Exploring Smart Speaker Privacy Misconceptions and Knowledge Gaps

Luuk Scheuneman (2609991)

Department of Psychology, University of Twente

Supervisors: Michelle Walterscheid & Nicole Huijts

Word count: 9269

Date: 24-01-25

Abstract

The rapid rise of smart speakers has raised significant privacy concerns, yet many users and non-users remain unaware of or hold mistaken beliefs about smart speaker privacy. This study examines the relationship between privacy misconceptions, perceived knowledge, and privacy-protective behaviours across four different user types, including primary users, secondary users, visitors, and non-users. The final sample consisted out of 155 participants. Results revealed that misconceptions about smart speaker privacy are equally prevalent across all user types, indicating that experience with the devices does not necessarily improve the understanding of privacy risks. Primary users perceived themselves as more knowledgeable than non-users, and a higher misconception score was weakly associated with a higher perceived knowledge. Contrary to expectations, non-users and visitors reported higher engagement with intended privacy-protective behaviours compared to the actual behaviours of primary users. These findings highlight the need for clearer privacy information from manufacturers and suggest that perceived knowledge does not necessarily lead to an accurate understanding of the privacy of smart speakers or protective actions to improve privacy. Future research should explore targeted interventions to address misconceptions and promote effective privacy behaviours.

Introduction

Since the rapid rise of smart home devices, such as smart speakers, thermostats, and cameras, concerns about individuals' privacy have emerged as a crucial issue. These smart home devices are called Internet of Things (IoT) devices, which refers to interconnected devices that communicate without human intervention. Understanding the privacy risks associated with smart home devices, especially smart speakers, is crucial because these devices continuously collect data within households, and this comes with privacy risks (Lau et al., 2018).

This study specifically focuses on smart speakers, such as Amazon Echo, Google Home, and Apple Home Pod, which have become widely adopted in the last decade. Despite their growing popularity, users and non-users alike often hold misconceptions about the privacy implications of these devices, such as how they record, store, and share data (Zheng et al., 2018; Lau et al., 2018). These misconceptions may influence privacy-protective behaviours and perceived knowledge of privacy risks. By exploring these misconceptions, this research aims to uncover critical gaps in understanding and evaluate the relationship between user type, perceived knowledge, and privacy-protective behaviours.

The number of interconnected devices has been growing drastically in the last few years and is expected to more than double from 15.9 billion in 2023 to 39.6 billion in 2033 (Statista, 2024). In the Netherlands alone, nearly three-quarters (72%) of the population aged 12 years or older indicated that they have an IoT device or system at home (CBS, 2022), and it could be that some individuals might not even know they have a smart TV or smart thermostat. This number is expected to rise even more in the upcoming years.

All these interconnected devices are connected by the IoT. By equipping these devices, such as doorbells or thermostats, with a computer they can communicate with each other without any need for human interaction. Although most IoT devices are connected to the

internet, they do not necessarily have to be. All the IoT devices are interconnected (Jarvis, 2023).

Smart home devices are not only used to activate and deactivate lights or heating; they also continuously monitor the activities of households and are used to automate certain aspects of someone's everyday life (Ricquebourg et al., 2006). With the rapid adoption of IoT devices, such as smart speakers and thermostats, users begin to use these technologies for efficiency and convenience in their daily lives. But, as the use of these devices grows, so do concerns about how personal data is handled. Users often expect that the manufacturers will keep their personal information away from other entities (Kim et al., 2018). These privacy expectations are not always correct. In 2015 for example, the personal data of five million consumers, including 200,000 children, was compromised through internet-connected toys. More than 4.8 million accounts were hacked. Exposing names, home addresses, emails and passwords of parents and names, genders and birthdays of children (Leetaru, 2015). Next to this, in 2017, passwords, email addresses and voice recordings of more than half a million people who bought smart fluffy animals were leaked (Kim et al., 2018). The collected sensitive personal data, including daily routines, personal locations, and one's preferences, is thus not always kept securely by companies.

The consequences of such data breaches can be severe. Stolen personal data can be used for identity fraud, which allows hackers to open bank accounts, apply for loans, or make purchases under the victim's name (Masterson, 2023). In addition, voice recordings could be exploited for blackmail or manipulated into deepfakes, where a person's voice is used in fabricated situations (Cruz, 2024). For example, criminals might use a brief clip of someone's voice to deceive their loved ones, pretending to be in a distressing situation and asking for money. Studies show that one in ten people have received such fake messages, with 77% of them falling victim to scams (Cruz, 2024). Especially for children, these privacy risks are

concerning because they lack the awareness and understanding of these risks (Console & Associates P.C., 2024), which makes it of specific concern for parents. Exposed data might also allow criminals to track personal habits or specific locations of individuals, leading to concerns about user information leaks and privacy violations for the consumers of these devices (Kim et al., 2018).

Privacy, regarding digital technologies, is often defined as informational privacy, meaning the control over access to personal information (Schomakers et al., 2020). In this research, privacy refers to how users' personal data is handled, stored, and potentially shared by the companies behind these devices. "Home" is defined as "a private, often familial realm clearly differentiated from public space and removed from public scrutiny and surveillance" by Mallet (2004, p. 71). Smart home devices with microphones do not align with this definition of home since they can make recordings, listen to conversations, and share personal data with their manufacturer outside of the home. This became clear in 2015, when it was discovered by journalists that conversations near a Samsung TV were recorded and shared with third parties (Harris, 2017).

The Samsung smart TV is not the only device that is constantly listening to its surroundings. Smart speakers are privacy-intrusive smart home devices because they listen to all the conversations held around them (Lau et al., 2018). They do this by using their sensors, which are microphones that always listen for a so-called "wake-word". When recognising this wake-word the smart speakers know it can expect an assignment, and it starts recording. As one can imagine, this function of constantly listening to what is said around the device raises great concerns about the privacy of individuals with smart speakers. People are wondering what exactly these speakers record, store, and share (Lutz & Newlands, 2021). Because of this large concern for the privacy of smart speaker owners, the focus of this research lies on the privacy misconceptions of users and non-users.

Knowledge Gaps

It is important to understand that users of smart speakers often remain unaware of the full extent of the privacy risks they face when using smart speakers (Al-Ameen et al., 2021). The lack of knowledge people have about their privacy regarding smart speakers is referred to in this research as knowledge gaps. It can be defined as "the discrepancy or difference between what an individual knows and what they need to know in order to make informed decisions or perform tasks" (Stringer, 2023).

For example, Malkin et al. (2019) found that almost half of their participants (41.4%), who were all owners of smart speakers, did not know that all their conversations, after the speaker notices the wake-word, are permanently stored by the companies that made the devices. The risk of this is that smart speakers can sometimes mistakenly detect the wake-word, causing unintended activation. For example, one participant in the study of Malkin et al. (2019) indicated that when a friend named Alexa comes over, the Amazon smart speaker falsely detects the wake-word. Next to this, more than half of their respondents (56%) did not know that they could review all the recordings from their smart speakers, and 45% did not know they could delete them.

Misconceptions

Several studies have pointed out misconceptions about the privacy risks of smart speakers. A misconception can be defined as "a belief or an idea that is not based on correct information, or that is not understood by people" (Oxford University Press, n.d.). Unlike knowledge gaps, which represent a lack of awareness or understanding, misconceptions involve incorrect beliefs about a topic. For example, Zheng et al. (2018) stated that owners tend to trust the big technological companies where they buy their smart speakers from. They believe that these companies will handle their data while respecting their privacy because of the simple reason that these companies are trusted by many people around the world. As can

be read in the research of Zheng et al. (2018), owners of smart speakers tend to believe that manufacturers respect their privacy, while these companies do save all their recordings, and their staff occasionally listens to them to improve the performance of their smart speakers (BBC News, 2019).

Lau et al. (2018) found that users and non-users of smart speakers reasoned that companies would not save their recordings because that would be too much data to store. Besides this, Lau et al. (2018) mentioned that some of their participants believed that their recordings could not be hacked because the manufacturers where such large companies that the devices could not be hacked.

Protective Behaviour

To protect one's privacy, individuals could perform different protective behaviours. Lutz and Newlands (2021) found that smart speaker owners often do not engage in privacy protection behaviour. Out of their respondents ($N = 367$), more than half (51%) of them indicated that they never turn off their smart speaker. Besides this, 72% of them indicated that they do not switch off their smart speaker when having a serious or private conversation. An even smaller number of participants engaged in reviewing or deleting their stored conversations. The least common behaviour observed was social protective behaviour, where individuals alter their language or speech around smart speakers to protect their privacy.

Perceived Knowledge

Knowledge gaps and misconceptions could play an important role in the performance of privacy-protective behaviour, as described by De Kimpe et al. (2021). Perceived knowledge can be defined as what one thinks one knows, and perceived knowledge and actual knowledge do not necessarily have to be similar. Often, people tend to overestimate their actual knowledge about a certain topic (De Kimpe et al., 2021). Higher perceived knowledge can lead individuals to feel more capable and less vulnerable, which in turn can motivate them

to engage in protective behaviours. For example, someone who believes they are knowledgeable about smart speaker privacy might feel more confident adjusting privacy settings or reviewing stored data. Conversely, lower perceived knowledge might lead to feelings of helplessness or a belief that protective behaviours are too complex or ineffective, reducing motivation to act.

User Types

These misconceptions, along with the lack of privacy-protective behaviours related to smart speakers, underscore a significant gap between users' perceptions of privacy risks and the actual risks they face. According to Zeng et al. (2017), users tend to have fewer misconceptions than non-users, but this does not mean that they have a complete understanding of what the privacy risks of smart speakers are. Additionally, it's important to recognise the differences in privacy behaviour across user types, including primary users, secondary users, visitors, and non-users. While primary users may feel more familiar and confident with the device, their privacy perceptions may not necessarily be more accurate. Secondary users, visitors, and non-users might hold different misconceptions, and their privacy-protective behaviours may be affected by their level of exposure to the device.

Current Study

This research aims to examine the misconceptions that users and non-users of smart speakers have about data collection, storage, and sharing that can potentially pose privacy risks and how these misconceptions are related to their perceived knowledge and performance of protective behaviours. Specifically, the study investigates how participants' misconception score aligns with their perceived knowledge and whether this score relates to the performance of privacy-protective behaviours.

This will be examined using a survey in which the user type of the participants will be determined, their perceived knowledge and misconceptions regarding data collection, storage

and sharing in relation to smart speakers is questioned, and their privacy protective behaviours is measured.

The research question that will be answered during this research is: "How do privacy misconceptions about smart speakers relate to perceived knowledge and privacy-protective behaviours across different user types?" Based on the reviewed literature, five hypotheses are formulated:

H1: “Non-users and visitors hold more misconceptions than primary and secondary users.” This hypothesis is grounded in research suggesting that direct interaction with smart speakers can improve familiarity and understanding of the privacy risks (Lau et al., 2018). Non-users and visitors, lacking such interaction, could be more likely to hold inaccurate beliefs about how these devices function.

H2: “Primary users perceive themselves as more knowledgeable about the privacy of smart speakers than secondary users, visitors, and non-users do.” As described, research indicates that perceived knowledge often increases with familiarity and repeated use, even if actual knowledge does not improve (De Kimpe et al., 2021). This suggests primary users, having the most exposure to smart speakers, may feel more confident in their understanding compared to less-engaged groups.

H3: “Individuals who hold less misconceptions about the privacy of smart speakers perceive themselves as more knowledgeable about smart speaker privacy.” As perceived knowledge is often influenced by the absence of misconceptions. People who believe their understanding is accurate are more likely to perceive themselves as knowledgeable, highlighting the connection between fewer misconceptions and higher perceived knowledge.

H4: “The number of misconceptions mediates the relation between user type and perceived knowledge.” User type is likely to influence perceived knowledge through the level of misconceptions individuals hold. De Kimpe et al. (2021) demonstrated that misconceptions

can shape perceptions of knowledge, either inflating confidence or diminishing it, depending on their prevalence.

H5: “Secondary users, visitors, and non-users engage less in privacy-protective behaviours related to smart speakers than primary users.” De Kimpe et al. (2021) suggest that perceived knowledge positively influences self-efficacy, which in turn drives protective behaviours. Since primary users are more likely to feel confident in their ability to manage privacy risks, they are expected to engage in more privacy-protective actions compared to other user types.

Methods

Participants

A total of 212 participants were recruited through a combination of convenience sampling, volunteer sampling, and snowball sampling methods. All the participants were required to read the informed consent (see Appendix A) and had the option to consent to it. Additionally, ethical approval was obtained from the Humanities & Social Sciences Ethical Committee of the University of Twente.

From the total number of participants, 57 participants were excluded for not meeting the inclusion criteria. Specifically, one individual was excluded for being seventeen or younger, 49 for not finishing the questionnaire, and seven for failing the attention check.

As a result of these exclusion criteria, the final sample consisted of 155 participants. The demographic characteristics of the final sample indicated that participants ranged in age from 18 to 96, with a mean age of 28.7 years (*SD* = 13.8). In terms of gender distribution, 46% participants identified as female, 54% as male, and 1% as non-binary or third gender. The educational backgrounds of the participants varied, with 46% holding a bachelor's degree, 27% completed secondary education, 15% holding a master's degree, and 12% pursuing or holding other educational qualifications. Furthermore, most of the participants described themselves as students (57%) or as employed (34%). The nationality of the participants also varied. 85% were Dutch, 11% were German, and 4% were from another nationality.

Material

The participants' data was gathered through the online survey tool Qualtrics.

Measurements

User Type. Participants were asked about their interactions with smart speakers to differentiate between different user types and non-users. This section included four questions designed to classify participants based on their interaction with smart speakers, such as *"I*

installed the smart speaker myself." or *"I can personally control the usage and privacy settings of the smart speaker through my phone.".* These questions were only presented to participants who were owners of a smart speaker. The questions, detailed in Appendix B, were based on the research of Lau et al. (2018), which also categorised between user types. The specific wording of the questions was formulated by the researcher.

Participants who answered at least three questions with "Agree" were classified as primary users, while those with fewer than three "Agree" responses were classified as secondary users. Participants without a smart speaker who visited smart speaker owners were classified as visitors, and those who had no interaction with smart speakers were considered non-users.

Perceived Knowledge. This category includes five questions like: "*How much do you know about the types of data smart speakers collect?"* and *"How much do you know about where and how smart speakers store collected data?".* These questions were adapted from the research by Lau et al. (2018), which also investigated participants' knowledge of smart speaker privacy. Participants could respond on a five-point Likert scale ranging from "Nothing" to "Very much". All the five questions can be found in Appendix C, together with the scores per question.

To examine the reliability of the perceived knowledge scale, internal consistency was evaluated by using Cronbach's alpha. The scale demonstrated good internal consistency, with a Cronbach's alpha of .88, indicating that the items reliably measure participants' perceived knowledge of the privacy of smart speakers. A factor analysis confirmed that all five items loaded on a single factor, explaining 61% of the total variance (factor loadings ranged from .71 to .83). This suggests that the perceived knowledge scale measures a single construct. The score for perceived knowledge ranged from 1 to 5. Participants reported a

mean score of 1.7 (*SD* = 0.7), indicating low overall perceived knowledge about smart speaker privacy.

Misconceptions. In this part of the questionnaire, participants were asked about their perceptions of their privacy regarding smart speakers. Participants responded to 15 statements in the categories of recording, storing, and sharing. For example, *"Smart speakers only collect data when they have an active internet connection*" and "*Smart speakers record every conversation held around them".* All the statements had the answer options "Strongly disagree", "Disagree", "Agree", "Strongly agree", and "I do not know". The last answer option was added to discourage participants from guessing and allow them to clearly indicate a lack of knowledge when applicable. All the misconception questions were devised from different earlier studies (Lau et al., 2018; Lutz & Newlands, 2021; Malkin et al., 2019) and were checked by three experts on security, risk perception, and privacy. This was done to make sure that the items measure privacy knowledge well and correctly. The items can be found in the questionnaire in Appendix D.

For an optimal analysis, the five answer options were simplified. "Strongly Agree" and "Somewhat Agree" were coded as "Agree", "Strongly disagree" and "Somewhat disagree" were coded as "Disagree", "I don't know" was changed to "Unknown". This led to three different answer options in the analysis: "Agree", "Disagree", and "Unknown". Based on this, the scores of the participants were calculated.

On a scale from 1 to 15, the mean incorrectness score was 6.48 (*SD* = 3.2). The number of "Unknown" responses had a mean of 3.0 (*SD* = 3.8). To calculate the misconception score, "Unknown" answers were excluded from the score. This resulted in a mean of 3.5 (*SD* = 2.0). In Table 1, the percentages of answers per misconception item and the total scores can be viewed. As can be seen the most common misconceptions were: *"Smart speakers record every conversation held around them",* which is not the case, and *"Smart speakers only*

collect data when they have an active internet connection", which participants thought was wrong.

Table 1

Misconception Scores from Mostly Incorrect (top) to Correct (bottom)

Item	*Correct answers*	*Incorrect answers*	*"I don't know" answers*
	%	*%*	*%*
Q17_2: Smart speakers record every conversation held around them.	29	50	21
Q17_1: Smart speakers only collect data when they have an active internet connection.	39	44	17
Q19_3: Government agencies can access my smart speaker data without my knowledge.	34	41	25
Q19_4: Specific employees of manufacturers listen to voice recordings of smart speakers.	30	41	29
Q18_4: Smart speakers can only access information like passwords or bank account details if you provide this information.	56	25	19
Q17_3: Smart speakers can only record spoken commands, not background noises or sounds.	62	21	17
Q19_5: As a smart speaker user, you have complete control over how your data is shared.	68	21	12
Q18_1: Manufacturers indefinitely store personal data collected by smart speakers, if you did not indicate you do not want this.	56	19	26
Q19_2: Smart speakers collect data from other connected smart home devices inside a home and share this with their manufacturer.	54	18	28
Q17_5: Smart speakers record conversations after the wake word (e.g. "Hey Google/Alexa") is spoken.	74	15	11
Q18_3: Spoken commands recorded by smart speakers are deleted immediately after the task is completed.	64	14	21
Q19_1: Manufacturers (first-party developers) share specific smart speaker data with third-party developers.	64	13	23
Q18_2: Smart speakers can recognize different human individuals and store separate data profiles.	70	11	19
Q18_5: Smart speakers can store or retain any personal data after the task is completed.	70	11	19
Q17_4: Smart speakers can accidentally think they hear the wake word and then start recording what has been said.	82	6	12
Total	57	23	20

Attention Check. In the misconceptions part of the questionnaire, an attention check was included to ensure data quality: "*To ensure you are paying attention, please select "Somewhat agree" as your answer for this statement."* Participants had to indicate that they had read the item correctly by choosing the *"Somewhat agree"* answer. Participants who failed this attention check, by answering wrong, were excluded from the analysis.

Protective Behaviours. In this part, the likelihood of participants engaging in privacy-protective behaviours related to smart speakers was measured. For participants who did not own a smart speaker, it was instructed to imagine owning one and indicate how likely they would be to engage in these behaviours. The items in this section were based on the exploratory factor analysis of the privacy protective behaviour items from research of Lutz and Newlands (2021). Items with a factor loading lower than .50 were excluded and the items were rephrased into I statements. While Lutz and Newland (2021) showed that protective behaviour consists of multiple dimensions, this study focuses on the average general protection intention."

Participants were presented with 13 statements, such as *"I turn off the smart speaker when I am not using it"* and *"I review the privacy settings of my smart speaker in the provider's (e.g., Alexa or Google) account."* The responses were rated on a five-point Likert scale ranging from "Extremely unlikely" to "Extremely likely." The full set of items is included in Appendix E, together with the scores on each statement.

To ensure the reliability of the protective behaviour scale, internal consistency was evaluated by using Cronbach's alpha. The scale demonstrated good internal consistency, with a Cronbach's alpha of .87, indicating that the items reliably measure participants' protective behaviours towards smart speakers. The scores of the participants had a mean of 2.2 (*SD* = 0.7).

Procedure

The Test Subject Pool of the University of Twente was used to gather participants. Moreover, the online link to the study was shared over social media. Students at the University of Twente could gain credit points after completing the study. For some students this is part of their study programme. After joining the study, the link for the online survey was shared. Participants were invited to engage in the online survey from a location of their choice, utilising their personal devices, such as laptops, smartphones, or any other digital tools compatible with Qualtrics. The survey took around 10 minutes in total. First, a description of the study was given, and informed consent was obtained. Participants were informed about the potential negative consequences of the study, anonymity, and their right to withdraw anytime. If the information was read and consent was given, the different categories of the questionnaire were answered, starting with the demographics, then the user type, perceived knowledge, misconceptions, and protective behaviour questions. All the data was collected anonymously, with no personally identifiable information recorded. After completion of the study, the data was transferred to the repository of the University of Twente, where it was securely stored.

Data Analysis

All analyses were conducted using RStudio (Version 2024.09.1+394). The dataset was first cleaned to ensure data quality by removing incomplete responses, participants who failed the attention check, or those who provided inconsistent answers (e.g., selecting the same response for all items). After data cleaning, key variables were computed to facilitate the hypothesis testing. Descriptive statistics, including means, standard deviations, and frequencies, were calculated for all key variables to provide an overview of the dataset. The internal consistency of the scales used in the questionnaire was assessed using Cronbach's alpha.

A self-reported knowledge variable was calculated as the sum of participants' responses to perceived knowledge-related questions. Additionally, a total misconception score was calculated by summing participants' responses to the items measuring misconceptions. The incorrectness score was calculated by summing participants' responses to the items measuring misconceptions. Incorrect answers were assigned a value of 1, while correct answers were assigned a value of 0. This led to a mean incorrectness score of 6.5 (SD = 3.2). After this, both correct and unknown answers were coded as 0 to calculate a misconception score (M = 3.5, SD = 2.0). At the end, a privacy-protective behaviour score was derived from the average of all responses to the protective behaviour scale (M = 2.2, SD = .74).

To test the first and second hypotheses, one-way analyses of variance (ANOVA) were performed to compare misconception and perceived knowledge scores across the four user groups. Post hoc analyses using Tukey's HSD were conducted to identify significant differences between groups when the ANOVA was significant. For the third hypothesis, a Spearman correlation was performed to assess the relationship between self-reported knowledge levels and misconception scores. This nonparametric test was chosen due to the rational nature of the knowledge level variable, which was measured using a five-point Likert scale. To examine the fourth hypothesis, the results of the first two hypotheses are used. Next to this, a causal mediation analysis was performed. To examine the fifth hypothesis, a Spearman correlation was conducted to evaluate the relationship between misconception scores and privacy-protective behaviour scores, again accounting for the ordinal nature of the data.

To gain deeper insight into the misconception data, an exploratory factor analysis (EFA) was conducted. This analysis aimed to identify underlying themes within the misconception items, such as those related to recording, storing, and sharing data.

Results

To test the first hypothesis, “non-users and visitors hold more misconceptions than primary and secondary users”, a Kruskal-Wallis test was conducted. Both total scores were used, including and excluding knowledge gaps. The score including knowledge gaps is referred to as the incorrectness score, and the score excluding knowledge gaps is the misconception score.

Incorrectness Score per User Type

As can be seen in Table 2, there was a minimal difference in the incorrectness score between the different user groups.

Table 2

Incorrectness Score per User Type

User type	Incorrectness Score		
	M	*SD*	*n*
Primary user	7.0	3.4	47
Secondary user	7.0	3.0	22
Visitor	6.1	3.3	61
Non-user	6.2	3.0	24

The Shapiro-Wilk test was conducted to assess the normality of the total incorrectness score across the four different user groups. This test was conducted since determining the distribution of the incorrectness score per user type was important for choosing further statistical methods. The results indicated significant deviations from normality for primary

users ($W = .94$, $p = .018$), secondary users ($W = .83$, $p = .002$), and visitors ($W = .90$, $p < .001$). Non-users had a higher Shapiro-Wilk p-value ($W = .95$, $p = .182$), suggesting a better fit to normality. This was insufficient to assume a normal distribution across all groups. Levene's test for homogeneity of variances confirmed that the assumption of equal variances was met across the different user groups ($F(3, 151) = 0.26$, $p = .851$).

Because the normality was violated in three groups, a Kruskal-Wallis test was conducted to compare the total incorrect answers among the different user types. The Kruskal-Wallis test revealed no significant differences between the groups ($\chi^2 = 3.49$, $df = 3$, $p = .322$). This indicated that the incorrectness score about privacy risks did not significantly differ among primary users, secondary users, visitors, and non-users.

Misconception Score per User Type

Table 3 describes the misconception scores. The differences were still small. The Shapiro-Wilk test was repeated to assess the normality of the total misconception scores excluding "Unknown" answers across the four different user groups. The results indicated that there were significant deviations from normality for primary users ($W = .95$, $p = .031$) and visitors ($W = .94$, $p = .003$). Secondary users ($W = .94$, $p = .178$) and non-users had a higher Shapiro-Wilk p-value ($W = .94$, $p = .106$). Yet, the assumption of normality was still violated across most participants ($n = 108$). Levene's test for homogeneity of variances again confirmed that the assumption of equal variances was met across the different user groups ($F(3, 151) = 1.83$, $p = .135$). Because the normality was violated in two groups, a Kruskal-Wallis test was conducted to compare the total incorrect answers among the different user types. The Kruskal-Wallis test revealed no significant differences between the groups ($\chi^2 = 1.20$, $df = 3$, $p = .752$). This indicated that the level of misconceptions about privacy risks did not significantly differ among primary users, secondary users, visitors, and non-users.

Table 3

Misconception Score per User Type

User type	Misconception score		
	M	*SD*	*n*
Primary user	3.5	2.4	47
Secondary user	3.6	1.7	22
Visitor	3.6	2.0	61
Non-user	3.0	1.7	24

Comparing Misconception Scores for Owners and Non-owners

Lastly, the misconception scores were compared between two combined groups: owners (primary and secondary users) and non-owners (non-users and visitors). The Shapiro-Wilk test indicated that both groups had significant deviations from normality (non-owners: $W = .94$, $p < .001$; owners: $W = .96$, $p = .039$). Levene's test for homogeneity of variances showed that the assumption of equal variances was met ($F(1, 153) = 2.40$, $p = .12$). Since normality was violated, a Kruskal-Wallis test was conducted to compare the misconception scores between the two groups. The Kruskal-Wallis test revealed no significant difference between the groups ($\chi^2 < .01$, $df = 3$, $p = .986$). This suggests that the level of misconceptions about privacy risks did not significantly differ between owners and non-owners and thus the first hypothesis can be rejected.

Perceived Knowledge Score per User Type

To evaluate the second hypothesis, "Primary users perceive themselves as more knowledgeable about the privacy of smart speakers than secondary users, visitors, and non-users do", another series of statistical analyses were carried out. The differences per user type can be seen in Table 4.

The Shapiro-Wilk test was conducted to determine the normality of the perceived knowledge scores. The results indicated that for every type of user there were significant deviations ($p < .05$) from normality (Primary users: $W = .91$, $p < .001$; Secondary users: $W = .87$, $p = .002$; Non-users: $W = .74$, $p < .001$; Visitors: $W = .90$, $p < .001$). Levene's Test for Homogeneity of variances confirmed that the assumption of equal variances was met across the different user groups ($F(3, 151) = 0.80$, $p = .493$).

Table 4

Perceived Knowledge Scores per User Type

User type	Perceived Knowledge		
	M	*SD*	*n*
Primary user	1.8	0.7	47
Secondary user	1.5	0.5	22
Visitor	1.7	0.7	61
Non-user	1.4	0.6	24

Because the normality was violated in all user groups, a Kruskal-Wallis rank sum test was conducted. This test revealed a significant difference in perceived knowledge scores

among the four user types ($\chi^2 = 7.87$, $df = 3$, $p = .049$). This means that there was a significant difference in perceived knowledge scores between at least two different groups of users. To determine which user types significantly differed, pairwise Wilcoxon rank-sum tests were conducted with a Holm correction for multiple comparisons. In Table 5, the adjusted *p*-values are provided. There was a significant difference between primary users and non-users ($p = .048$), which indicated that primary users ($M = 1.8$) perceived themselves as more knowledgeable about smart speakers compared to non-users ($M = 1.4$).

Table 5

Pairwise comparisons for perceived knowledge scores

Comparison	Adjusted *p*-value	Significance
Primary users vs. non-users	.04	Significant
Secondary users vs. non-users	.88	Not significant
Visitors vs. non-users	.24	Not significant
Secondary users vs. primary users	.20	Not significant
Visitors vs. primary users	.51	Not significant
Visitors vs. secondary users	.88	Not significant

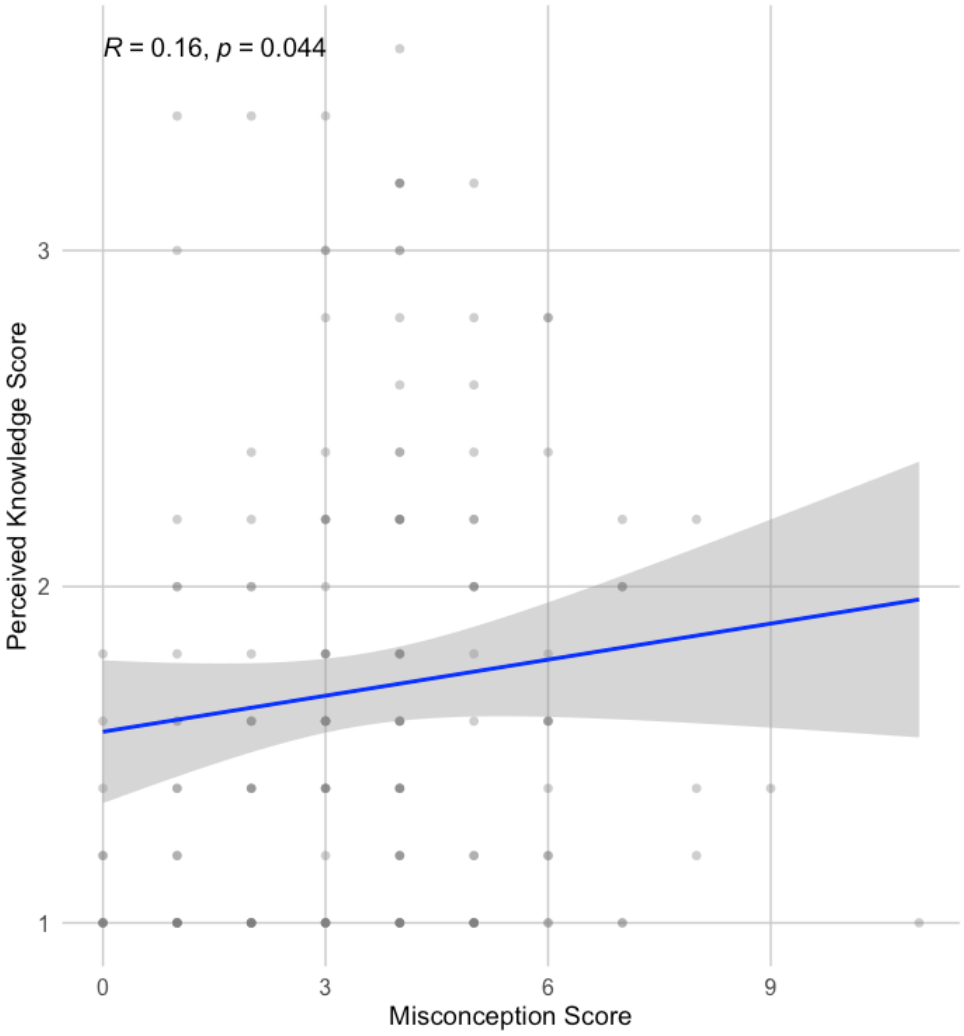
Relationship Between Misconception and Perceived Knowledge Score

To test the third hypothesis, "Individuals who hold less misconceptions about the privacy of smart speakers perceive themselves as more knowledgeable about smart speaker privacy", the perceived knowledge and misconception scores were further analysed using Spearman's rank correlation, since normality was violated. The results showed a weak but

statistically significant positive correlation, $r(153) = .16$, $p = .044$. This suggests that participants who perceived themselves as more knowledgeable tended to hold slightly more misconceptions about the privacy risks of smart speakers. This means that the hypothesis can be rejected. In Figure 1, this relationship is visualised.

Figure 1

Relationship Between Misconception and Perceived Knowledge Score



Note. Each point represents an individual score. If a point is darker, this means that multiple participants had this score. The blue line represents the linear regression fit, with the shaded areas indicating a 95% confidence interval.

Mediation Analysis of Misconception Score on User Type and Perceived Knowledge

To evaluate the fourth hypothesis, "The number of misconceptions mediates the relation between user type and perceived knowledge," causal mediation analyses were conducted for four user types: primary users, secondary users, visitors, and non-users.

For primary users, the mediation effect (ACME = 0.00, p = 0.962) was not statistically significant, suggesting no evidence of mediation by misconceptions. The direct effect (ADE = 0.2084, p = 0.080) was also not significant. For secondary users, the mediation effect (ACME = 0.0026, p = 0.848) was not significant. The direct effect (ADE = -0.2486, p = 0.036) was significant, suggesting a negative direct impact of secondary user type on perceived knowledge. The total effect for secondary users was significant (Total Effect = -0.2460, p = 0.040), indicating an overall negative relationship between secondary user type and perceived knowledge. However, misconceptions did not mediate this relationship (Prop. Mediated = -0.0106, p = 0.870). For visitors, no significant effects were found, either for the mediation (ACME = 0.0080, p = 0.61), the direct effect (ADE = 0.0604, p = 0.59), or the total effect (Total Effect = 0.0685, p = 0.56). Misconceptions did not significantly mediate the relationship between visitor user type and perceived knowledge (Prop. Mediated = 0.1171, p = 0.80). For non-users, there was no significant mediation effect (ACME = -0.0156, p = 0.38), and the direct effect (ADE = -0.2096, p = 0.18) was also not significant. The total effect (Total Effect = -0.2252, p = 0.15) was not significant, and misconceptions did not mediate the relationship between non-user status and perceived knowledge (Prop. Mediated = 0.0693, p = 0.45). In summary, while there was some evidence of direct effects, the mediation effect of misconceptions was generally not significant across user types.

Protective Behaviour Score per User Type

To evaluate the last hypothesis: "Secondary users, visitors, and non-users engage less in privacy-protective behaviours related to smart speakers than primary users", another series of statistical analyses was conducted. Also, it was checked if participants engaged in less protective behaviours if they held more misconceptions. First, it was calculated what the protective behaviour scores per user group were. This can be seen in Table 6.

Table 6

Protective Behaviour Score per User Type

User type	Protective Behaviours		
	M	*SD*	*n*
Primary user	1.8	0.6	47
Secondary user	1.9	0.6	22
Visitor	2.5	0.8	61
Non-user	2.4	0.7	24

As shown in Table 6, the mean protective behaviour scores varied slightly among the different user types. Non-users and visitors had higher mean protective behaviour scores compared to primary and secondary users.

The Shapiro-Wilk test was conducted to determine the normality of the protective behaviour scores. The results indicated that only for primary users there was a significant deviation from normality ($W = .94$, $p = .015$). The remaining groups did not show significant deviations (Secondary users: $W = .95$, $p = .328$; Non-users: $W = .93$, $p = .084$; Visitors: $W = .97$, $p = .223$), suggesting that their protective behaviour scores were normally distributed.

Levene's Test for Homogeneity of variances confirmed that the assumption of equal variances was met across the different user groups ($F(3, 151) = 2.81$, $p = .081$).

Given that only one group, primary users, violated the normality assumption but the homogeneity of variances was satisfied, a one-way ANOVA was conducted to compare behaviour scores among the different user types. The ANOVA results revealed a significant effect of user type on protective behaviour scores, $F(3, 151) = 11.37$, $p < 0.001$, $\eta^2 = 0.18$. This suggests that approximately 18% of the variance in protective behaviour scores could be explained by user type.

To identify which specific groups differed from each other, Tukey's Honestly Significant Difference (HSD) post-hoc test was conducted. The results are presented in Table 7. Primary ($p = .001$) and secondary users ($p = .036$) had significantly lower protective behaviour scores compared to non-users. Visitors had significantly higher protective behaviour scores compared to both primary ($p < .001$) and secondary users ($p = .007$). There was no significant difference between visitors and non-users ($p = .999$) or between primary and secondary users ($p = .927$). The results are visualised in Figure 2.

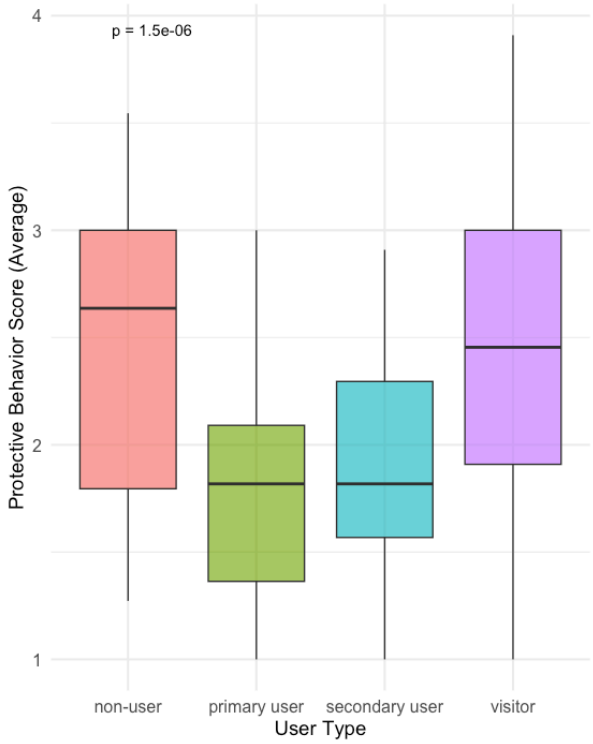
Table 7

Tukey's HSD Post Hoc Test Results for Protective Behaviour Scores

Comparison	Difference	Lower CI	Upper CI	Adjusted *p*-value
Primary users vs. non-users	-0.65	-1.09	-0.21	.001
Secondary users vs. non-users	-0.54	-1.06	-0.02	.036
Visitors vs. non-users	0.01	-0.41	0.43	.999
Secondary users vs. primary users	0.11	-0.35	0.56	.927
Visitors vs. primary users	0.66	0.32	1.00	.000
Visitors vs. secondary users	0.55	0.12	0.99	.007

Figure 2

Boxplot of Protective Behaviour Scores across User Types



Correlation Between Misconception and Behaviour Scores

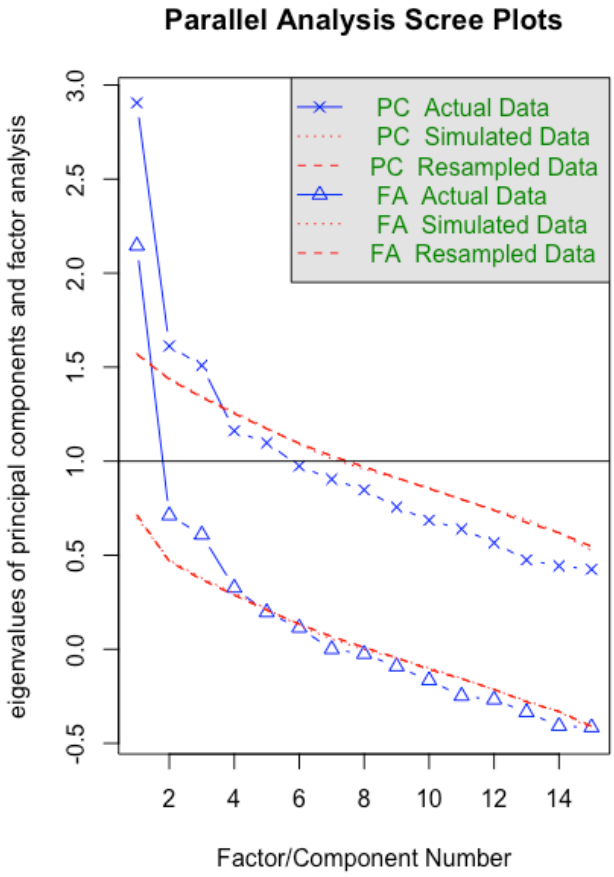
The relationship between total misconception scores and protective behaviour scores was examined using Spearman's rank correlation, as normality was violated for both variables. The results revealed no significant correlation, $r(153) = -.05$, $p = .537$, suggesting no meaningful relationship between the level of misconceptions and the engagement in privacy protective behaviour.

Exploratory Analysis

The misconception scores were further explored through an Exploratory Factor Analysis (EFA), to check if there was an underlying factor explaining misconceptions scores. Prior to conducting the EFA, a Kaiser-Meyer-Olkin (KMO) measure and Bartlett's test of sphericity were performed to assess the suitability of the data. The KMO value was 0.68 and Bartlett's test of sphericity was significant ($\chi^2(105) = 4532.95$, $p < .001$), indicating that the correlations between the items were sufficient for factor analysis. Parallel Analysis was conducted to determine the number of factors to extract for the factor analysis. The scree plot, as is shown in Figure 3, suggests that three factors could be retained.

Figure 3

Parallel Analysis Scree Plots



Note. This scree plot displays the results of the parallel analysis for factor extraction, comparing the actual data (represented by the blue line), simulated data (represented by the dotted red line), and resampled data (represented by the dashed red line). The x-axis represents the factor number, while the y-axis shows the eigenvalues of the principal factors. The scree plot reveals that the eigenvalues for the actual data drop beneath the red line from the fourth factor. This suggests that three factors are supported by the data.

In Table 8, the factor loadings were presented. Oblimin rotation was used instead of varimax because the factors were expected to be correlated. Misconceptions about smart speakers, such as recording behaviour, data storage, and sharing practices, are likely interconnected, making oblimin rotation the most suitable choice for capturing these

relationships. Three distinct factors (PA1, PA2, and PA3) were identified. These factors accounted for 19% (PA1), 11% (PA2), and 10% (PA3) of the variance. The first factor is called “manufacturers and third parties misconceptions” since almost all these misconceptions are about what manufacturers, or third parties do with your data. The second factor is called “recording and collection misconceptions” since this covers the topics of these misconceptions. The last factor is called “spoken commands”. Most of these misconceptions mention spoken commands.

Table 8

*Factor loadings based on a principal components analysis with oblimin rotation for the 15 items of the Misconception Scale (*N = *155)*

Item	PA1	PA2	PA3
Q17_1: Smart speakers only collect data when they have an active internet connection. (Correct)		.62	
Q17_2: Smart speakers record every conversation held around them. (Incorrect)		.40	
Q17_3: Smart speakers can only record spoken commands, not background noises or sounds. (Incorrect)			.39
Q17_4: Smart speakers can accidentally think they hear the wake word and then start recording what has been said. (Correct)		.37	.40
Q17_5: Smart speakers record conversations after the wake word (e.g. "Hey Google/Alexa") is spoken. (Correct)		.37	
Q18_1: Manufacturers indefinitely store personal data collected by smart speakers, if you did not indicate you do not want this. (Correct)	.47		
Q18_2: Smart speakers can recognize different human individuals and store separate data profiles. (Correct)	.26		-.22
Q18_3: Spoken commands recorded by smart speakers are deleted immediately after the task is completed. (Incorrect)			.31
Q18_4: Smart speakers can only access information like passwords or bank account details if you provide this information. (Correct)		.39	
Q18_5: Smart speakers can store or retain any personal data after the task is completed. (Correct)	.31		
Q19_1: Manufacturers (first-party developers) share specific smart speaker data with third-party developers. (Correct)	.61		
Q19_2: Smart speakers collect data from other connected smart home devices inside a home and share this with their manufacturer. (Correct)	.55		
Q19_3: Government agencies can access my smart speaker data without my knowledge. (Correct)	.52		
Q19_4: Specific employees of manufacturers listen to voice recordings of smart speakers. (Correct)	.60		
Q19_5: As a smart speaker user, you have complete control over how your data is shared. (Incorrect)			.73

Note. Between brackets is indicated if the item is factual correct or incorrect. Factor loadings < .20 are suppressed

Discussion

This research aimed to address the question of how privacy misconceptions about smart speakers relate to perceived knowledge and privacy-protective behaviours across different user types. The results indicate that misconceptions about the privacy of smart speakers were prevalent across all user groups, with no significant differences between primary users, secondary users, non-users, and visitors. The most common misconceptions were: *"Smart speakers record every conversation held around them"* (incorrect), and *"Smart speakers only collect data when they have an active internet connection"* (correct).

For perceived knowledge, the study demonstrates a significant difference between primary users and non-users. Primary users perceived themselves as more knowledgeable than non-users did. Surprisingly, participants who perceived themselves as more knowledgeable tended to hold slightly more misconceptions. The protective behaviour scores also varied significantly among the user groups. The data suggests that visitors and non-users reported that they would engage more in protective behaviours than primary and secondary users intended to. There was no significant correlation between misconceptions and the protective behaviour score.

Contrary to the formulated hypothesis, "Non-users and visitors hold more misconceptions than primary and secondary users", misconceptions were equally prevalent across all user groups. This suggests that user experience does not necessarily improve the knowledge people have about smart speaker privacy. These results contradict the research of Zeng et al. (2017), who stated that visitors know less of the privacy risks of smart speakers than users, as is also mentioned by Meng et al. (2021). However, it is important to note that Zeng et al. (2017) employed semi-structured interviews to explore participants' privacy concerns and technical understanding of smart homes. Their findings focused primarily on knowledge gaps, which are incomplete or insufficient understandings, rather than on

misconceptions, which can be defined as false beliefs. As is shown in my study, there was a different result when participants were tested on knowledge gaps (Incorrectness score) and not on misconceptions. This discrepancy and the fact that Zeng et al. (2017) used other methods in their research, may explain the different conclusions.

A possible explanation for the lack of difference is that both users and non-users have a similar incomplete understanding of the privacy implications associated with smart speakers. As is discussed by Lau et al. (2018), there is a lack of clear, detailed information about the technical workings of smart speakers, such as how recordings are stored, shared, or processed. Malkin et al. (2019) also indicated that manufacturers do not provide users of smart speakers with enough understandable and detailed information about their privacy. All of this could explain that there is no difference in misconceptions between the different user groups, contrary to what was hypothesised.

The second hypothesis proposed that primary users perceive themselves as more knowledgeable about smart speaker privacy than secondary users, visitors, and non-users. Results showed a significant difference, with primary users perceiving themselves as more knowledgeable than non-users. Note that the significant variability is small. The third hypothesis suggested that fewer misconceptions correlate with higher perceived knowledge. However, participants with more misconceptions reported higher perceived knowledge, highlighting a discrepancy between perceived and actual understanding. The results of both hypotheses could be the consequence of the low variability in the perceived knowledge scale. The mean score of all the participants was 1.7 (SD = 0.7), so the results were al skewed to the left. This could lead to different correlations to the other variables because the general perceived knowledge of the participants was low. Besides this, the first question of the perceived knowledge scale is quite general: *"How much do you know about the privacy aspects of a smart speaker?",* while the questions 2 until 5 are more specific, for example:

"How much do you know about the sharing and selling of data collected by manufacturers of smart speakers?". It could be that people felt that they know quite a lot in general, but they realised the know little when they got asked about specifics. This could also have influenced the perceived knowledge score.

The results of the second and third hypotheses do align with findings from De Kimpe et al. (2021), who explored the relationship between perceived knowledge, trust, and protective behaviour in a cybersecurity context. Their study showed that individuals with higher perceived knowledge tend to feel less vulnerable to risks. This means that users may overestimate their understanding of smart speaker privacy while underestimating potential dangers. This phenomenon is consistent with the Dunning-Kruger effect, where individuals with limited knowledge or expertise in a domain overrate their abilities (Kruger & Dunning, 1999). In the case of smart speaker privacy, primary users who perceive themselves as well-informed may misjudge their understanding, leading to flawed knowledge. For instance, while many of their participants considered themselves as well-informed, a significant number misunderstood important privacy features, showing that a high perceived knowledge can coexist with misconceptions. Thus, while primary users perceive themselves as more knowledgeable, their actual understanding of smart speaker privacy remains flawed, as was demonstrated by the similar misconception scores.

The fifth hypothesis was that secondary users, visitors, and non-users engage less in privacy-protective behaviours related to smart speakers than primary users. The findings showed that user type had no significant effect on the misconception scores and misconception scores had no significant effect on the protective behaviour score. However, there was a significant difference in the protective behaviour scores of different user types. In contrast to what was hypothesised, primary and secondary users had a lower protective behaviour score than non-users and visitors. This suggests that non-users would be more

likely to engage in protective behaviours than users. Note that non-users reported hypothetical behaviours since they had to imagine owning a smart speaker.

A possible explanation for this result is the fact that the protective behaviour questions are placed at the end of the questionnaire. As is shown by Neuert (2021), items placed at the end of a questionnaire tend to be answered with less attention than items at the beginning. It was indicated in the questionnaire that users had to fill in what kind of behaviours they perform and that non-users had to imagine what behaviours they hypothetically would perform if they had a smart speaker. This could also have influenced the scores of non-users. Since non-users and visitors had to report hypothetical, future behaviour, it could be that they might not have realised yet that these behaviours take effort and time. Despite all their good intentions, it could be that because of this they will not carry out the behaviours in practice. It is also possible that some people choose not to own a smart speaker because they perceive the privacy risks to be too high. If non-users were to imagine themselves having a speaker, they might become more aware of the associated risks and, in turn, report higher intentions to engage in protective behaviours. However, this reported behaviour remains hypothetical, and the effort required to sustain such actions in practice might prevent these intentions from being realised.

As is described by Risius et al. (2020), there is a phenomenon called the privacy paradox, which explains that despite people's best privacy-protecting intentions, it is often found that they poorly protect their information online. It could be the case that non-users did not think far enough and indicated that they would perform these protective behaviours because they just answered all sorts of statements about the privacy risks of smart speakers.

Additionally, research by De Kimpe et al. (2021) highlights that individuals with greater perceived knowledge often feel less vulnerable to privacy risks. This sense of invulnerability may lead them to perform fewer protective behaviours. One reason for this is

that primary users may develop a higher level of trust in the manufacturer or the device itself. This trust could stem from the assumption that the device is secure or that the manufacturer has implemented sufficient safeguards to protect their privacy. As a result, these users might feel comfortable trading a part of their privacy for the convenience and functionality that smart speakers offer (Lau et al., 2018). They might prioritize convenience over privacy concerns, assuming that any potential risks are adequately managed by manufacturers.

Implications

The findings of this study emphasise the importance of providing clear and accessible privacy information from manufacturers. Regardless of their experience with smart speakers, users tend to hold significant misconceptions about privacy risks. This indicates that manufacturers have a responsibility to offer transparent and user-friendly information about how data is collected, stored, and shared. This is important because then users can make more well-considered choices in buying smart speakers or not.

For policymakers, these results underline the importance of stricter regulations on privacy disclosures. Privacy disclosures refer to the information that companies provide to consumers about how their data is collected, used, stored, and shared. These disclosures should be clear, concise, and easy to understand, as demonstrated by findings from research on data transparency (Acquisti et al., 2015). Simplified summaries of data usage policies or visual aids that highlight key privacy risks and protection measures have been shown to enhance comprehension and engagement. Policymakers should enforce standards that ensure these disclosures are consistent and accessible to all consumers.

Lastly, the perceived knowledge scale and the misconception scale were created by the researcher. These scales could be a benefit for the scientific community because they could be used in further research around this topic.

Strengths and Limitations

This study had several strengths that enhance its contribution to the understanding of privacy misconceptions and protective behaviours related to smart speakers. Firstly, the measurement tools used in this research, mostly created by the researcher, all demonstrated high reliability, as is shown by the Cronbach's alpha values exceeding .85. This ensures that the findings are based on reliable measurements. Next to this, this study focuses on an underexplored but important topic. Privacy misconceptions and behaviours regarding smart speakers are not yet studied much, which means that this research could add important new information to this topic.

Despite the strengths, this study is not without limitations. Since the participants are predominantly recruited through the social network of the researcher, the sample was rather small ($N = 155$) and consisted mostly out of Dutch students. This limits the generalisability of the findings to other cultural and educational contexts. Besides this, the results are based on self-reported measures. This may have caused several biases in the protective behaviour scale, such as social desirability and hypothetical responses.

Future Research

Future research could build on the findings of this study by focusing on how specific user types form their privacy misconceptions. It could be investigated if campaigns about misconceptions could improve people's privacy-protective behaviour. These could for example be online campaigns that show people what smart speakers do with all your personal data. Including qualitative methods, such as interviews or focus groups, would be a good addition to the survey findings and could provide more data on the motivations and perceptions of participants. Future studies could also dive deeper into the relation between perceived knowledge and actual knowledge to better understand this discrepancy. It would be

interesting to investigate on what people base their knowledge and why they overestimate their actual knowledge about smart speaker privacy. Next to this, it could be interesting to calculate correlations between the items or the three factors of the misconception scale and the perceived knowledge scale, to see whether specific misconceptions are related to specific perceived knowledge types. Finally, the long-term relationship between perceived knowledge, misconceptions and privacy behaviours could be examined to gain valuable insights for improving user awareness and behaviour.

Conclusion

Privacy concerns related to smart speakers have been a significant issue for some time. This study researched the relationship between user type, privacy misconceptions, perceived knowledge, and privacy-protective behaviours. The conclusions are that misconceptions about privacy are equally prevalent across all four user types, which suggests that the experience participants have with smart speakers does not necessarily mean that they know more about their privacy risks. Furthermore, primary users perceive themselves as more knowledgeable than other users, but their actual understanding of smart speakers is similar compared to other user types. Additionally, there was no significant correlation between the misconception score and protective behaviours, but users tend to engage in fewer privacy-protective behaviours than non-users and visitors. This could be because of the time and effort required for these behaviours, or because of their willingness to trade privacy for convenience or their trust in the manufacturers. Future research could investigate why users tend to engage less in privacy-protective behaviours, examining factors such as perceived effort, convenience, and trust in manufacturers. Additionally, studies could explore how to effectively reduce misconceptions and encourage protective behaviours among different user types.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Al-Ameen, M. N., Chauhan, A., Ahsan, M. M., & Kocabas, H. (2021). A look into user's privacy perceptions and data practices of IoT devices. *Information And Computer Security*, *29*(4), 573–588. https://doi.org/10.1108/ics-08-2020-0134

Arm Ltd. (n.d.). *What are smart devices*. Arm | The Architecture for the Digital World. https://www.arm.com/glossary/smart-devices

BBC News. (2019, April 11). *Smart speaker recordings reviewed by humans*. https://www.bbc.com/news/technology-47893082

CBS. (2022, January) *How many people use the Internet of Things? - The Netherlands in numbers 2021*. How Many People Use The Internet Of Things? - The Netherlands in Numbers 2021 | CBS. https://longreads.cbs.nl/the-netherlands-in-numbers-2021/how-many-people-use-the-internet-of-things/#:~:text=Nearly%20three%2Dquarters%20of%20the,data%20online%20without%20human%20intervention.&text=Cars%2C%20refrigerators%2C%20ovens%2C%20speakers,be%20connected%20to%20the%20internet.

Console & Associates P.C. (2024, July 22). The Impact of Data Breaches on Children and Minors. *Data Breach Information*. https://databreachclassaction.io/blog/the-impact-of-data-breaches-on-children-and-minors

Cruz, B. (2024, September 24). *2024 Deepfakes Guide and Statistics*. Security.org. https://www.security.org/resources/deepfake-statistics/

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived

knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour And Information Technology*, *41*(8), 1796–1808. https://doi.org/10.1080/0144929x.2021.1905066

Gartner, Inc. (2014, March 24). Gartner says a thirty-fold increase in internet-connected physical devices by 2020 will significantly alter how the supply chain operates. Gartner. Retrieved October 1, 2024, from https://www.gartner.com/en/newsroom/press-releases/2014-03-24-gartner-says-a-thirty-fold-increase-in-internet-connected-physical-devices-by-2020-will-significantly-alter-how-the-supply-chain-operates

Harris, S. (2017, April 14). Your Samsung SmartTV Is Spying on You, Basically. *The Daily Beast*. https://www.thedailybeast.com/your-samsung-smarttv-is-spying-on-you-basically

Jarvis, J. (2023, November 9). IoT vs Smart Devices: what is the difference? - James Jarvis-Medium. *Medium*. https://medium.com/@jamesjarviscyber/iot-vs-smart-devices-what-is-the-difference-ae40664fc1ec

Kim, D., Park, K., Park, Y., & Ahn, J. (2018). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2009). Smart objects as building blocks for the Internet of things. *IEEE Internet Computing*, *14*(1), 44–51. https://doi.org/10.1109/mic.2009.143

Kraft, A. (2015). VTech toymaker hack exposes parents and kids. CBS News. https://www.cbsnews.com/news/vtech-toymaker-hack-exposes-parents-and-their-kids/

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal Of Personality And Social Psychology*, *77*(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121

Lau, J., Zimmerman, B., & Schaub, F. (2018). *Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers*. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 2, No. CSCW, pp. 1-31). https://doi.org/10.1145/3274371

Leetaru, K. (2015, December 13). When toys are hackable and our children become data breach victims. *Forbes*. https://www.forbes.com/sites/kalevleetaru/2015/12/12/when-toys-are-hackable-and-our-children-become-data-breach-victims/

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

Masterson, K. (2023, February 6). *Criminals Target Children for Identity Theft and Fraud*. AARP. https://www.aarp.org/money/scams-fraud/info-2022/child-identity-theft.html

Meng, N., Keküllüoğlu, D., & Vaniea, K. (2021). Owning and Sharing. *Proceedings Of The ACM On Human-Computer Interaction*, *5*(CSCW1), 1–29. https://doi.org/10.1145/3449119

Neuert, C. E. (2021). The Effect of Question Positioning on Data Quality in Web Surveys. *Sociological Methods & Research*, *53*(1), 279–295. https://doi.org/10.1177/0049124120986207

Shelley Mallett. (2004). Understanding Home: A Critical Review of the Literature. The Sociological Review 52, 1 (February 2004), 62–89. https://doi.org/10.1111/j.1467-954X.2004.00442.x

Oxford University Press. (n.d.). *Misconception*. *Oxford Learner's Dictionaries*. https://www.oxfordlearnersdictionaries.com/definition/american_english/misconception

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., & Logé, C. (2006). *The smart home concept: Our immediate future*. LTI, EDF R&D, LaRIA.

Risius, M., Baumann, A., & Krasnova, H. (2020). Developing a New Paradigm: Introducing the Intention-Behaviour Gap to the Privacy Paradox Phenomenon. *European Conference On Information Systems*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1149&context=ecis2020_rp

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*(15), 1-53.

Schomakers, E., Biermann, H., & Ziefle, M. (2020). Understanding Privacy and Trust in Smart Home Environments. In *Lecture notes in computer science* (pp. 513–532). https://doi.org/10.1007/978-3-030-50309-3_34

Statista. (2024, September 11). *Number of IoT connections worldwide 2022-2033*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Stringer, G. (2023, August 15). What is a knowledge gap? HowNow. https://www.gethownow.com/blog/what-is-a-knowledge-gap

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 65-80).

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-20. https://doi.org/10.1145/3274469

Appendix A

Informed Consent

Informed Consent

Informed Consent for Research Participation
You are invited to participate in a research study about privacy perceptions, knowledge, and protective behaviours related to smart speakers, such as Amazon Echo (Alexa), Google Home (Google Assistant), and Apple Home Pod (Siri). The study is conducted by Luuk Scheuneman at the University of Twente under the supervision of Michelle Walterscheid and Nicole Huijts. The purpose of this research is to understand how much users know about the privacy of smart speakers, and how they protect their privacy. If you choose to participate, you will complete a questionnaire about your knowledge, concerns, and behaviours regarding smart speakers. The survey will take about 15 minutes. Participation in this study is entirely voluntary. You can choose not to participate, or you may stop at any time without penalty. If you withdraw, your data will not be used in the analysis. Your responses will remain confidential and anonymous. No personally identifiable information will be collected, and the results will be used only for research purposes. The data will be securely stored and may be published or presented in an anonymized format. There are no known risks to participating in this study. While there are no direct benefits to you, your responses will help improve our understanding of privacy issues with smart speakers, potentially leading to better privacy protections. You can withdraw at any time without any consequences. If you have any questions, feel free to contact the researcher, Luuk Scheuneman, at l.scheuneman@student.utwente.nl.

Demographics

IC1 I have read and understood the study information.

- ○ Yes (1)
- ○ No (2)

IC2 I consent voluntarily to be a participant in this study and understand that I can withdraw from the study at any time, without having to give a reason.

- ○ Yes (1)
- ○ No (2)

IC4 I consent that the information I provide may be used for analysis and research, and may be published in scientific outlet in an anonymized form.

- ○ Yes (1)
- ○ No (2)

IC5 I understand that personal information collected about me that can identify me, such as my name, will not be recorded by the study team.

- ○ Yes (1)
- ○ No (2)

IC6 I understand that the answers I provide will be deleted from Qualtrics and stored in the repository of the University of Twente after the data collection is finished.

- ○ Yes (1)
- ○ No (2)

Appendix B

Primary or Secondary User Questions and Percentages

Primary or secondary Please indicate if you agree or disagree with the following statements about the smart speaker in your home.

	Percentage Agreed	Percentage Disagreed
I installed the smart speaker myself. (1)	71	29
I can personally control the usage and privacy settings of the smart speaker through my phone. (2)	77	23
The smart speaker is connected to my personal account. (3)	71	29
I regularly use the smart speaker (daily or multiple times a week). (4)	74	26

Appendix C

Perceived Knowledge Questions and Scores

Table C1

Perceived Knowledge Scores

Question	“Nothing”	“A little”	“A moderate amount”	“Much”	“Very much”
How much do you know about the privacy aspects of a smart speaker?	57	61	31	6	0
How much do you know about the types of data smart speakers collect?	61	66	19	8	1
How much do you know about where and how smart speakers store collected data?	91	46	14	4	0
How much do you know about who can access the data collected by smart speakers?	99	38	15	3	0
How much do you know about the sharing and selling of data collected by manufacturers of smart speakers?	82	52	15	5	1
Total	390	263	94	26	2

Appendix D

Misconception Questions

Q17 Please indicate how much you agree or disagree with the given statement.

	Strongly disagree (6)	Somewhat disagree (7)	Somewhat agree (8)	Strongly agree (9)	I don't know (10)
Smart speakers only collect data when they have an active internet connection. (17_1)	○	○	○	○	○
Smart speakers record every conversation held around them. (17_2)	○	○	○	○	○
Smart speakers can only record spoken commands, not background noises or sounds. (17_3)	○	○	○	○	○
Smart speakers can accidentally think they hear the wake word and then start recording what has been said. (17_4)	○	○	○	○	○
Smart speakers record conversations after the wake word (e.g. "Hey Google/Alexa") is spoken. (17_5)	○	○	○	○	○

Correct answers: 17_1: Agree 17_2: Disagree 17_3: Disagree 17_4: Agree 17_5: Agree

	Strongly disagree (6)	Somewhat disagree (7)	Somewhat agree (8)	Strongly agree (9)	I don't know (10)
Manufacturers indefinitely store personal data collected by smart speakers, if you did not indicate you do not want this. (18_1)	○	○	○	○	○
Smart speakers can recognize different human individuals and store separate data profiles. (18_2)	○	○	○	○	○
To ensure you are paying attention, please select “Somewhat agree” as your answer for this statement. (A)	○	○	○	○	○
Spoken commands recorded by smart speakers are deleted immediately after the task is completed. (18_3)	○	○	○	○	○

Smart speakers can only access information like passwords or bank account details if you provide this information. (18_4)	○	○	○	○	○
Smart speakers can store or retain any personal data after the task is completed. (18_5)	○	○	○	○	○

Correct answers: 18_1: Agree 18_2: Agree 18_3: Disagree 18_4: Agree 18_5: Agree

	Strongly disagree (1)	Somewhat disagree (2)	Somewhat agree(3)	Strongly agree (4)	I don't know (5)
Manufacturers (first-party developers) share specific smart speaker data with third-party developers. (19_1)	○	○	○	○	○
Smart speakers collect data from other connected smart home devices inside a home and share this with their manufacturer. (19_2)	○	○	○	○	○
Government agencies can access my smart speaker data without my knowledge. (19_3)	○	○	○	○	○
Specific employees of manufacturers listen to voice recordings of smart speakers. (19_4)	○	○	○	○	○
As a smart speaker user, you have complete control over how your data is shared. (19_5)	○	○	○	○	○

Correct answers: 19_1: Agree 19_2: Agree 19_3: Agree 19_4: Agree 19_5: Disagree

Appendix E

Protective Behaviour Scores and Questions

Table E1

Protective Behaviour Scores

Question	"Extremely unlikely"	"Unlikely"	"Neutral"	"Likely"	"Extremely likely"	Mean Scores
Q26_1	42	51	18	31	13	2.5
Q26_2	76	47	14	12	6	1.9
Q26_3	66	57	17	13	2	1.9
Q26_4	57	57	18	17	6	2.1
Q26_5	35	53	23	27	17	2.6
Q26_6	22	39	27	39	28	3.1
Q26_7	58	58	22	13	4	2.0
Q26_8	54	47	24	20	10	2.3
Q26_9	38	55	21	31	9	2.5
Q26_10	90	46	14	3	1	1.6
Q26_11	86	48	16	5	0	1.6
Total	624	558	214	211	96	2.2

	Extremely unlikely (1)	Unlikely (5)	Neutral (6)	Likely (7)	Extremely likely (3)
I turn off the smart speaker when I am not using it. (26_1)	○	○	○	○	○
I unplug the smart speaker when I am not using it. (26_2)	○	○	○	○	○
I unplug the smart speaker when I am having private conversations. (26_3)	○	○	○	○	○
I turn off the smart speaker when I am having private conversations. (26_4)	○	○	○	○	○
I review the privacy settings of my smart speaker in the providers (e.g. Alexa or Google) account. (26_5)	○	○	○	○	○
Through the settings, I restrict the amount of data that the smart speaker is allowed to collect. (26_6)	○	○	○	○	○
I review my smart speaker recordings. (26_7)	○	○	○	○	○

I delete my smart speaker recordings. (26_8)	○	○	○	○	○
I change the password of my smart speaker account. (26_9)	○	○	○	○	○
I speak very quietly around the smart speaker, in case I do not want to be recorded. (26_10)	○	○	○	○	○
I give misleading information to the smart speaker. (26_11)	○	○	○	○	○
I moderate my language around the smart speaker so that it does not record private matters, even if accidentally. (26_12)	○	○	○	○	○
I avoid private conversations around the smart speaker. (26_13)	○	○	○	○	○