = c("IN2.", "IN3.",
"IN4", "Descriptive.norm.1", "DN2", "DN3."))

#combine datasets
socialnorm_combined <- rbind(socialnorm_gifted, socialnorm_owning)

####### all PERCEIVED EFFORT into one subset ############
effort_gifted <- subset(smart_speaker_subset_gifted, select = c("PE1.", "PE2.", "PE3.",
"PE4.", "PE5."))
effort_owning <- subset(smart_speaker_subset_owning, select = c("Q210", "Q211", "Q212",
"Q213", "Q214"))

# rename columns
names(effort_gifted) <- c("PE1", "PE2", "PE3", "PE4", "PE5")
names(effort_owning) <- c("PE1", "PE2", "PE3", "PE4", "PE5")

#combine datasets
effort_combined <- rbind(effort_gifted, effort_owning)

#########################################################################
########FACTOR ANALYSIS###########################################
#### factor analysis protective behavior ######
describe(combined_dataset)
combined_dataset %>% cor()
KMO(combined_dataset)
cortest.bartlett(combined_dataset)

# Kaiser's Criterion
pca_protective_behavior <- combined_dataset %>%
  cor() %>%
  eigen()
pca_protective_behavior$values

# elbow criterion to determine the number of factors
combined_dataset %>%
  scree(., factors = FALSE)

#factor analysis with varimax rotation
FA_protective_behavior <- factanal(combined_dataset, factors = 2, rotation = "varimax")
FA_protective_behavior

# Calculate Cronbach's alpha physical behavior
```

```
results_behavior_physical <- alpha(combined_dataset[c("PB1", "PB2", "PB3", "PB4", "PB5",
"PB11", "PB12", "PB13", "PB14")], check.keys = TRUE)
print(results_behavior_physical$total)

# Calculate Cronbach's alpha data handling
results_behavior_data <- alpha(combined_dataset[c("PB6", "PB7", "PB8", "PB9", "PB10")],
check.keys = TRUE)
print(results_behavior_data$total)

####################################################
#### factor analysis social norm ######
describe(socialnorm_combined)
socialnorm_combined %>% cor()
KMO(socialnorm_combined)
cortest.bartlett(socialnorm_combined)

# Kaiser's Criterion
pca_social <- socialnorm_combined %>%
  cor() %>%
  eigen()
pca_social$values

# elbow criterion to determine the number of factors
socialnorm_combined %>%
  scree(., factors = FALSE)

#factor analysis with varimax rotation
FA_social <- factanal(socialnorm_combined, factors = 1, rotation = "varimax")
FA_social

# Calculate Cronbach's alpha
results_social <- alpha(socialnorm_combined[c("IN2.", "IN3.", "IN4", "Descriptive.norm.1",
"DN2", "DN3.")], check.keys = TRUE)
print(results_social$total)

#################################
#### factor analysis perceived effort ######
describe(effort_combined)
effort_combined %>% cor()
KMO(effort_combined)
cortest.bartlett(effort_combined)

# Kaiser's Criterion
pca_effort <- effort_combined %>%
  cor() %>%
  eigen()
pca_effort$values

# elbow criterion to determine the number of factors
effort_combined %>%
  scree(., factors = FALSE)

#factor analysis with varimax rotation
FA_effort <- factanal(effort_combined, factors = 1, rotation = "varimax")
FA_effort

# Calculate Cronbach's alpha
results_effort <- alpha(effort_combined[c("PE1", "PE2", "PE3", "PE4", "PE5")], check.keys
= TRUE)
print(results_effort$total)

############################################################
########CRONBACH'S ALPHA FOR ALL FACTORS ############################

#############hedonism#############
hedonism_gifted <- subset(smart_speaker_subset_gifted, select = c(H1, H2, H3,H4))
hedonism_owning <- subset(smart_speaker_subset_owning, select = c(Ho1, Ho2, Ho3, Ho4))

# rename columns
names(hedonism_gifted) <- c("H1", "H2", "H3","H4")
names(hedonism_owning) <- c("H1", "H2", "H3","H4")

combined_hedonism <- rbind(hedonism_gifted, hedonism_owning)

#alpha
results_hedonism <- alpha(combined_hedonism[c("H1", "H2", "H3", "H4")], check.keys =
TRUE)
print(results_hedonism$total)

##############usefulness#############
use_gifted <- subset(smart_speaker_subset_gifted, select = c("PU1", "PU2",
"PU3","PU4","PU5"))
use_owning <- subset(smart_speaker_subset_owning, select = c("PUo1", "PUo2",
"PUo3","PUo4","PUo5"))

names(use_gifted) <- c("PU1", "PU2", "PU3","PU4","PU5")
names(use_owning) <- c("PU1", "PU2", "PU3","PU4","PU5")

combined_use <- rbind(use_gifted, use_owning)
view(combined_use)
```

```
#alpha
results_use <- alpha(combined_use[c("PU1", "PU2", "PU3","PU4","PU5")], check.keys =
TRUE)
print(results_use$total)

##############trust##############
trust_gifted <- subset(smart_speaker_subset_gifted, select = c("T1", "T2",
"T3","T4","T5","T6","T7"))
trust_owning <- subset(smart_speaker_subset_owning, select = c("T1", "T2",
"T3","T4","T5","T6","T7"))

#combine datasets
combined_trust <- rbind(trust_gifted, trust_owning)
view(combined_trust)

#alpha
results_trust <- alpha(combined_trust[c("T1", "T2", "T3","T4","T5","T6","T7")], check.keys
= TRUE)
print(results_trust$total)

##############nothing to hide ##############
nth_gifted <- subset(smart_speaker_subset_gifted, select = c("NTH1", "NTH2",
"NTH3","NTH4","NTH5"))
nth_owning <- subset(smart_speaker_subset_owning, select = c("NTH1", "NTH2",
"NTH3","NTH4","NTH5"))

#combine datasets
combined_nth <- rbind(nth_gifted, nth_owning)

#alpha
results_nth <- alpha(combined_nth[c("NTH1", "NTH2", "NTH3","NTH4","NTH5")],
check.keys = TRUE)
print(results_nth$total)

##############resignation##############
resignation_gifted <- subset(smart_speaker_subset_gifted, select = c("R1", "R2", "R3"))
resignation_owning <- subset(smart_speaker_subset_owning, select = c("R1", "R2", "R3"))

#combine datasets
combined_resignation <- rbind(resignation_gifted, resignation_owning)

#alpha
results_resignation <- alpha(combined_resignation[c("R1", "R2", "R3")], check.keys =
TRUE)
```

```
print(results_resignation$total)

###############powerlessness##############
power_gifted <- subset(smart_speaker_subset_gifted, select = c("R4","R5","R6"))
power_owning <- subset(smart_speaker_subset_owning, select = c("R4","R5","R6"))

#combine datasets
combined_power <- rbind(power_gifted, power_owning)

#alpha
results_power <- alpha(combined_power[c("R4","R5","R6")], check.keys = TRUE)
print(results_power$total)

###############privacy self-efficacy##############
efficacy_gifted <- subset(smart_speaker_subset_gifted, select = c("SE1", "SE2", "SE3",
"SE4", "SE5"))
efficacy_owning <- subset(smart_speaker_subset_owning, select = c("SE1", "SE2", "SE3",
"SE4", "SE5"))

#combine datasets
combined_efficacy <- rbind(efficacy_gifted, efficacy_owning)

#alpha
results_efficacy <- alpha(combined_efficacy[c("SE1", "SE2", "SE3", "SE4", "SE5")],
check.keys = TRUE)
print(results_efficacy$total)

###############securitry self-efficacy##############
security_gifted <- subset(smart_speaker_subset_gifted, select = c("SE6", "SE7", "SE8",
"SE9"))
security_owning <- subset(smart_speaker_subset_owning, select = c("SE6", "SE7", "SE8",
"SE9"))

#combine datasets
combined_security <- rbind(security_gifted, security_owning)

#alpha
results_security <- alpha(combined_security[c("SE6", "SE7", "SE8", "SE9")], check.keys =
TRUE)
print(results_security$total)

###############privacy risk perception##############
risk_gifted <- subset(smart_speaker_subset_gifted, select = c("PRP1", "PRP2", "PRP3"))
risk_owning <- subset(smart_speaker_subset_owning, select = c("prpO1", "prpO2",
"prpO3"))
```

```
# rename columns
names(risk_gifted) <- c("PRP1", "PRP2", "PRP3")
names(risk_owning) <- c("PRP1", "PRP2", "PRP3")

#combine datasets
combined_risk <- rbind(risk_gifted, risk_owning)

#alpha
results_risk <- alpha(combined_risk[c("PRP1", "PRP2", "PRP3")], check.keys = TRUE)
print(results_risk$total)

###########################################################################
#######ANOVA testing for POSSESSION PERIOD##################
possession_physical <- subset(smart_speaker_subset_owning, select = c("possession.period.",
"protective_behaviors_physical"))
possession_physical$possession.period. <- factor(possession_physical$possession.period.,
                         levels = c("less than 1 month", "2-3 months", "4 months to 1 year",
                                "1-2 years", "more than 2 years"))


possession_data <- subset(smart_speaker_subset_owning, select = c("possession.period.",
"protective_behaviors_data"))
possession_data$possession.period. <- factor(possession_data$possession.period.,
                         levels = c("less than 1 month", "2-3 months", "4 months to 1 year",
                                "1-2 years", "more than 2 years"))


possession <- subset(smart_speaker_subset_owning, select = c("possession.period.",
"privacy_risk_perception"))
possession$possession.period. <- factor(possession$possession.period.,
                         levels = c("less than 1 month", "2-3 months", "4 months to 1 year",
                                "1-2 years", "more than 2 years"))
levels(possession$possession.period.)
str(possession)

# ANOVA physical protective behaviour
model_possession_physical <- lm(protective_behaviors_physical ~ possession.period., data =
possession_physical)
```

```
anova_results_physical <- anova(model_possession_physical)
print(anova_results_physical)
summary(model_possession_physical)
r_squared_physical <- summary(model_possession_physical)$r.squared
r_squared_physical

#  mean values
mean_values_physical <- possession_physical %>%
  group_by(possession.period.) %>%
  summarise(mean_physical_protective = mean(protective_behaviors_physical))

# bar plot
ggplot(mean_values_physical, aes(x = possession.period., y = mean_physical_protective)) +
  geom_bar(stat = "identity", fill = "skyblue", color = "black") +
  geom_text(aes(label = round(mean_physical_protective, 2)), vjust = -0.5, size = 3.5, color =
"black") +
  labs(x = "Possession Period", y = "Mean Physical Protective Behaviors") +
  ggtitle("Mean Physical Protective Behaviors by Possession Period") +
  theme_minimal() +
  theme(axis.text.x = element_text(angle = 45, hjust = 1))
###############################################
# ANOVA online data handling protective behaviour
model_possession_data <- lm(protective_behaviors_data ~ possession.period., data =
possession_data)
anova_results_data <- anova(model_possession_data)
print(anova_results_data)
summary(model_possession_data)
r_squared_data <- summary(model_possession_data)$r.squared
r_squared_data

# mean values
mean_values_data <- possession_data %>%
  group_by(possession.period.) %>%
  summarise(mean_data_protective = mean(protective_behaviors_data))
```

```
#bar plot
ggplot(mean_values_data, aes(x = possession.period., y = mean_data_protective)) +
  geom_bar(stat = "identity", fill = "skyblue", color = "black") +
  geom_text(aes(label = round(mean_data_protective, 2)), vjust = -0.5, size = 3.5, color =
"black") +
  labs(x = "Possession Period", y = "Mean Online Data Handling Protective Behaviors") +
  ggtitle("Mean Online Data Handling Protective Behaviors by Possession Period") +
  theme_minimal() +
  theme(axis.text.x = element_text(angle = 45, hjust = 1))
#########################################
# ANOVA risk perception
model_possession <- lm(privacy_risk_perception ~ possession.period., data = possession)
anova_results <- anova(model_possession)
print(anova_results)
summary(model_possession)
model_possession$r.squared

#mean values
mean_values <- possession %>%
  group_by(possession.period.) %>%
  summarise(mean_privacy_risk = mean(privacy_risk_perception))

#bar plot
ggplot(mean_values, aes(x = possession.period., y = mean_privacy_risk)) +
  geom_bar(stat = "identity", fill = "skyblue", color = "black") +
  geom_text(aes(label = round(mean_privacy_risk, 2)), vjust = -0.5, size = 3.5, color =
"black") +
  labs(x = "Possession Period", y = "Mean Privacy Risk Perception") +
  ggtitle("Mean Privacy Risk Perception by Possession Period") +
  theme_minimal() +
  theme(axis.text.x = element_text(angle = 45, hjust = 1))
###########################################################################
###########################################################
```

```
#CREATING OVERALL COMBINED DATASET FOR BOTH CONDITIONS with
composite scores ####
########

# Select specified columns from smart_speaker_subset_gifted
subset_gifted <- smart_speaker_subset_gifted[, c("privacy_risk_perception",
"protective_behaviors_physical", "protective_behaviors_data", "perceived_enjoyableness",
"perceived_usefulness", "perceived_effort", "perceived_trust_companies", "nothing_to_hide",
"resignation_2", "powerlessness_2","social_norm_2", "self_efficacy", "security_efficacy")]

# Select specified columns from smart_speaker_subset_owning
subset_owning <- smart_speaker_subset_owning[, c("privacy_risk_perception",
"protective_behaviors_physical", "protective_behaviors_data", "perceived_enjoyableness",
"perceived_usefulness", "perceived_effort", "perceived_trust_companies", "nothing_to_hide",
"resignation_2", "powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")]

# Rename columns gifted
colnames(subset_gifted) <- c("privacy_risk_perception", "protective_behaviors_physical",
"protective_behaviors_data", "perceived_enjoyableness", "perceived_usefulness",
"perceived_effort", "perceived_trust_companies", "nothing_to_hide", "resignation_2",
"powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")

# Rename columns owning
colnames(subset_owning) <- c("privacy_risk_perception", "protective_behaviors_physical",
"protective_behaviors_data", "perceived_enjoyableness", "perceived_usefulness",
"perceived_effort", "perceived_trust_companies", "nothing_to_hide", "resignation_2",
"powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")

# Combine the selected columns into a new dataset
combined_composite <- rbind(subset_gifted, subset_owning)

view(combined_composite)

#######
#CREATING OVERALL COMBINED DATASET FOR BOTH CONDITIONS with
composite scores ####
########

# Select specified columns from smart_speaker_subset_gifted
subset_gifted_1 <- smart_speaker_subset_gifted[, c("privacy_risk_perception",
"protective_behaviors_physical", "protective_behaviors_data", "perceived_enjoyableness",
"perceived_usefulness", "perceived_effort", "perceived_trust_companies", "nothing_to_hide",
"resignation_2", "powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")]

# Select specified columns from smart_speaker_subset_owning
```

```
subset_owning_1 <- smart_speaker_subset_owning[, c("privacy_risk_perception",
"protective_behaviors_physical", "protective_behaviors_data", "perceived_enjoyableness",
"perceived_usefulness", "perceived_effort", "perceived_trust_companies", "nothing_to_hide",
"resignation_2", "powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")]

# Rename columns gifted
colnames(subset_gifted_1) <- c("privacy_risk_perception", "protective_behaviors_physical",
"protective_behaviors_data", "perceived_enjoyableness", "perceived_usefulness",
"perceived_effort", "perceived_trust_companies", "nothing_to_hide", "resignation_2",
"powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")

# Rename columns owning
colnames(subset_owning_1) <- c("privacy_risk_perception",
"protective_behaviors_physical", "protective_behaviors_data", "perceived_enjoyableness",
"perceived_usefulness", "perceived_effort", "perceived_trust_companies", "nothing_to_hide",
"resignation_2", "powerlessness_2", "social_norm_2", "self_efficacy", "security_efficacy")

# Combine the selected columns into a new dataset
combined_dataset <- rbind(subset_gifted_1, subset_owning_1)

view(combined_dataset)

############################################################################
############# CORRELATION ANALYSIS ####################################
#combined correlation but for each variable
#### correlation analysis Hedonism + PRIVACY RISK####################
variable_hed <- c("privacy_risk_perception", "perceived_enjoyableness")
correlation_matrix_hed <- cor(combined_composite[, variable_hed])
print(correlation_matrix_hed)
describe(correlation_matrix_hed)
correlation_test_hed <- cor.test(combined_composite$privacy_risk_perception,
combined_composite$perceived_enjoyableness)
print(correlation_test_hed)

#### correlation analysis Hedonism + protective behaviors physical ####################
variable_hed_pb <- c("protective_behaviors_physical", "perceived_enjoyableness")
correlation_matrix_hed_pb <- cor(combined_composite[, variable_hed_pb])
print(correlation_matrix_hed_pb)
describe(correlation_matrix_hed_pb)
correlation_test_hed_pb <- cor.test(combined_composite$protective_behaviors_physical,
combined_composite$perceived_enjoyableness)
print(correlation_test_hed_pb)

#### correlation analysis Hedonism + protective behaviors data ####################
variable_hed_pbd <- c("protective_behaviors_data", "perceived_enjoyableness")
```

```
correlation_matrix_hed_pbd <- cor(combined_composite[, variable_hed_pbd])
print(correlation_matrix_hed_pbd)
describe(correlation_matrix_hed_pbd)
correlation_test_hed_pbd <- cor.test(combined_composite$protective_behaviors_data,
combined_composite$perceived_enjoyableness)
print(correlation_test_hed_pbd)

######################################################
#### correlation analysis usefulness + PRIVACY RISK####################
variable_use <- c("privacy_risk_perception", "perceived_usefulness")
correlation_matrix_use <- cor(combined_composite[, variable_use])
print(correlation_matrix_use)
describe(correlation_matrix_use)
correlation_test_use <- cor.test(combined_composite$privacy_risk_perception,
combined_composite$perceived_usefulness)
print(correlation_test_use)

#### correlation analysis Usefulness + protective behaviors physical ####################
variable_use_pb <- c("protective_behaviors_physical", "perceived_usefulness")
correlation_matrix_use_pb <- cor(combined_composite[, variable_use_pb])
print(correlation_matrix_use_pb)
describe(correlation_matrix_use_pb)
correlation_test_use_pb <- cor.test(combined_composite$protective_behaviors_physical,
combined_composite$perceived_usefulness)
print(correlation_test_use_pb)

#### correlation analysis Usefulness + protective behaviors data ####################
variable_use_pbd <- c("protective_behaviors_data", "perceived_usefulness")
correlation_matrix_use_pbd <- cor(combined_dataset[, variable_use_pbd])
print(correlation_matrix_use_pbd)
describe(correlation_matrix_use_pbd)
correlation_test_use_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$perceived_usefulness)
print(correlation_test_use_pbd)

######################################################
#### correlation analysis trust + PRIVACY RISK####################
variable_trust <- c("privacy_risk_perception", "perceived_trust_companies")
correlation_matrix_trust <- cor(combined_dataset[, variable_trust])
print(correlation_matrix_trust)
describe(correlation_matrix_trust)
correlation_test_trust <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$perceived_trust_companies)
print(correlation_test_trust)
```

```
#### correlation analysis Trust + protective behaviors physical####################
variable_trust_pb <- c("protective_behaviors_physical", "perceived_trust_companies")
correlation_matrix_trust_pb <- cor(combined_dataset[, variable_trust_pb])
print(correlation_matrix_trust_pb)
describe(correlation_matrix_trust_pb)
correlation_test_trust_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$perceived_trust_companies)
print(correlation_test_trust_pb)

#### correlation analysis Trust + protective behaviors data####################
variable_trust_pbd <- c("protective_behaviors_data", "perceived_trust_companies")
correlation_matrix_trust_pbd <- cor(combined_dataset[, variable_trust_pbd])
print(correlation_matrix_trust_pbd)
describe(correlation_matrix_trust_pbd)
correlation_test_trust_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$perceived_trust_companies)
print(correlation_test_trust_pbd)

########################################################
#### correlation analysis nothing to hide + PRIVACY RISK####################
variable_hide <- c("privacy_risk_perception", "nothing_to_hide")
correlation_matrix_hide <- cor(combined_dataset[, variable_hide])
print(correlation_matrix_hide)
describe(correlation_matrix_hide)
correlation_test_hide <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$nothing_to_hide)
print(correlation_test_hide)

#### correlation analysis nothing to hide + protective behaviors
physical####################
variable_hide_pb <- c("protective_behaviors_physical", "nothing_to_hide")
correlation_matrix_hide_pb <- cor(combined_dataset[, variable_hide_pb])
print(correlation_matrix_hide_pb)
describe(correlation_matrix_hide_pb)
correlation_test_hide_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$nothing_to_hide)
print(correlation_test_hide_pb)

#### correlation analysis nothing to hide + protective behaviors data
handling####################
variable_hide_pbd <- c("protective_behaviors_data", "nothing_to_hide")
correlation_matrix_hide_pbd <- cor(combined_dataset[, variable_hide_pbd])
print(correlation_matrix_hide_pbd)
describe(correlation_matrix_hide_pbd)
```

```
correlation_test_hide_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$nothing_to_hide)
print(correlation_test_hide_pbd)

###################################################################
#### correlation analysis resignation + PRIVACY RISK#########################
variable_resignation <- c("privacy_risk_perception", "resignation_2")
correlation_matrix_resignation <- cor(combined_dataset[, variable_resignation])
print(correlation_matrix_resignation)
describe(correlation_matrix_resignation)
correlation_test_resignation <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$resignation_2)
print(correlation_test_resignation)

#### correlation analysis Resignation + protective behaviors
physical########################
variable_resignation_pb <- c("protective_behaviors_physical", "resignation_2")
correlation_matrix_resignation_pb <- cor(combined_dataset[, variable_resignation_pb])
print(correlation_matrix_resignation_pb)
describe(correlation_matrix_resignation_pb)
correlation_test_resignation_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$resignation_2)
print(correlation_test_resignation_pb)

#### correlation analysis Resignation + protective behaviors data#########################
variable_resignation_pbd <- c("protective_behaviors_data", "resignation_2")
correlation_matrix_resignation_pbd <- cor(combined_dataset[, variable_resignation_pbd])
print(correlation_matrix_resignation_pbd)
describe(correlation_matrix_resignation_pbd)
correlation_test_resignation_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$resignation_2)
print(correlation_test_resignation_pbd)

###################################################################
#### correlation analysis powerlessness + PRIVACY RISK#########################
variable_pow<- c("privacy_risk_perception", "powerlessness_2")
correlation_matrix_pow <- cor(combined_dataset[, variable_pow])
print(correlation_matrix_pow)
describe(correlation_matrix_pow)
correlation_test_pow <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$powerlessness_2)
print(correlation_test_pow)

###################################################################
#### correlation analysis social norm + protective behaviors physical#########################
```

```
variable_so_pb <- c("protective_behaviors_physical", "social_norm_2")
correlation_matrix_so_pb <- cor(combined_dataset[, variable_so_pb])
print(correlation_matrix_so_pb)
describe(correlation_matrix_so_pb)
correlation_test_so_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$social_norm_2)
print(correlation_test_so_pb)

#### correlation analysis social norm + protective behaviors data
variable_so_pbd <- c("protective_behaviors_data", "social_norm_2")
correlation_matrix_so_pbd <- cor(combined_dataset[, variable_so_pbd])
print(correlation_matrix_so_pbd)
describe(correlation_matrix_so_pbd)
correlation_test_so_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$social_norm_2)
print(correlation_test_so_pbd)

######################################################
#### correlation analysis self_efficacy + PRIVACY RISK####################
variable_eff <- c("privacy_risk_perception", "self_efficacy")
correlation_matrix_eff <- cor(combined_dataset[, variable_eff])
print(correlation_matrix_eff)
describe(correlation_matrix_eff)
correlation_test_eff <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$self_efficacy)
print(correlation_test_eff)

#### correlation analysis self_efficacy + protective behaviors
physical####################
variable_eff_pb <- c("protective_behaviors_physical", "self_efficacy")
correlation_matrix_eff_pb <- cor(combined_dataset[, variable_eff_pb])
print(correlation_matrix_eff_pb)
describe(correlation_matrix_eff_pb)
correlation_test_eff_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$self_efficacy)
print(correlation_test_eff_pb)

#### correlation analysis self_efficacy + protective behaviors data
handling####################
variable_eff_pbd <- c("protective_behaviors_data", "self_efficacy")
correlation_matrix_eff_pbd <- cor(combined_dataset[, variable_eff_pbd])
print(correlation_matrix_eff_pbd)
describe(correlation_matrix_eff_pbd)
correlation_test_eff_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$self_efficacy)
```

```
print(correlation_test_eff_pbd)

#######################################################
#### correlation analysis security_efficacy + PRIVACY RISK####################
variable_security <- c("privacy_risk_perception", "security_efficacy")
correlation_matrix_security <- cor(combined_dataset[, variable_security])
print(correlation_matrix_security)
describe(correlation_matrix_security)
correlation_test_security <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$security_efficacy)
print(correlation_test_security)

#### correlation analysis security_efficacy + protective behaviors
physical####################
variable_security_pb <- c("protective_behaviors_physical", "security_efficacy")
correlation_matrix_security_pb <- cor(combined_dataset[, variable_security_pb])
print(correlation_matrix_security_pb)
describe(correlation_matrix_security_pb)
correlation_test_security_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$security_efficacy)
print(correlation_test_security_pb)

#### correlation analysis security_efficacy + protective behaviors
data####################
variable_security_pbd <- c("protective_behaviors_data", "security_efficacy")
correlation_matrix_security_pbd <- cor(combined_dataset[, variable_security_pbd])
print(correlation_matrix_security_pbd)
describe(correlation_matrix_security_pbd)
correlation_test_security_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$security_efficacy)
print(correlation_test_security_pbd)

#######################################################
#### correlation analysis effort + protective behaviors physical####################
variable_effort_pb <- c("protective_behaviors_physical", "perceived_effort")
correlation_matrix_effort_pb <- cor(combined_dataset[, variable_effort_pb])
print(correlation_matrix_effort_pb)
describe(correlation_matrix_effort_pb)
correlation_test_effort_pb <- cor.test(combined_dataset$protective_behaviors_physical,
combined_dataset$perceived_effort)
print(correlation_test_effort_pb)

#### correlation analysis effort + protective behaviors data####################
variable_effort_pbd <- c("protective_behaviors_data", "perceived_effort")
correlation_matrix_effort_pbd <- cor(combined_dataset[, variable_effort_pbd])
```

```
print(correlation_matrix_effort_pbd)
describe(correlation_matrix_effort_pbd)
correlation_test_effort_pbd <- cor.test(combined_dataset$protective_behaviors_data,
combined_dataset$perceived_effort)
print(correlation_test_effort_pbd)

#######################################################
#### correlation analysis Protective Behaviour physical + PRIVACY
RISK####################
variable_behavior <- c("privacy_risk_perception", "protective_behaviors_physical")
correlation_matrix_behavior <- cor(combined_dataset[, variable_behavior])
print(correlation_matrix_behavior)
describe(correlation_matrix_behavior)
correlation_test_behavior <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$protective_behaviors_physical)
print(correlation_test_behavior)

#### correlation analysis Protective Behavior data handling + PRIVACY
RISK####################
variable_behavior_pbd <- c("privacy_risk_perception", "protective_behaviors_data")
correlation_matrix_behavior_pbd <- cor(combined_dataset[, variable_behavior_pbd])
print(correlation_matrix_behavior_pbd)
describe(correlation_matrix_behavior_pbd)
correlation_test_behavior_pbd <- cor.test(combined_dataset$privacy_risk_perception,
combined_dataset$protective_behaviors_data)
print(correlation_test_behavior_pbd)
#####################################################################
##### GIFTED SCENARIO###############
###### protective behaviors physical + privacy risk
variable_pb_prp <- c("privacy_risk_perception", "protective_behaviors_physical")
correlation_matrix_pb_prp <- cor(smart_speaker_subset_gifted[, variable_pb_prp])
print(correlation_matrix_pb_prp)
describe(correlation_matrix_pb_prp)
correlation_test_pb_prp <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$protective_behaviors_physical)
print(correlation_test_pb_prp)

###### protective behaviors data handling + privacy risk
variable_pbd_prp <- c("privacy_risk_perception", "protective_behaviors_data")
correlation_matrix_pbd_prp <- cor(smart_speaker_subset_gifted[, variable_pbd_prp])
print(correlation_matrix_pbd_prp)
describe(correlation_matrix_pbd_prp)
correlation_test_pbd_prp <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$protective_behaviors_data)
print(correlation_test_pbd_prp)
```

```
###### HEDONISM + privacy risk
variable_hed <- c("privacy_risk_perception", "perceived_enjoyableness")
correlation_matrix_hed <- cor(smart_speaker_subset_gifted[, variable_hed])
print(correlation_matrix_hed)
describe(correlation_matrix_hed)
correlation_test_hed <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$perceived_enjoyableness)
print(correlation_test_hed)

###### HEDONISM + protective behaviors physical
variable_hed_pb <- c("protective_behaviors_physical", "perceived_enjoyableness")
correlation_matrix_hed_pb <- cor(smart_speaker_subset_gifted[, variable_hed_pb])
print(correlation_matrix_hed_pb)
describe(correlation_matrix_hed_pb)
correlation_test_hed_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$perceived_enjoyableness)
print(correlation_test_hed_pb)

##### HEDONISM + protective behaviors data handling
variable_hed_pbd <- c("protective_behaviors_data", "perceived_enjoyableness")
correlation_matrix_hed_pbd <- cor(smart_speaker_subset_gifted[, variable_hed_pbd])
print(correlation_matrix_hed_pbd)
describe(correlation_matrix_hed_pbd)
correlation_test_hed_pbd <- cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$perceived_enjoyableness)
print(correlation_test_hed_pbd)

###### USEFULNESS + privacy risk
variable_use <- c("privacy_risk_perception", "perceived_usefulness")
correlation_matrix_use <- cor(smart_speaker_subset_gifted[, variable_use])
print(correlation_matrix_use)
describe(correlation_matrix_use)
correlation_test_use <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$perceived_usefulness)
print(correlation_test_use)

###### USEFULNESS + protective behaviors physical
variable_use_pb <- c("protective_behaviors_physical", "perceived_usefulness")
correlation_matrix_use_pb <- cor(smart_speaker_subset_gifted[, variable_use_pb])
print(correlation_matrix_use_pb)
describe(correlation_matrix_use_pb)
```

```
correlation_test_use_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$perceived_usefulness)
print(correlation_test_use_pb)

###### USEFULNESS + protective behaviors data handling
variable_use_pbd <- c("protective_behaviors_data", "perceived_usefulness")
correlation_matrix_use_pbd <- cor(smart_speaker_subset_gifted[, variable_use_pbd])
print(correlation_matrix_use_pbd)
describe(correlation_matrix_use_pbd)
correlation_test_use_pbd <- cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$perceived_usefulness)
print(correlation_test_use_pbd)

###### TRUST + privacy risk
variable_trust <- c("privacy_risk_perception", "perceived_trust_companies")
correlation_matrix_trust <- cor(smart_speaker_subset_gifted[, variable_trust])
print(correlation_matrix_trust)
describe(correlation_matrix_trust)
correlation_test_trust <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$perceived_trust_companies)
print(correlation_test_trust)

###### TRUST + protective behaviors physical
variable_trust_pb <- c("protective_behaviors_physical", "perceived_trust_companies")
correlation_matrix_trust_pb <- cor(smart_speaker_subset_gifted[, variable_trust_pb])
print(correlation_matrix_trust_pb)
describe(correlation_matrix_trust_pb)
correlation_test_trust_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$perceived_trust_companies)
print(correlation_test_trust_pb)

###### TRUST + protective behaviors data
variable_trust_pbd <- c("protective_behaviors_data", "perceived_trust_companies")
correlation_matrix_trust_pbd <- cor(smart_speaker_subset_gifted[, variable_trust_pbd])
print(correlation_matrix_trust_pbd)
describe(correlation_matrix_trust_pbd)
correlation_test_trust_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$perceived_trust_companies)
print(correlation_test_trust_pbd)

###### NOTHING TO HIDE + privacy risk
variable_hide <- c("privacy_risk_perception", "nothing_to_hide")
```

```
correlation_matrix_hide <- cor(smart_speaker_subset_gifted[, variable_hide])
print(correlation_matrix_hide)
describe(correlation_matrix_hide)
correlation_test_hide <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$nothing_to_hide)
print(correlation_test_hide)

###### NOTHING TO HIDE + protective behaviors physical
variable_hide_pb <- c("protective_behaviors_physical", "nothing_to_hide")
correlation_matrix_hide_pb <- cor(smart_speaker_subset_gifted[, variable_hide_pb])
print(correlation_matrix_hide_pb)
describe(correlation_matrix_hide_pb)
correlation_test_hide_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$nothing_to_hide)
print(correlation_test_hide_pb)

###### NOTHING TO HIDE + protective behaviors data handling
variable_hide_pbd <- c("protective_behaviors_data", "nothing_to_hide")
correlation_matrix_hide_pbd <- cor(smart_speaker_subset_gifted[, variable_hide_pbd])
print(correlation_matrix_hide_pbd)
describe(correlation_matrix_hide_pbd)
correlation_test_hide_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$nothing_to_hide)
print(correlation_test_hide_pbd)

###### RESIGNATION + privacy risk
variable_res <- c("privacy_risk_perception", "resignation_2")
correlation_matrix_res <- cor(smart_speaker_subset_gifted[, variable_res])
print(correlation_matrix_res)
describe(correlation_matrix_res)
correlation_test_res <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$resignation_2)
print(correlation_test_res)

###### RESIGNATION + protective behaviors physical
variable_res_pb <- c("protective_behaviors_physical", "resignation_2")
correlation_matrix_res_pb <- cor(smart_speaker_subset_gifted[, variable_res_pb])
print(correlation_matrix_res_pb)
describe(correlation_matrix_res_pb)
correlation_test_res_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$resignation_2)
print(correlation_test_res_pb)
```

```
###### RESIGNATION + protective behaviors data handling
variable_res_pbd <- c("protective_behaviors_data", "resignation_2")
correlation_matrix_res_pbd <- cor(smart_speaker_subset_gifted[, variable_res_pbd])
print(correlation_matrix_res_pbd)
describe(correlation_matrix_res_pbd)
correlation_test_res_pbd <- cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$resignation_2)
print(correlation_test_res_pbd)

###### POWERLESSNESS + privacy risk
variable_pow <- c("privacy_risk_perception", "powerlessness_2")
correlation_matrix_pow <- cor(smart_speaker_subset_gifted[, variable_pow])
print(correlation_matrix_pow)
describe(correlation_matrix_pow)
correlation_test_pow <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$powerlessness_2)
print(correlation_test_pow)

###### POWERLESSNESS + protective behaviors physical
variable_pow_pb <- c("protective_behaviors_physical", "powerlessness_2")
correlation_matrix_pow_pb <- cor(smart_speaker_subset_gifted[, variable_pow_pb])
print(correlation_matrix_pow_pb)
describe(correlation_matrix_pow_pb)
correlation_test_pow_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$powerlessness_2)
print(correlation_test_pow_pb)

###### POWERLESSNESS + protective behaviors data handling
variable_pow_pbd <- c("protective_behaviors_data", "powerlessness_2")
correlation_matrix_pow_pbd <- cor(smart_speaker_subset_gifted[, variable_pow_pbd])
print(correlation_matrix_pow_pbd)
describe(correlation_matrix_pow_pbd)
correlation_test_pow_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$powerlessness_2)
print(correlation_test_pow_pbd)

###### PRIVACY SELF-EFFICACY + privacy risk
variable_self <- c("privacy_risk_perception", "self_efficacy")
correlation_matrix_self <- cor(smart_speaker_subset_gifted[, variable_self])
print(correlation_matrix_self)
describe(correlation_matrix_self)
```

```
correlation_test_self <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$self_efficacy)
print(correlation_test_self)

###### PRIVACY SELF-EFFICACY + protective behaviors physical
variable_self_pb <- c("protective_behaviors_physical", "self_efficacy")
correlation_matrix_self_pb <- cor(smart_speaker_subset_gifted[, variable_self_pb])
print(correlation_matrix_self_pb)
describe(correlation_matrix_self_pb)
correlation_test_self_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$self_efficacy)
print(correlation_test_self_pb)

###### PRIVACY SELF-EFFICACY + protective behaviors data handling
variable_self_pbd <- c("protective_behaviors_data", "self_efficacy")
correlation_matrix_self_pbd <- cor(smart_speaker_subset_gifted[, variable_self_pbd])
print(correlation_matrix_self_pbd)
describe(correlation_matrix_self_pbd)
correlation_test_self_pbd <- cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$self_efficacy)
print(correlation_test_self_pbd)

###### SECURITY SELF-EFFICACY + privacy risk
variable_security <- c("privacy_risk_perception", "security_efficacy")
correlation_matrix_security <- cor(smart_speaker_subset_gifted[, variable_security])
print(correlation_matrix_security)
describe(correlation_matrix_security)
correlation_test_security <- cor.test(smart_speaker_subset_gifted$privacy_risk_perception,
smart_speaker_subset_gifted$security_efficacy)
print(correlation_test_security)

###### SECURITY SELF-EFFICACY + protective behaviors physical
variable_security_pb <- c("protective_behaviors_physical", "security_efficacy")
correlation_matrix_security_pb <- cor(smart_speaker_subset_gifted[, variable_security_pb])
print(correlation_matrix_security_pb)
describe(correlation_matrix_security_pb)
correlation_test_security_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$security_efficacy)
print(correlation_test_security_pb)

###### SECURITY SELF-EFFICACY + protective behaviors data handling
variable_security_pbd <- c("protective_behaviors_data", "security_efficacy")
```

```
correlation_matrix_security_pbd <- cor(smart_speaker_subset_gifted[,
variable_security_pbd])
print(correlation_matrix_security_pbd)
describe(correlation_matrix_security_pbd)
correlation_test_security_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$security_efficacy)
print(correlation_test_security_pbd)


###### SOCIAL NORM + protective behaviors physical
variable_norm_pb <- c("protective_behaviors_physical", "social_norm_2")
correlation_matrix_norm_pb <- cor(smart_speaker_subset_gifted[, variable_norm_pb])
print(correlation_matrix_norm_pb)
describe(correlation_matrix_norm_pb)
correlation_test_norm_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$social_norm_2)
print(correlation_test_norm_pb)

###### SOCIAL NORM + protective behaviors data
variable_norm_pbd <- c("protective_behaviors_data", "social_norm_2")
correlation_matrix_norm_pbd <- cor(smart_speaker_subset_gifted[, variable_norm_pbd])
print(correlation_matrix_norm_pbd)
describe(correlation_matrix_norm_pbd)
correlation_test_norm_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$social_norm_2)
print(correlation_test_norm_pbd)


###### EFFORT + protective behaviors physical
variable_effort_pb <- c("protective_behaviors_physical", "perceived_effort")
correlation_matrix_effort_pb <- cor(smart_speaker_subset_gifted[, variable_effort_pb])
print(correlation_matrix_effort_pb)
describe(correlation_matrix_effort_pb)
correlation_test_effort_pb <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_physical,
smart_speaker_subset_gifted$perceived_effort)
print(correlation_test_effort_pb)

###### EFFORT + protective behaviors data handling
variable_effort_pbd <- c("protective_behaviors_data", "perceived_effort")
correlation_matrix_effort_pbd <- cor(smart_speaker_subset_gifted[, variable_effort_pbd])
print(correlation_matrix_effort_pbd)
```

```
describe(correlation_matrix_effort_pbd)
correlation_test_effort_pbd <-
cor.test(smart_speaker_subset_gifted$protective_behaviors_data,
smart_speaker_subset_gifted$perceived_effort)
print(correlation_test_effort_pbd)

######################################
####### OWNING SCENARIO ############

###### protective behaviors physical + privacy risk
variable_pb_prp_ow <- c("privacy_risk_perception", "protective_behaviors_physical")
correlation_matrix_pb_prp_ow <- cor(smart_speaker_subset_owning[, variable_pb_prp_ow])
print(correlation_matrix_pb_prp_ow)
describe(correlation_matrix_pb_prp_ow)
correlation_test_pb_prp_ow <-
cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$protective_behaviors_physical)
print(correlation_test_pb_prp_ow)

###### protective behaviors data handling + privacy risk
variable_pbd_prp_ow <- c("privacy_risk_perception", "protective_behaviors_data")
correlation_matrix_pbd_prp_ow <- cor(smart_speaker_subset_owning[,
variable_pbd_prp_ow])
print(correlation_matrix_pbd_prp_ow)
describe(correlation_matrix_pbd_prp_ow)
correlation_test_pbd_prp_ow <-
cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$protective_behaviors_data)
print(correlation_test_pbd_prp_ow)

###### HEDONISM + privacy risk
variable_hed_ow <- c("privacy_risk_perception", "perceived_enjoyableness")
correlation_matrix_hed_ow <- cor(smart_speaker_subset_owning[, variable_hed_ow])
print(correlation_matrix_hed_ow)
describe(correlation_matrix_hed_ow)
correlation_test_hed_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$perceived_enjoyableness)
print(correlation_test_hed_ow)

###### HEDONISM + protective behaviors physical
variable_hed_pb_ow <- c("protective_behaviors_physical", "perceived_enjoyableness")
correlation_matrix_hed_pb_ow <- cor(smart_speaker_subset_owning[, variable_hed_pb_ow])
print(correlation_matrix_hed_pb_ow)
describe(correlation_matrix_hed_pb_ow)
```

```
correlation_test_hed_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$perceived_enjoyableness)
print(correlation_test_hed_pb_ow)

###### HEDONISM + protective behaviors data handling
variable_hed_pbd_ow <- c("protective_behaviors_data", "perceived_enjoyableness")
correlation_matrix_hed_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_hed_pbd_ow])
print(correlation_matrix_hed_pbd_ow)
describe(correlation_matrix_hed_pbd_ow)
correlation_test_hed_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$perceived_enjoyableness)
print(correlation_test_hed_pbd_ow)

###### USEFULNESS + privacy risk
variable_use_ow <- c("privacy_risk_perception", "perceived_usefulness")
correlation_matrix_use_ow <- cor(smart_speaker_subset_owning[, variable_use_ow])
print(correlation_matrix_use_ow)
describe(correlation_matrix_use_ow)
correlation_test_use_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$perceived_usefulness)
print(correlation_test_use_ow)

###### USEFULNESS + protective behaviors physical
variable_use_pb_ow <- c("protective_behaviors_physical", "perceived_usefulness")
correlation_matrix_use_pb_ow <- cor(smart_speaker_subset_owning[, variable_use_pb_ow])
print(correlation_matrix_use_pb_ow)
describe(correlation_matrix_use_pb_ow)
correlation_test_use_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$perceived_usefulness)
print(correlation_test_use_pb_ow)

###### USEFULNESS + protective behaviors data handling
variable_use_pbd_ow <- c("protective_behaviors_data", "perceived_usefulness")
correlation_matrix_use_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_use_pbd_ow])
print(correlation_matrix_use_pbd_ow)
describe(correlation_matrix_use_pbd_ow)
correlation_test_use_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$perceived_usefulness)
print(correlation_test_use_pbd_ow)
```

```
###### TRUST + privacy risk
variable_trust_ow <- c("privacy_risk_perception", "perceived_trust_companies")
correlation_matrix_trust_ow <- cor(smart_speaker_subset_owning[, variable_trust_ow])
print(correlation_matrix_trust_ow)
describe(correlation_matrix_trust_ow)
correlation_test_trust_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$perceived_trust_companies)
print(correlation_test_trust_ow)

###### TRUST + protective behaviors physical
variable_trust_pb_ow <- c("protective_behaviors_physical", "perceived_trust_companies")
correlation_matrix_trust_pb_ow <- cor(smart_speaker_subset_owning[,
variable_trust_pb_ow])
print(correlation_matrix_trust_pb_ow)
describe(correlation_matrix_trust_pb_ow)
correlation_test_trust_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$perceived_trust_companies)
print(correlation_test_trust_pb_ow)

###### TRUST + protective behaviors data
variable_trust_pbd_ow <- c("protective_behaviors_data", "perceived_trust_companies")
correlation_matrix_trust_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_trust_pbd_ow])
print(correlation_matrix_trust_pbd_ow)
describe(correlation_matrix_trust_pbd_ow)
correlation_test_trust_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$perceived_trust_companies)
print(correlation_test_trust_pbd_ow)

###### NOTHING TO HIDE + privacy risk
variable_hide_ow <- c("privacy_risk_perception", "nothing_to_hide")
correlation_matrix_hide_ow <- cor(smart_speaker_subset_owning[, variable_hide_ow])
print(correlation_matrix_hide_ow)
describe(correlation_matrix_hide_ow)
correlation_test_hide_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$nothing_to_hide)
print(correlation_test_hide_ow)

###### NOTHING TO HIDE + protective behaviors physical
variable_hide_pb_ow <- c("protective_behaviors_physical", "nothing_to_hide")
correlation_matrix_hide_pb_ow <- cor(smart_speaker_subset_owning[,
variable_hide_pb_ow])
```

```
print(correlation_matrix_hide_pb_ow)
describe(correlation_matrix_hide_pb_ow)
correlation_test_hide_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$nothing_to_hide)
print(correlation_test_hide_pb_ow)

###### NOTHING TO HIDE + protective behaviors data
variable_hide_pbd_ow <- c("protective_behaviors_data", "nothing_to_hide")
correlation_matrix_hide_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_hide_pbd_ow])
print(correlation_matrix_hide_pbd_ow)
describe(correlation_matrix_hide_pbd_ow)
correlation_test_hide_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$nothing_to_hide)
print(correlation_test_hide_pbd_ow)

###### RESIGNATION + privacy risk
variable_res_ow <- c("privacy_risk_perception", "resignation_2")
correlation_matrix_res_ow <- cor(smart_speaker_subset_owning[, variable_res_ow])
print(correlation_matrix_res_ow)
describe(correlation_matrix_res_ow)
correlation_test_res_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$resignation_2)
print(correlation_test_res_ow)

###### RESIGNATION + protective behaviors physical
variable_res_pb_ow <- c("protective_behaviors_physical", "resignation_2")
correlation_matrix_res_pb_ow <- cor(smart_speaker_subset_owning[, variable_res_pb_ow])
print(correlation_matrix_res_pb_ow)
describe(correlation_matrix_res_pb_ow)
correlation_test_res_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$resignation_2)
print(correlation_test_res_pb_ow)

###### RESIGNATION + protective behaviors data
variable_res_pbd_ow <- c("protective_behaviors_data", "resignation_2")
correlation_matrix_res_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_res_pbd_ow])
print(correlation_matrix_res_pbd_ow)
describe(correlation_matrix_res_pbd_ow)
```

```
correlation_test_res_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$resignation_2)
print(correlation_test_res_pbd_ow)

###### POWERLESSNESS + privacy risk
variable_pow_ow <- c("privacy_risk_perception", "powerlessness_2")
correlation_matrix_pow_ow <- cor(smart_speaker_subset_owning[, variable_pow_ow])
print(correlation_matrix_pow_ow)
describe(correlation_matrix_pow_ow)
correlation_test_pow_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$powerlessness_2)
print(correlation_test_pow_ow)

###### POWERLESSNESS + protective behaviors  physical
variable_pow_pb_ow <- c("protective_behaviors_physical", "powerlessness_2")
correlation_matrix_pow_pb_ow <- cor(smart_speaker_subset_owning[,
variable_pow_pb_ow])
print(correlation_matrix_pow_pb_ow)
describe(correlation_matrix_pow_pb_ow)
correlation_test_pow_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$powerlessness_2)
print(correlation_test_pow_pb_ow)

###### POWERLESSNESS + protective behaviors  data handling
variable_pow_pbd_ow <- c("protective_behaviors_data", "powerlessness_2")
correlation_matrix_pow_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_pow_pbd_ow])
print(correlation_matrix_pow_pbd_ow)
describe(correlation_matrix_pow_pbd_ow)
correlation_test_pow_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$powerlessness_2)
print(correlation_test_pow_pbd_ow)

###### PRIVACY SELF-EFFICACY + privacy risk
variable_self_ow <- c("privacy_risk_perception", "self_efficacy")
correlation_matrix_self_ow <- cor(smart_speaker_subset_owning[, variable_self_ow])
print(correlation_matrix_self_ow)
describe(correlation_matrix_self_ow)
correlation_test_self_ow <- cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$self_efficacy)
print(correlation_test_self_ow)
```

```
###### PRIVACY SELF-EFFICACY + protective behaviors physical
variable_self_pb_ow <- c("protective_behaviors_physical", "self_efficacy")
correlation_matrix_self_pb_ow <- cor(smart_speaker_subset_owning[, variable_self_pb_ow])
print(correlation_matrix_self_pb_ow)
describe(correlation_matrix_self_pb_ow)
correlation_test_self_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$self_efficacy)
print(correlation_test_self_pb_ow)

###### PRIVACY SELF-EFFICACY + protective behaviors data handling
variable_self_pbd_ow <- c("protective_behaviors_data", "self_efficacy")
correlation_matrix_self_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_self_pbd_ow])
print(correlation_matrix_self_pbd_ow)
describe(correlation_matrix_self_pbd_ow)
correlation_test_self_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$self_efficacy)
print(correlation_test_self_pbd_ow)

###### SECURITY SELF-EFFICACY + privacy risk
variable_security_ow <- c("privacy_risk_perception", "security_efficacy")
correlation_matrix_security_ow <- cor(smart_speaker_subset_owning[,
variable_security_ow])
print(correlation_matrix_security_ow)
describe(correlation_matrix_security_ow)
correlation_test_security_ow <-
cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$security_efficacy)
print(correlation_test_security_ow)

###### SECURITY SELF-EFFICACY + protective behaviors physical
variable_security_pb_ow <- c("protective_behaviors_physical", "security_efficacy")
correlation_matrix_security_pb_ow <- cor(smart_speaker_subset_owning[,
variable_security_pb_ow])
print(correlation_matrix_security_pb_ow)
describe(correlation_matrix_security_pb_ow)
correlation_test_security_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$security_efficacy)
print(correlation_test_security_pb_ow)

###### SECURITY SELF-EFFICACY + protective behaviors data handling
variable_security_pbd_ow <- c("protective_behaviors_data", "security_efficacy")
```

```
correlation_matrix_security_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_security_pbd_ow])
print(correlation_matrix_security_pbd_ow)
describe(correlation_matrix_security_pbd_ow)
correlation_test_security_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$security_efficacy)
print(correlation_test_security_pbd_ow)

###### SOCIAL NORM + protective behaviors physical
variable_norm_pb_ow <- c("protective_behaviors_physical", "social_norm_2")
correlation_matrix_norm_pb_ow <- cor(smart_speaker_subset_owning[,
variable_norm_pb_ow])
print(correlation_matrix_norm_pb_ow)
describe(correlation_matrix_norm_pb_ow)
correlation_test_norm_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$social_norm_2)
print(correlation_test_norm_pb_ow)

###### SOCIAL NORM + protective behaviors data handling
variable_norm_pbd_ow <- c("protective_behaviors_data", "social_norm_2")
correlation_matrix_norm_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_norm_pbd_ow])
print(correlation_matrix_norm_pbd_ow)
describe(correlation_matrix_norm_pbd_ow)
correlation_test_norm_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$social_norm_2)
print(correlation_test_norm_pbd_ow)

###### EFFORT + protective behaviors physical
variable_effort_pb_ow <- c("protective_behaviors_physical", "perceived_effort")
correlation_matrix_effort_pb_ow <- cor(smart_speaker_subset_owning[,
variable_effort_pb_ow])
print(correlation_matrix_effort_pb_ow)
describe(correlation_matrix_effort_pb_ow)
correlation_test_effort_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$perceived_effort)
print(correlation_test_effort_pb_ow)

###### EFFORT + protective behaviors data handling
variable_effort_pbd_ow <- c("protective_behaviors_data", "perceived_effort")
```

```
correlation_matrix_effort_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_effort_pbd_ow])
print(correlation_matrix_effort_pbd_ow)
describe(correlation_matrix_effort_pbd_ow)
correlation_test_effort_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$perceived_effort)
print(correlation_test_effort_pbd_ow)

###### POSSESSION PERIOD + privacy risk
variable_possession_ow <- c("privacy_risk_perception", "possession.period.")
correlation_matrix_possession_ow <- cor(smart_speaker_subset_owning[,
variable_possession_ow])
print(correlation_matrix_possession_ow)
describe(correlation_matrix_possession_ow)
correlation_test_possession_ow <-
cor.test(smart_speaker_subset_owning$privacy_risk_perception,
smart_speaker_subset_owning$possession.period.)
print(correlation_test_possession_ow)

###### POSSESSION PERIOD + protective behaviors physical
variable_possession_pb_ow <- c("protective_behaviors_physical", "possession.period.")
correlation_matrix_possession_pb_ow <- cor(smart_speaker_subset_owning[,
variable_possession_pb_ow])
print(correlation_matrix_possession_pb_ow)
describe(correlation_matrix_possession_pb_ow)
correlation_test_possession_pb_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_physical,
smart_speaker_subset_owning$possession.period.)
print(correlation_test_possession_pb_ow)

###### POSSESSION PERIOD + protective behaviors data handling
variable_possession_pbd_ow <- c("protective_behaviors_data", "possession.period.")
correlation_matrix_possession_pbd_ow <- cor(smart_speaker_subset_owning[,
variable_possession_pbd_ow])
print(correlation_matrix_possession_pbd_ow)
describe(correlation_matrix_possession_pbd_ow)
correlation_test_possession_pbd_ow <-
cor.test(smart_speaker_subset_owning$protective_behaviors_data,
smart_speaker_subset_owning$possession.period.)
print(correlation_test_possession_pbd_ow)

#####REGRESSION ANALYSIS#####
################################
## combined regression model Privacy Risk Perception
```

```
model_beta <- lm(formula = privacy_risk_perception ~ perceived_enjoyableness +
                 perceived_usefulness + perceived_trust_companies +
                 nothing_to_hide + resignation_2 + powerlessness_2 + self_efficacy +
security_efficacy, data = combined_dataset)
summary(model_beta)

# Obtain the coefficients
coef_values_p <- coef(model_beta)
std_dev_p <- apply(model_beta$model, 2, sd)
std_coef_p <- coef_values_p / std_dev_p
std_coef_p

# combined regression model Protective Behaviors physical
model_pb_beta <- lm(formula = protective_behaviors_physical ~ perceived_enjoyableness +
                    perceived_usefulness + perceived_effort + perceived_trust_companies +
                    nothing_to_hide + resignation_2 + powerlessness_2 + social_norm_2 +
self_efficacy + security_efficacy, data = combined_dataset)

# Obtain the coefficients
coef_values_pb <- coef(model_pb_beta)
std_dev_pb <- apply(model_pb_beta$model, 2, sd)
std_coef_pb <- coef_values_pb / std_dev_pb
std_coef_pb

# combined regression model Protective Behaviors data handling
model_pbd_beta <- lm(formula = protective_behaviors_data ~ perceived_enjoyableness +
                     perceived_usefulness + perceived_effort + perceived_trust_companies +
                     nothing_to_hide + resignation_2 + powerlessness_2 + social_norm_2 +
self_efficacy + security_efficacy, data = combined_dataset)

# Obtain the coefficients
coef_values_pbd <- coef(model_pbd_beta)
std_dev_pbd <- apply(model_pbd_beta$model, 2, sd)
std_coef_pbd <- coef_values_pbd / std_dev_pbd
std_coef_pbd

###########################################################################
######## REGRESSION ANALYSIS FOR SIGNIFICANT FACTORS##############
## combined regression model Privacy Risk Perception
model_beta_2 <- lm(formula = privacy_risk_perception ~ perceived_enjoyableness +
                 perceived_usefulness +
                 perceived_trust_companies +
                 nothing_to_hide + resignation_2, data = combined_dataset)
summary(model_beta_2)
```

```
# Obtain the coefficients
coef_values_p_2 <- coef(model_beta_2)
std_dev_p_2 <- apply(model_beta_2$model, 2, sd)
std_coef_p_2 <- coef_values_p_2 / std_dev_p_2
std_coef_p_2

# combined regression model Protective Behaviors physical
model_pb_beta_2 <- lm(formula = protective_behaviors_physical ~ perceived_enjoyableness
+
                perceived_usefulness +
                nothing_to_hide +
                resignation_2 +
                security_efficacy +
                social_norm_2, data = combined_dataset)

# Obtain the coefficients
coef_values_pb_2 <- coef(model_pb_beta_2)
std_dev_pb_2 <- apply(model_pb_beta_2$model, 2, sd)
std_coef_pb_2 <- coef_values_pb_2 / std_dev_pb_2
std_coef_pb_2


# combined regression model Protective Behaviors data handling
model_pbd_beta_2 <- lm(formula = protective_behaviors_data ~ perceived_enjoyableness +
                perceived_usefulness +
                nothing_to_hide +
                resignation_2 +
                social_norm_2 +
                security_efficacy, data = combined_dataset)

# Obtain the coefficients
coef_values_pbd_2 <- coef(model_pbd_beta_2)
std_dev_pbd_2 <- apply(model_pbd_beta_2$model, 2, sd)
std_coef_pbd_2 <- coef_values_pbd_2 / std_dev_pbd_2
std_coef_pbd_2
```