Developing and Testing a Multidimensional Scale for Perceived Privacy Concerns of Smart Speakers

Sanae Akchich (s2954001)
Faculty of Behavioural Management and Social Sciences, University of Twente
Department of Psychology of Conflict, Risk and Safety
1st Supervisor: Dr. Nicole Huijts
2nd Supervisor: Michelle Walterscheid
1st July 2025

Abstract

Smart home technologies, particularly voice-controlled devices like smart speakers, have introduced new privacy challenges for users. While previous research has highlighted that privacy concerns influence user acceptance, existing measurement approaches are inconsistent and often fail to reflect the multidimensional nature of perceived privacy concerns. This study addresses this gap by developing and empirically testing a scale that captures users' perceived privacy concerns across five stakeholder-related dimensions: company, government, household, third-party and cybersecurity threats. Drawing on prior frameworks and a literature-informed item development process, a survey was conducted among mostly German participants (N = 127) and analysed using exploratory factor analysis and reliability testing. Results support a four-factor model, excluding the third-party dimension due to insufficient empirical support. Additional analyses examined associations between privacy concerns, protective behaviours, gender, and device ownership. Findings revealed that household and cybersecurity concerns predicted privacy-protective behaviours, with non-owners reporting higher concern and action levels than owners, and women reporting slightly more protective behaviours than men. The findings provide an empirically tested tool for future privacy research and offer practical implications for developers and policymakers seeking to address user concerns in smart home environments.

Keywords: Smart home; Smart speakers; Perceived privacy concerns

Introduction

The growing integration of smart speakers, such as Amazon Echo or Google Home, into everyday life has transformed domestic routines by enabling voice-controlled automation, personalized assistance, and seamless interaction with other smart home devices. These technologies offer users convenience and efficiency by allowing remote control of home functions, facilitating daily tasks, and collecting usage data for system optimization. However, the increasing presence of smart speakers has also raised significant concerns regarding data security and privacy. These devices are typically always-on, equipped with microphones, constantly listening for voice commands, and often connected to cloud-based systems that store and process personal data. As a result, users may feel uncertain about who can access their data, how it is used, and whether their privacy is adequately protected (Emami-Naeini et al., 2019).

While many users may benefit from these technologies, they also face trade-offs between convenience and control over personal data. These tensions have prompted researchers to investigate how individuals perceive privacy risks associated with smart home devices. So far, most studies have approached this topic by examining general attitudes or specific behaviours, but few have offered a comprehensive way to measure privacy concerns in a structured and multidimensional manner. This study aims to address that gap by developing and empirically testing a scale for perceived privacy concerns related to smart speakers.

Perceived Privacy Concerns

A distinction must be made between objective and perceived privacy concerns. Objective privacy concerns refer to actual risks posed by smart home IoT systems, such as technical vulnerabilities or unauthorized access. In contrast, perceived privacy concerns reflect users' subjective impressions; what they believe might happen, who they think may access their data, and how vulnerable they feel, regardless of the technical reality. For instance, some users may assume that any data collected by their smart speaker is automatically shared with third-party advertisers or government agencies, even without concrete evidence. Others may feel uneasy using the device simply because they do not fully understand how it operates or what data it collects.

Lenhart et al. (2023) emphasize that such perceptions are shaped less by actual security vulnerabilities and more by individual experience, media coverage, and personal awareness. Similarly, Kehr et al. (2015) highlight that privacy concerns are not purely rational, but are also influenced by emotional responses. Users who feel anxious or distrustful about how their

data is handled are less likely to adopt smart home devices. This distinction is critical, as perceived risks have been found to play a more influential role in shaping user behaviour than objective risks (Al-Husamiyah & Al-Bashayreh, 2021; Shuhaiber & Mashal, 2019).

Existing Models and Measurement Gaps

Despite the growing attention to privacy issues in smart home contexts, existing studies have used a wide variety of instruments to measure perceived privacy risks (e.g., Al-Husamiyah & Al-Bashayreh, 2021; Fantinato et al., 2018; Kowalczuk, 2018; Sanguinetti et al., 2018; Shuhaiber & Mashal, 2019; Yang et al., 2018). These instruments often differ in their conceptual focus and rarely provide a systematic or empirically tested way to assess how users perceive distinct privacy threats. To our knowledge, no study has yet developed and empirically tested a comprehensive, multidimensional measure that captures how individuals perceive various types of privacy risks posed by smart home IoT devices. The present study addresses this gap by introducing and empirically testing a new scale of perceived privacy concerns, with a specific focus on smart speakers. The scale considers concerns related to different types of actors or sources of risk. In developing such a scale, it is essential to account not only for the existence of privacy concerns but also for their complexity.

An important source of this complexity lies in the multi-stakeholder nature of smart home IoT environments, which exposes users to a range of privacy threats originating from various actors (Guhr et al., 2020; Lutz & Newlands, 2021; Zeng et al., 2017). Traditionally, privacy concerns have focused on external threats, such as unauthorized access by hackers or government surveillance. These risks have dominated the discourse around data security, particularly in terms of system vulnerabilities and large-scale data misuse (Guhr et al., 2020). However, recent research emphasizes that institutional actors, such as technology companies and regulatory bodies, also play a crucial role in shaping privacy concerns (Emami-Naeini et al., 2019; Zheng et al., 2018). These entities are responsible for data collection, processing, and enforcement of privacy policies, which adds another layer of perceived risk. As Lenhart et al. (2023) argue, privacy in smart homes must be understood beyond a narrow cybersecurity lens.

Finally, and perhaps most uniquely to smart homes, are the interpersonal privacy concerns that arise within the household itself. Huang et al. (2020) and Lutz and Newlands (2021) highlight that users often worry about housemates, landlords, or family members accessing personal data via shared devices, challenging the conventional understanding of privacy as solely an individual versus external entity issue. These interpersonal dynamics illustrate that smart home privacy is not only about external intrusions but also about

managing boundaries within shared living environments. Taken together, these developments call for a conceptualization of privacy that includes cybersecurity, institutional, and interpersonal risks.

However, translating this conceptual complexity into a consistent and reliable measurement has proven difficult (Al-Husamiyah & Al-Bashayreh, 2021; Fantinato et al., 2018). Many studies use single-item measures or ad-hoc scales (Al-Husamiyah & Al-Bashayreh, 2021). Although some focus on specific dimensions like institutional or cybersecurity threats (Haug et al., 2020), there remains a lack of integrated, stakeholder-sensitive models.

A notable exception is the work by Lutz and Newlands (2021), who proposed a multidimensional framework for smart speaker privacy concerns, including categories such as device, institutional, government, household, contractor, and third-party risks. While their framework is conceptually rich, it was not empirically validated through techniques such as exploratory factor analysis (EFA), leaving open questions about the actual structure of these concern domains. The present study builds on their work by conducting an EFA to uncover the latent structure of perceived privacy concerns and to assess whether user concerns meaningfully cluster around different types of risk sources. In doing so, this study follows established scale development procedures (e.g., Boateng et al., 2018), including systematic item generation, expert review, and psychometric evaluation.

Dimensions of Perceived Privacy Concerns

As discussed earlier, privacy concerns in smart home environments stem from a range of sources, reflecting the involvement of multiple stakeholders. In this section, we elaborate on the five core dimensions of perceived privacy concerns that guided the development of the present scale: institutional, governmental, household, third-party, and cybersecurity-related risks.

(1) Institutional or Manufacturer Privacy Concerns

These concerns pertain to how manufacturers and corporations collect, store, and share user data. Users are often apprehensive about unclear privacy policies and the lack of user control over data collection. Companies often justify data collection by citing service improvements or personalization benefits, yet users remain wary of how this data is stored, who can access it, and whether it is shared with third parties for advertising or other commercial purposes. The ambiguity surrounding data retention policies exacerbates these fears, leading to heightened scepticism toward smart home IoT manufacturers (Dinev & Hart, 2006; Kehr et al., 2015; Lutz & Newlands, 2021).

(2) Government Surveillance Concerns

These reflect fears about state authorities accessing smart home data. Lenhart et al. (2023) argue that concerns about mass surveillance have intensified with the growing presence of IoT devices that continuously monitor and transmit data. Some users express apprehension about the potential for law enforcement agencies or intelligence services to exploit smart home technologies for surveillance purposes. These fears are often fuelled by media reports on government data collection programs, reinforcing a perception that smart home data could be used for monitoring or investigative purposes without explicit user consent.

(3) Household Privacy Concerns

These introduce a more interpersonal dimension to privacy concerns. Unlike institutional or governmental risks, these involve worries about data access within shared living spaces. Lutz & Newlands (2021) highlight that smart home devices can inadvertently create conflicts among cohabitants, as they may expose personal activities or interactions to roommates, landlords, or family members. This issue is particularly significant in multi-person households, where different users may have varying levels of privacy sensitivity. For example, a smart speaker that logs voice commands may store interactions that another household member could later access, creating unintended privacy violations (Huang et al., 2020).

(4) Third-Party Data Access Concerns

These risks stem from the possibility of access to smart home data by external entities that are not the manufacturer of the device but may receive user data for purposes such as advertising, analytics, or service delivery. Examples include marketing agencies, software vendors, or data brokers. Lenhart et al. (2023) emphasize that users fear that smart home ecosystems could be exploited for targeted marketing, cyber-attacks, or even identity theft. The interconnected nature of smart home devices, which often rely on cloud computing and third-party integrations, increases users' vulnerabilities to such risks.

(5) Cybersecurity Concerns.

These remain a significant deterrent for smart home IoT adoption. Lutz & Newlands (2021) point out that users perceive smart home devices as vulnerable to hacking, unauthorized access, and device manipulation. The increasing number of cybersecurity incidents involving IoT devices, such as smart cameras being hacked or unauthorized third parties taking control of smart locks, reinforces the perception that smart home ecosystems are susceptible to exploitation. Users who have lower confidence in the security features of

these devices may also perceive them as more privacy-invasive, which can influence their willingness to adopt such technologies.

Together, these five dimensions form the foundation for developing a multidimensional scale to assess perceived privacy concerns. By addressing the multidimensional nature of privacy concerns, this scale will provide a more comprehensive assessment of user perceptions and allow for more consistent comparisons across studies.

Current Study

This study aims to develop and empirically test a multidimensional scale for measuring perceived privacy concerns associated with smart home IoT devices. The scale focuses on five key dimensions as outlined above.

In addition to developing the scale, this study also takes a first step toward validating it by examining both predictive and discriminant validity, which are crucial for establishing the practical and conceptual usefulness of a measurement instrument.

Discriminant validity refers to whether the scale can differentiate between groups that, based on theory and prior research, are expected to vary in their privacy perceptions and behaviours. Ownership status is expected to influence privacy concerns and behaviours. From a theoretical perspective, this expectation aligns with the privacy paradox and technology acceptance models, which suggest that users who adopt and regularly interact with a technology tend to adjust their risk perceptions over time (Gerber et al., 2018). As individuals become more familiar with smart speakers, they may develop a sense of control or habituation, leading to lower perceived privacy risks despite the continued presence of objective risks (Kokolakis, 2015; Wairimu et al., 2018). This process reflects a cognitive adaptation, where repeated exposure reduces uncertainty and perceived threat.

In terms of behaviour, owners are also theorized to engage less frequently in privacy-protective actions. This may be due to desensitization or the perception that initial protective steps (e.g., disabling certain features) are sufficient. Alternatively, continued use despite concerns may lead to resigned acceptance, wherein users perceive privacy violations as unavoidable trade-offs for convenience (Wairimu et al., 2018). Thus, both psychological adaptation and behavioural normalization are expected to differentiate owners from non-owners in how they perceive and manage privacy risks.

Gender is likewise expected to shape both the perception of privacy risks and the behaviours adopted to cope with them. Prior research has shown that women generally report higher levels of privacy concern, which may stem from heightened sensitivity to surveillance, increased perceived vulnerability, or broader socialization patterns that emphasize caution and

self-protection (Stevic et al., 2021). These elevated concerns often translate into more proactive privacy-preserving behaviours. For instance, women are more likely than men to limit the amount of personal information they share and to adjust privacy settings to restrict data access (Tifferet, 2018). Such patterns suggest that gender differences in privacy management are not only a matter of perception but also of response, shaped by differences in risk appraisal, emotional reactivity, and the perceived consequences of exposure. As a result, female participants are expected to report both higher perceived privacy concerns and greater engagement in privacy-protective behaviours compared to their male counterparts. To formally test these assumptions, the following hypotheses were formulated:

H1: Higher perceived privacy concerns will be positively correlated with more privacy-protective behaviours.

H2a: Participants who own a smart speaker will perceive lower privacy concerns than those who were asked to imagine owning one.

H2b: Participants who own a smart speaker will engage in fewer privacy-protective behaviours than participants imagining ownership.

H3a: Female participants will report higher perceived privacy concerns than male participants.

H3b: Female participants will report more privacy-protective behaviours than male participants.

Methods

Participants

Participants were recruited through convenience sampling, the university SONA system (online participant recruitment platform), and social media platforms. Inclusion criteria required participants to be at least 18 years old and sufficiently proficient in English to understand the questionnaire. A total of 152 participants participated in the survey. Of the 152 participants who completed the survey, 18 were excluded for failing the embedded attention check and 7 were removed due to incomplete responses, resulting in a final sample of 127 participants. This meets the recommended minimum of 100 participants required to conduct exploratory factor analysis (EFA) (Kline, 2014).

Participants were on average 32 years old (median 25; *SD* = 14.67; range from 18 to 75), indicating a young to middle-aged profile. The sample consisted of 52 females (40.9%), 72 males (56.7%), and 3 participants who identified as another gender (2.4%). Most participants were of German nationality (62.2%), followed by Dutch (11.0%), American (6.3%), Turkish (3.1%), and other nationalities (17.3%). Regarding educational background,

35.3% had completed high school, 45.7% held a bachelor's degree, 15.8% a master's degree, and 3.2% held a PhD. Slightly more than half of the participants (52.0%) were currently enrolled as students. In terms of smart speaker ownership, 29.1% of the participants owned a smart speaker, while the remaining 70.9% did not. Participants detailed demographic characteristics can be found in Appendix B. Participation was completely voluntary and anonymous, and the study was approved by the Ethical Review Committee of the Faculty of Behavioural, Management and Social Sciences at the University of Twente.

Design & Materials

This study employed a cross-sectional survey design. Participants were grouped based on their self-reported smart speaker ownership status: those who owned a smart speaker and those who did not. Although ownership status was not experimentally manipulated, it served as a quasi-independent variable, allowing for comparisons between actual owners and non-owners who were asked to imagine owning a device. The main dependent variables were perceived privacy concerns, which were measured across five dimensions, and privacy-protective behaviours, which were assessed across three categories. The survey was administered online via the Qualtrics platform and can be found in Appendix C.

Measurements

Perceived Privacy Concerns Scale. The items used to measure perceived privacy concerns were developed based on established literature on privacy concerns in the context of smart home IoT. The five-dimensional structure of privacy concerns (e.g. manufacturer, government, household, third-party, cybersecurity) was adapted from the conceptual framework proposed by Lutz and Newlands (2021). The item development process followed the recommendations outlined by Boateng et al. (2018) for scale construction in social science research.

To construct items for each dimension, a range of prior studies that explored user perceptions, concerns, and behaviours related to smart devices were consulted. For example, Zeng et al. (2017) provided qualitative insights into users' privacy concerns in smart homes, especially in relation to data sharing, surveillance, and unintended access. Similarly, Emami-Naeini et al. (2019) examined how users evaluate privacy concerns and what factors shape their protective choices. Lee and Kobsa (2016) offered quantitative measures of perceived risk and trust in smart home systems, while Lenhart et al. (2023) developed and validated items tailored to privacy concerns with smart speakers, which served as a contemporary benchmark.

Although no single existing scale aligned exactly with the five selected dimensions, the wording and structure of items were inspired by previously validated items and

thematically adapted to the smart speaker context. Items were carefully crafted to reflect concrete user concerns while maintaining clarity and conceptual alignment with the targeted dimension. All items were reviewed by an expert in the field (Dr. Nicole Huijts).

The final scale included five dimensions: (1) Manufacturer Privacy Concerns, (2) Government Surveillance Concerns, (3) Household Privacy Concerns, (4) Third-Party Data Access Concerns, and (5) Cybersecurity Concerns. Each dimension consisted of five statements, resulting in a total of 25 items. The order of the statements was randomized. Participants were asked to rate their agreement with each statement on a 7-point Likert scale (1 = Strongly disagree to 7 = Strongly agree). The full scale can be found in Table 1.

Table 1

Perceived Privacy Concerns Scale

Item	Statement
	I am concerned that…
	Manufacturer Privacy Concerns
1	…I have no control over what happens with my data once it's collected by the company.
2	… people working at the manufacturer could access my personal data.
3	… smart speaker companies know too much about me through the data they collect.
4	… my data might be used by smart speaker manufacturers for purposes I'm not aware of.
5	… smart speaker companies may share my data without my consent.
	Government Surveillance Concerns
6	… laws do not sufficiently protect my smart speaker data from government access.
7	… smart speaker technology increases the risk of government surveillance.
8	… government agencies could access data collected by my smart speaker.
9	… my conversations at home could be used by government agencies.
10	… government agencies might not respect my privacy when it comes to data collected by my smart speaker.
	Household Privacy Concerns
11	… smart speakers could accidentally reveal private information to other household members during use.
12	… other household members might access my personal information through the smart speaker.
13	… the smart speaker records conversations I don't want others in my household to hear.
14	… the smart speaker can be used to monitor my activities at home by people I live with.
15	… others in my household could use the smart speaker to impersonate me or access features intended only for me.
	Third-Party Access Concerns
16	… third parties could gain access to my smart speaker data.
17	… third parties may use data from my smart speaker for advertising purposes.
18	… my smart speaker data could be sold to unknown companies without my knowledge.
19	… my smart speaker data could be shared with other companies for purposes I did not agree to.
20	… companies use vague policies to justify sharing my smart speaker data with third parties.
	Cybersecurity Concerns
21	… my smart speaker could be hacked.
22	… storing my smart speaker data in the cloud increases the risk of being hacked.
23	… technical vulnerabilities in my smart speaker could compromise my privacy.
24	… my smart speaker may not receive important security updates to protect it from new threats.
25	… my smart speaker does not have strong security measures in place.

Privacy-Protective Behaviours. Privacy-protective behaviours were measured using an adapted version of the scale developed by Pottkamp (2024), which was itself based on the

work of Lutz and Newlands (2021). Lutz and Newlands had originally proposed a three-category model of privacy protection behaviours, namely physical protection (e.g., unplugging the device), settings-based protection (e.g., adjusting privacy settings), and behavioural protection (e.g., avoiding sensitive conversations near the device), and have found empirical support for this structure. Pottkamp adopted the same conceptual structure, but their factor analysis only showed two factors.

In the present study, we aimed to build on this prior work by extending the scale of Pottkamp (2024) with three new items (Items 6, 13, and 17; see Table 2), leading to a total of 17 items. These additions aimed to expand the scale's coverage of household-related privacy dynamics, which may influence protective behaviours in shared living environments. Depending on ownership status, participants either reported on their actual behaviours (owners) or imagined behaviours (non-owners), all rated on a 7-point Likert scale (1 = Never to 7 = Always/ 1 = Extremely unlikely to 7 = Extremely likely), and the item order was randomized. A full list of the items and their categorization can be found in Table 2.

Table 2

Privacy-Protective Behaviour (gifted)

Category	Item	
Physical	1	I will turn off the smart speaker when I am not using it.
	2	I will unplug the smart speaker when I am not using it.
	3	I will turn off the smart speaker when I am having sensitive or private conversations.
	4	I will unplug the smart speaker when I am having sensitive or private conversations.
	5	I will place my smart speaker where I typically don't have sensitive or private conversations.
	6	I will avoid placing the smart speaker in shared spaces (e.g., living room) to reduce the chance that others in my household hear or access personal interactions.
Settings-based	7	I will mute the smart speakers microphone when I am not using it.
	8	I will review and adjust the privacy settings of my smart speaker.
	9	I will review which applications/services have access to my smart speaker.
	10	I will restrict the amount of data that the device is allowed to collect through the smart speakers' settings.
	11	I will delete my smart speaker recordings.
	12	In the app I will delete sensitive information that the smart speaker stored about me.
	13	I will set up multiple user accounts or voice profiles on the smart speaker to manage what other household members can access.
Behavioural	14	I will speak very quietly around the smart speaker when I don't want to be recorded.
	15	I will moderate my language around the smart speaker to avoid recording private matters.
	16	I will avoid sensitive or private conversations around the smart speaker.
	17	I will avoid giving voice commands to the smart speaker when other people in the household are around.

An exploratory factor analysis (EFA) was conducted on the 17 items to examine the underlying structure of the scale. Prior to conducting the EFA, the Kaiser-Meyer-Olkin

(KMO) measure confirmed sampling adequacy (*KMO* = .79), and Bartlett's test of sphericity was significant, $\chi^2(136) = 784.69$, $p < .001$, indicating the data were suitable for factor analysis. Based on eigenvalues greater than 1 and inspection of the scree plot, a three-factor solution was retained, aligning with the originally theorized structure. Given the conceptual overlap between protective strategies, principal axis factoring with oblimin rotation was employed to allow for correlated factors. Together, the three factors accounted for approximately 53.4% of the total variance.

The three factors corresponded well to the proposed dimensions. Factor loadings and communalities are presented in Table 3. The internal consistency of the overall scale was high (α = .89), with reliability coefficients for each subscale also indicating good internal consistency (α = .87 for physical, α = .75 for settings-based, and α = .80 for behavioural). Descriptive statistics (means and standard deviations) for each subscale and the full scale are reported in Table 4. For further analyses, items were grouped into the three subscales.

Table 3

Exploratory Factor Analysis of the 17-Item Privacy-Protective Behaviour Scale

Category	Item	1	2	3	Communality
Physical	I will turn off the smart speaker when I am not using it.	.72			.54
	I will unplug the smart speaker when I am not using it.	.76			.64
	I will turn off the smart speaker when I am having sensitive or private conversations.	.57			.52
	I will unplug the smart speaker when I am having sensitive or private conversations.	.54			.62
	I will place my smart speaker where I typically don't have sensitive or private conversations.	.71			.56
	I will avoid placing the smart speaker in shared spaces (e.g., living room) to reduce the chance that others in my household hear or access personal interactions.	.70			.61
Settings-based	I will mute the smart speakers microphone when I am not using it.		.60		.53
	I will review and adjust the privacy settings of my smart speaker.		.69		.51
	I will review which applications/services have access to my smart speaker.		.77		.61
	I will restrict the amount of data that the device is allowed to collect through the smart speakers' settings.		.72		.52
	I will delete my smart speaker recordings.		.53		.43
	In the app I will delete sensitive information that the smart speaker stored about me.		.49		.38
	I will set up multiple user accounts or voice profiles on the smart speaker to manage what other household members can access.		.43		.26
Behavioural	I will speak very quietly around the smart speaker when I don't want to be recorded.			.85	.78
	I will moderate my language around the smart speaker to avoid recording private matters.			.91	.78
	I will avoid sensitive or private conversations around the smart speaker.			.68	.62
	I will avoid giving voice commands to the smart speaker when other people in the household are around.			.56	.47

Note. Factor loadings < .30 are suppressed.

Table 4

Means, Standard Deviations, and Cronbach's Alpha for the Privacy-Protective Behaviour Scale and Its Three Dimensions

	Cronbach's α	*M*	*SD*
Overall Privacy-Protective Behaviour Scale	.89	4.53	1.05
Physical Privacy Protection	.87	4.52	1.41
Settings-based Privacy Protection	.75	5.27	1.13
Behavioural Privacy Protection	.80	4.04	1.30

Procedure

The survey began with an informed consent form that explained the purpose, procedure, and participants' rights. It clarified that participation was entirely voluntary, that

individuals could withdraw at any time without consequences, and that responses would remain completely anonymous. Participants were asked to confirm that they were at least 18 years old and that they agreed to take part in the study, only participants who gave active consent could proceed to the rest of the survey.

After providing consent, the survey began with demographic questions, including age, gender, nationality, education level, living arrangement, smart speaker ownership, and knowledge about smart speakers. Based on their self-reported ownership status, participants were automatically assigned to one of two conditions. Those who indicated that they owned a smart speaker were instructed to answer all subsequent questions based on their actual experience with the device. In contrast, participants who reported not owning a smart speaker were presented with a brief scenario asking them to imagine they had been gifted a smart speaker and were now using it in their home. This scenario was designed to ensure that all participants, regardless of actual ownership, could respond to the same set of statements.

All participants then completed the same Perceived Privacy Concerns Scale, followed by the Privacy-Protective Behaviour Scale. While the item content of the Privacy-Protective Behaviour Scale remained identical across conditions, minor wording adjustments were made: owners were asked to report their actual behaviour in the last three months, while non-owners rated the likelihood of engaging in the same actions. To enhance data quality, an attention check item was embedded within both sections. Additionally, the order of all scale items was randomized to minimize response bias. The full questionnaire is included in Appendix C.

Data Analysis

All analyses were conducted using RStudio (Version 2025.05.0+496.pro5). First, descriptive statistics were calculated to summarize the demographic characteristics of the participants and to inspect the distributions of key variables. To examine the structure of the Perceived Privacy Concerns Scale an exploratory factor analysis (EFA) was conducted using principal axis factoring with oblimin rotation, as the underlying factors were assumed to be correlated. The number of factors was determined based on a combination of theoretical expectations, eigenvalues greater than 1, and visual inspection of the scree plot. The adequacy of the data for factor analysis was confirmed through Kaiser–Meyer–Olkin (KMO) test and Bartlett's test of sphericity. Items were retained or removed based on established criteria: a minimum primary factor loading of ≥ .40, the absence of significant cross-loadings (< .20 difference between primary and secondary loadings), and conceptual coherence with the intended construct (Hinkin, 1995; 1998). Items not meeting these criteria were removed, and a

second EFA was conducted on the remaining items to refine the factor structure. Internal consistency was assessed using Cronbach's alpha for each dimension and for the total scale.

A similar procedure was used for the Privacy-Protective Behaviour Scale. An EFA was conducted on the 17 items to determine the underlying factor structure, again using principal axis factoring with oblimin rotation. The KMO value and Bartlett's test indicated that the data were suitable for factor analysis. Factor retention was guided by eigenvalues greater than 1 and visual inspection of the scree plot. Cronbach's alpha was calculated for each subscale and the full scale to assess reliability.

To test H1 a multiple linear regression analysis was conducted. The overall protective behaviour score was entered as the dependent variable, and the four refined privacy concern dimensions (manufacturer, government, household, cybersecurity) were entered as predictors. In addition, separate regression models were computed for each type of protective behaviour to examine differential predictive effects.

To test H2 and H3 two multiple linear regression analyses were conducted. In both models, ownership status and gender were entered simultaneously as predictors. The first model examined their effect on the overall privacy concerns score, while the second model tested their effect on the overall privacy-protective behaviour score. These scores were computed by averaging all items from the subscales. This composite score was used in the regression analyses.

In addition, exploratory follow-up regressions were conducted to assess whether ownership and gender had differential effects across specific subscales of privacy concerns (manufacturer, government, household, cybersecurity) and types of privacy-protective behaviours (physical, settings-based, behavioural). Participants identifying as another gender (n = 3) were excluded from gender-based comparisons due to insufficient sample size. Assumptions for linear regression analyses (normality, homoscedasticity, linearity, and absence of multicollinearity) were checked and met for all models.

Results

Factor Structure

To examine the underlying structure of perceived privacy concerns an exploratory factor analysis (EFA) was conducted on all 25 items of the initial scale. The analysis used principal axis factoring with oblimin rotation, based on theoretical expectations that the dimensions of perceived privacy concerns would be correlated. The Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy was excellent ($KMO = .90$), and Bartlett's test of sphericity was significant, $\chi^2(300) = 2231.69$, $p < .001$, indicating that the data were suitable for factor analysis.

A five-factor solution was extracted to reflect the original theoretical framework, which included manufacturer privacy concerns, government surveillance concerns, household privacy concerns, third-party data access concerns, and cybersecurity concerns. The initial factor solution broadly followed this structure, with many items loading on their intended dimensions. However, as discussed in the following section, several issues emerged that motivated a refinement of the scale and a second EFA on a reduced item set. The factor loadings and communalities from the initial 25-item EFA are presented in Table 5.

Table 5

Exploratory Factor Analysis of the Initial 25-Item Privacy Concern Scale

Item		1	2	3	4	5	Communality
	I am concerned that…						
1	…I have no control over what happens with my data once it's collected by the company.	.74					.70
2	… people working at the manufacturer could access my personal data.		.44				.50
3	… smart speaker companies know too much about me through the data they collect.	.33					.60
4	… my data might be used by smart speaker manufacturers for purposes I'm not aware of.	.55					.54
5	… smart speaker companies may share my data without my consent.	.83					.77
6	… laws do not sufficiently protect my smart speaker data from government access.		.70				.49
7	… smart speaker technology increases the risk of government surveillance.		.81				.75
8	… government agencies could access data collected by my smart speaker.		.82				.72
9	… my conversations at home could be used by government agencies.		.88				.81
10	… government agencies might not respect my privacy when it comes to data collected by my smart speaker.		.91				.75
11	… smart speakers could accidentally reveal private information to other household members during use.			.78			.69
12	… other household members might access my personal information through the smart speaker.			.90			.77
13	… the smart speaker records conversations I don't want others in my household to hear.			.72			.59
14	… the smart speaker can be used to monitor my activities at home by people I live with.			.79			.62
15	… others in my household could use the smart speaker to impersonate me or access features intended only for me.			.70			.53
16	… third parties could gain access to my smart speaker data.	.36			.37		.68
17	… third parties may use data from my smart speaker for advertising purposes.				.80		.76
18	… my smart speaker data could be sold to unknown companies without my knowledge.	.41			.55		.80
19	… my smart speaker data could be shared with other companies for purposes I did not agree to.	.57			.38		.77
20	… companies use vague policies to justify sharing my smart speaker data with third parties.	.65					.67
21	… my smart speaker could be hacked.					.67	.52
22	… storing my smart speaker data in the cloud increases the risk of being hacked.					.52	.49
23	… technical vulnerabilities in my smart speaker could compromise my privacy.					.58	.60
24	… my smart speaker may not receive important security updates to protect it from new threats.					.33	.26
25	… my smart speaker does not have strong security measures in place.	.37				.47	.56

Note. Factor loadings < .30 are suppressed.

The results of the initial exploratory factor analysis (EFA) provided partial support for the hypothesized five-factor structure. Several items loaded clearly on their intended factors with sufficient strength (≥ .40), supporting the theoretical dimensions of manufacturer privacy, government surveillance, household privacy, and cybersecurity concerns. However, closer inspection revealed several issues requiring item removal and reassignment. The criteria for item retention and removal were guided by established recommendations (Hinkin,1995; Hinkin 1998), which suggest that acceptable primary factor loadings should exceed .40 and that items with cross-loadings closer than .20 between primary and alternative factors may indicate conceptual ambiguity.

Item 2 was removed because it loaded more strongly on a factor different from its theoretical assignment, violating conceptual coherence. While the other manufacturer items focus on the company as an institution, this item emphasizes individual employees, introducing a different level of analysis. Items 3 and 24 were excluded due to weak primary loadings below the .40 threshold, indicating limited alignment with any latent construct. Items 16, 18, and 25 were removed due to problematic cross-loadings: while their primary loadings were marginally acceptable or near-threshold (e.g., Item 18 = .41), the difference between their primary and secondary loadings fell below the recommended .20, suggesting insufficient discriminant validity.

Most critically, the third-party privacy concern dimension failed to form a cohesive factor. Although one item (Item 17) loaded strongly on its intended factor (.80), the other items in this dimension (Items 16, 18, 19, and 20) failed to meet the required statistical and conceptual criteria. Given that a latent factor should be represented by at least three reliable and conceptually coherent items, the third-party dimension was considered empirically and theoretically too weak to retain (Alhija, 2010; Howard, 2015). Despite its statistical strength, Item 17 was removed due to being the only item. However, Items 19 and 20, which had inadequate loadings within the third-party dimension, exhibited stronger secondary loadings on the manufacturer privacy factor. Conceptually, these items address the way companies handle data sharing and communication about such practices, concerns that users typically associate with the manufacturer's data policies and trustworthiness. Therefore, based on both their statistical pattern and theoretical alignment, these items were reassigned to the manufacturer privacy concern dimension.

In total, seven items were removed from the original pool, resulting in a refined 18-item scale. The revised factor structure was subsequently re-evaluated through a second EFA to assess whether these refinements improved the scale's clarity, internal consistency, and

construct validity. The Kaiser–Meyer–Olkin (KMO) measure remained excellent (*KMO* = .89), and Bartlett's test of sphericity was again significant, $\chi^2(153) = 1495.1$, $p < .001$, confirming the suitability of the data for factor analysis. Based on eigenvalues greater than 1 and visual inspection of the scree plot, four factors were retained, explaining 60% of the total variance. The factor loadings and communalities for the refined scale are presented in Table 6.

Table 6

Exploratory Factor Analysis of the Refined 18-Item Privacy Concern Scale

Item		1	2	3	4	Communality
	I am concerned that…					
1	… I have no control over what happens with my data once it's collected by the company.	.85				.73
4	… my data might be used by smart speaker manufacturers for purposes I'm not aware of.	.63				.51
5	… smart speaker companies may share my data without my consent.	.78				.70
19	… my smart speaker data could be shared with other companies for purposes I did not agree to.	.84				.71
20	… companies use vague policies to justify sharing my smart speaker data with third parties.	.84				.71
6	… laws do not sufficiently protect my smart speaker data from government access.		.64			.52
7	… smart speaker technology increases the risk of government surveillance.		.80			.75
8	… government agencies could access data collected by my smart speaker.		.79			.72
9	… my conversations at home could be used by government agencies.		.92			.82
10	… government agencies might not respect my privacy when it comes to data collected by my smart speaker.		.89			.74
11	… smart speakers could accidentally reveal private information to other household members during use.			.77		.66
12	… other household members might access my personal information through the smart speaker.			.92		.79
13	… the smart speaker records conversations I don't want others in my household to hear.			.70		.57
14	… the smart speaker can be used to monitor my activities at home by people I live with.			.78		.63
15	… others in my household could use the smart speaker to impersonate me or access features intended only for me.			.69		.53
21	… my smart speaker could be hacked.				.79	.65
22	… storing my smart speaker data in the cloud increases the risk of being hacked.				.55	.52
23	… technical vulnerabilities in my smart speaker could compromise my privacy.				.67	.59

Note. Factor loadings < .30 are suppressed.

The oblimin-rotated solution supported the presence of four distinct factors, aligning with the dimensions of manufacturer privacy concerns, government surveillance concerns, household privacy concerns, and cybersecurity concerns. All retained items loaded significantly on their respective factors (≥ .55), with no cross-loadings. Communalities ranged from .51 to .82, indicating that each item shared a sufficient proportion of variance with the extracted factors.

To assess the reliability of each factor Cronbach's alpha coefficients were computed (see Table 7). The overall privacy concerns score was calculated by averaging the four subscale scores. All four factors demonstrated good to excellent internal consistency, exceeding the commonly accepted threshold of $\alpha \geq .70$ (Nunnally, 1978).

Table 7

Internal Consistency (Cronbach's α), Means, Standard Deviations and Inter-Scale Correlations of the Perceived Privacy Concerns Dimensions

Dimension	Cronbach's α	*M*	*SD*	1	2	3	4
Overall Privacy Concerns Scale	.92	4.96	1.06				
Manufacturer Privacy Concerns	.90	5.80	1.18	1.00	.57	.31	.57
Government Surveillance Concerns	.92	5.06	1.46	.57	1.00	.40	.51
Household Privacy Concerns	.89	4.07	1.56	.31	.40	1.00	.39
Cybersecurity Concerns	.75	4.99	1.27	.57	.51	.39	1.00

In line with hypotheses 1, we found that two privacy concerns were positively correlated with privacy-protective behaviours, while two were not. A multiple linear regression was conducted with general privacy-protective behaviour as the dependent variable and the four privacy concern dimensions as predictors. The overall model was statistically significant, $F(4, 119) = 9.91$, $p < .001$, explaining approximately 25% of the variance in protective behaviour. Both household privacy concerns ($\beta = .28$, $p = .001$) and cybersecurity concerns ($\beta = .24$, $p = .041$) significantly predicted protective behaviour. In contrast, manufacturer and government concerns did not significantly contribute to the model ($p > .05$), suggesting that general protective behaviours are primarily driven by concerns about intra-household exposure and cybersecurity threats.

To further explore whether different types of protective strategies were differentially predicted by these concern dimensions, three additional regression models were computed for physical, settings-based, and behavioural protection. The physical protection model (e.g., unplugging or muting the device) was significant, $F(4, 119) = 6.33$, $p < .001$, but explained a

smaller portion of variance (Adjusted $R^2 = .15$). Only household privacy concerns emerged as a significant predictor ($\beta = .36$, $p = .002$).

The settings-based protection model (e.g., adjusting privacy settings) was also significant, $F(4, 119) = 9.81$, $p < .001$, with an Adjusted R^2 of .22. Here, both household concerns ($\beta = .23$, $p = .011$) and cybersecurity concerns ($\beta = .30$, $p = .021$) were significant predictors.

The behavioural protection model (e.g., avoiding sensitive conversations near the device) yielded a significant result as well, $F(4, 119) = 8.29$, $p < .001$, explaining 19% of the variance. In this case, household concerns ($\beta = .30$, $p = .004$) and government surveillance concerns ($\beta = .27$, $p = .031$) were significant predictors, while cybersecurity concerns showed a marginal effect ($\beta = .25$, $p = .078$). The results of all regression analyses are summarized in Table 8.

Table 8

Regression Analyses Predicting Types of Privacy-Protective Behaviour from Dimensions of Perceived Privacy Concerns

Dependent Variable	Predictor	*β*	*SE*	*t*	*p*
Overall Privacy-Protective Behaviours	Manufacturer Concerns	.00	.61	.03	.978
	Government Concerns	.12	.13	1.16	.249
	Household Concerns	.28	.08	3.35	.001**
	Cybersecurity Concerns	.24	.12	2.07	.041*
Physical Protection	Manufacturer Concerns	-.09	.17	-.52	.605
	Government Concerns	.14	.14	1.03	.307
	Household Concerns	.36	.11	3.22	.001**
	Cybersecurity Concerns	.22	.16	1.36	.177
Settings-Based Protection	Manufacturer Concerns	.19	.14	1.39	.169
	Government Concerns	.03	.11	.28	.784
	Household Concerns	.23	.09	2.59	.011*
	Cybersecurity Concerns	.30	.13	2.34	.021*
Behavioural Protection	Manufacturer Concerns	-.20	.16	-1.27	.205
	Government Concerns	.27	.12	2.18	.031*
	Household Concerns	.30	.10	2.91	.004**
	Cybersecurity Concerns	.25	.14	1.78	.078

Note. p < .05*, p < .01**, p < .001***

Hypotheses 2 and 3 examined the effects of ownership status (owners vs. non-owners) and gender (female vs. male) on perceived privacy concerns and privacy-protective behaviour. Two multiple regression analyses were conducted, with ownership and gender entered as predictors of (1) the overall privacy-protective behaviour score and (2) the overall privacy concerns score.

An overall privacy concerns score was calculated by averaging the items across the four retained dimensions (manufacturer, government, household, cybersecurity). For perceived privacy concerns, the overall model was significant, $F(2, 121) = 8.54$, $p < .001$, explaining 11% of the variance. Ownership was a significant predictor ($\beta = –.78$, $p < .001$), indicating that participants who own a smart speaker reported significantly lower privacy concerns than those imagining ownership. Gender did not significantly predict privacy concerns ($\beta = .11$, $p = .57$).

For privacy-protective behaviours, the regression model was also significant, $F(2, 118) = 68.95$, $p < .001$, accounting for 54% of the variance. Both predictors contributed significantly: ownership ($\beta = –2.18$, $p < .001$) and gender ($\beta = .39$, $p = .045$). Specifically, owners reported fewer protective behaviours than non-owners, and female participants engaged in significantly more protective behaviours than males.

These findings support H2a, H2b, and H3b, but not H3a. While ownership had a strong and consistent effect on both outcomes, gender differences were only evident in behavioural responses, not in perceived privacy concerns.

To examine whether the effects of ownership and gender differ across specific types of privacy concerns and behaviours, follow-up analyses were conducted using the individual subscales. Ownership significantly predicted all four privacy concern dimensions, with participants imagining ownership reporting higher concern levels than current owners. Gender, however, did not significantly affect any concern dimension. For protective behaviours, ownership again emerged as a consistent predictor across all three behavioural strategies. Participants imagining ownership engaged in significantly more protective actions across all subtypes. Gender significantly predicted physical and behavioural protection, with women reporting greater engagement in these behaviours. Detailed regression coefficients, standard errors, and significance levels are reported in Table 9.

Table 9

Regression Analyses Predicting Privacy Concern Dimensions and Protective Behaviours from Ownership and Gender

Dependent Variable	Predictor	*β*	*SE*	*t*	*p*
Overall Privacy Concerns	Ownership	-.78	.20	-3.81	<.001***
	Gender	.11	.19	.57	.568
Overall Protective-Behaviours	Ownership	-2.18	.21	-10.63	<.001***
	Gender	.39	.19	2.03	.044*
Manufacturer Concerns	Ownership	-.50	.24	-2.09	.039*
	Gender	-.06	.22	-.29	.773
Government Concerns	Ownership	-.93	.29	-3.20	.002**
	Gender	.02	.27	.08	.939
Household Concerns	Ownership	-1.11	.30	-3.69	<.001***
	Gender	.35	.28	1.29	.201
Cybersecurity Concerns	Ownership	-.60	.26	-2.33	.021*
	Gender	.05	.24	.22	.828
Physical Protection	Ownership	-2.57	.28	-9.34	<.001***
	Gender	.77	.26	3.02	.003**
Settings-Based Protection	Ownership	-2.32	.25	-9.47	<.001***
	Gender	-.15	.23	-.67	.507
Behavioural Protection	Ownership	-1.86	.29	-6.5	<.001***
	Gender	-.90	.27	3.4	<.001***

Note. p < .05*, p < .01**, p < .001***

Discussion

The primary aim of this study was to develop and empirically examine a new scale to measure perceived privacy concerns in the context of smart home Internet of Things (IoT) technologies, with a particular focus on cloud-based smart speakers. While prior work, such as Lutz and Newlands (2021), has explored both perceived risks and behavioural responses, their framework was not empirically validated through factor analysis.

A secondary aim was to evaluate the predictive and discriminant validity of the newly developed scale by examining the structure of privacy-protective behaviours and assessing group differences in both perceived concerns and behavioural responses. Specifically, we investigated whether ownership status (owners vs. non-owners) and gender influence the degree to which individuals perceive concerns and engage in protective actions. While the development of the Perceived Privacy Concerns Scale represents the main theoretical and methodological contribution, these additional analyses provide insight into how well the scale captures theoretically expected patterns of behaviour and perception.

Evaluation of Perceived Privacy Concerns Scale

The exploratory factor analysis (EFA) of the developed Perceived Privacy Concerns Scale revealed a four-factor solution, representing concerns related to Companies, Governments, Household members, and Cybersecurity threats. This structure partially aligns with the five-dimensional model introduced by Lutz and Newlands (2021), who validated privacy-protective behaviours across these domains, including a fifth dimension: third-party actors (e.g., advertisers or data brokers).

In contrast, a distinct third-party factor did not emerge in the present study. While one item targeting third-party concerns demonstrated meaningful loadings, other items showed weak factor loadings and higher cross-loadings with the manufacturer-related factor. This may suggest that participants do not clearly distinguish between third-party and manufacturer risks, possibly because they perceive the manufacturer as the entity that enables or controls third-party access. In this sense, concerns about third-party actors may be conceptually embedded within broader company-related worries. Alternatively, the wording of these items (specifically Items 19 and 20) may not have adequately isolated the conceptual boundaries of third-party concerns, contributing to the overlap in interpretation.

These findings indicate that while the overall multidimensionality of perceived privacy concerns can be empirically captured, further refinement of the item pool is necessary, particularly for capturing third-party concerns.

Evaluation of Privacy-Protective Behaviour Scale

In addition to developing the privacy concern scale, we explored the structure of privacy-protective behaviours using an adapted version of the scale introduced by Pottkamp (2024), which was originally based on Lutz and Newlands (2021). The scale encompassed three types of actions users take to protect their privacy: physical actions (e.g., unplugging the device), settings-based adjustments (e.g., changing privacy settings), and behavioural adaptations (e.g., avoiding sensitive conversations near the device).

An exploratory factor analysis supported this three-factor structure, aligning with the original conceptualization by Lutz and Newlands (2021). This finding strengthens the theoretical and empirical basis for categorizing privacy-protective behaviours into distinct yet complementary strategies.

Moreover, our version included three new items that expanded the behavioural dimension, particularly aiming to capture concerns related to household dynamics. Together, these results indicate that users adopt a variety of distinct strategies to safeguard their privacy, and these strategies can be meaningfully classified across multiple dimensions.

Relationship Between Privacy Concerns and Protective Behaviours

The study also found a positive association between perceived privacy concerns and privacy-protective behaviours (H1), supporting predictive validity of the Perceived Privacy Concerns Scale. Analysis revealed that two privacy concern dimensions in particular, namely household and cybersecurity concerns were significant predictors of increased protective behaviours. Follow-up analyses using the subscales of privacy-protective behaviours further clarified these relationships. Household concerns were the only dimension that significantly predicted all three types of protective behaviours (physical, settings-based, and behavioural). This may reflect the particularly salient and immediate nature of interpersonal privacy risks in domestic environments. Prior work suggests that individuals tend to be especially vigilant when their personal space or relationships are involved, likely due to stronger emotional associations and a greater sense of control or accountability within the home (Petronio et al., 2021). For instance, the idea that a family member, child, or roommate could overhear or misuse information may elicit concrete and proactive responses because these risks are easier to imagine and directly influence.

In addition, cybersecurity concerns, such as fear of being hacked or unauthorized access primarily predicted settings-based protections (e.g., disabling features, managing permissions). This aligns with the technical nature of cybersecurity threats and the belief that such risks can be mitigated through specific system-level adjustments. Previous studies have

shown that users who are aware of digital threats often resort to settings-based behaviours as they are perceived to be more effective and within user control (Moustafa et al., 2021; Zwilling et al., 2020).

Interestingly, concerns about government surveillance only predicted behavioural strategies, such as avoiding sensitive speech near the device, while manufacturer-related concerns did not significantly predict any protective behaviours. One possible explanation is that concerns about institutional actors such as companies or governments feel psychologically distant or less actionable for many users. This phenomenon has been described in the literature as the "privacy paradox," where people express high levels of concern about their privacy but do not take corresponding actions to protect it, possibly due to a lack of perceived control or low efficacy of personal actions (Kokolakis, 2015).

These findings reinforce the importance of conceptualizing privacy concerns as multidimensional, as different types of concerns appear to motivate different levels or types of behavioural responses. They also highlight the potential need for more targeted educational and design interventions, in which users may need clearer guidance on how to protect themselves from risks like government surveillance.

Evaluation of Group Differences

Perceived privacy concerns and privacy-protective behaviours varied across user characteristics. The results revealed that smart speaker owners reported significantly lower levels of perceived privacy concerns compared to non-owners across all four dimensions. This trend may reflect a habituation or familiarity effect, wherein continued use of the device reduces perceived risk due to increased comfort or the illusion of control (Wairimu et al., 2018). These findings align with prior studies which show that owners often downplay risks in favour of convenience, rarely review or delete stored data, and tend to rely on basic settings adjustments while ignoring deeper vulnerabilities (Malkin et al., 2019; Zheng et al., 2018; Williams et al., 2018). Alternatively, this pattern could also reflect a selection effect, whereby individuals with lower baseline privacy concerns are more likely to adopt smart speakers in the first place.

In line with these findings, smart speaker owners also reported engaging less frequently in privacy-protective behaviours, particularly in the physical and settings-based categories. This further reinforces the notion that prolonged use may foster a diminished sense of risk or urgency, whether due to habituation, a perception of having already taken sufficient precautions, or increased comfort with the technology over time. Additionally, it is possible that non-owners overestimate the extent to which they would take protective actions, as their

responses reflect hypothetical intentions rather than real-world behaviours. Conversely, once people begin using a smart speaker, they may find that certain protective behaviours are too inconvenient or easy to forget, which may reduce how often they actually engage in them.

Gender differences were more nuanced. While females did not report higher levels of privacy concern, they reported slightly more engagement in protective behaviours, particularly behavioural strategies (e.g., avoiding sensitive speech near the device). The results suggest that gender differences in the smart home context are more nuanced, varying by the type of protective response.

Theoretical Contributions and Practical Implications

This study makes several contributions to the growing body of research on privacy in smart home environments. First and foremost, it introduces a newly developed scale for assessing perceived privacy concerns specific to smart home IoT devices, with a focus on smart speakers. Unlike prior tools that measured general attitudes or privacy behaviours, this scale is tailored to capture user-specific concerns across four empirically supported dimensions namely, Manufacturer, Government, Household, and Cybersecurity. Theoretically, these findings reinforce the notion that privacy is not a one-dimensional construct. Specifically, users assess privacy concerns through multiple relational lenses, ranging from institutional and governmental actors to interpersonal dynamics within shared households. This distinction has often been underexplored in prior studies that relied on single-item measures or conceptualized privacy as a general concern (Al-Husamiyah & Al-Bashayreh, 2021; Fantinato et al., 2018; Kowalczuk, 2018; Sanguinetti et al., 2018; Shuhaiber & Mashal, 2019; Yang et al., 2018). The multidimensional scale developed in this study thus offers a preliminary step toward a more refined understanding of privacy concern perception and lays the groundwork for future research.

Practically, the scale can serve as a diagnostic tool for researchers, policymakers, and developers seeking to assess and address user concerns. It enables more targeted investigations into which types of risks are most salient to different user groups and offers a basis for evaluating the effectiveness of privacy interventions or policy changes. For instance, if users report high manufacturer risk concerns, manufacturers might prioritize greater transparency around data handling and implement clearer consent mechanisms.

Moreover, the scale can also be used in longitudinal research to track how privacy concerns shift as smart home technologies become more integrated into everyday life or as new regulatory frameworks are introduced. This offers a foundation for understanding the evolving landscape of privacy perceptions in relation to technological and societal change.

Limitations

While this study offers valuable insights and introduces a promising measurement tool, several limitations should be considered when interpreting the results. One of the most prominent limitations concerns the sample size. Although the exploratory factor analysis (EFA) revealed a clear four-factor structure a confirmatory factor analysis (CFA) is needed to validate this structure more robustly (Boateng et al., 2018). Conducting a CFA requires a substantially larger sample typically at least 200 participants which was not feasible in the current study (Myers et al., 2011; Krejcie & Morgan, 1970). In addition, the number of smart speaker owners in the sample (N = 37) was relatively small, limiting the statistical power of the ownership-based comparisons. Findings from these analyses should therefore be interpreted with caution and verified in larger and more diverse samples.

Another limitation relates to the measurement approach used for participants who did not own a smart speaker. These individuals were asked to imagine receiving a smart speaker as a gift and to report their intended privacy behaviours. While this allowed for a structured comparison between owners and non-owners, imagined behaviour may not fully reflect real-world tendencies, thereby potentially affecting the validity of responses in the non-owner group.

The design of the survey itself may also have introduced some limitations. The overall length and use of forced-response formats could have contributed to participant fatigue, particularly in the later sections. Although attention checks were included to assess engagement, dropout patterns suggest that some participants may have disengaged, which could have implications for data quality.

Furthermore, while this study focused on smart speakers as representative smart home devices, the findings may not generalize to other Internet of Things (IoT) technologies, such as smart cameras, thermostats, or smart TVs. These devices may raise different privacy concerns and elicit different protective strategies. However, the conceptual framework and structure of the developed scale could be adapted to other device types with appropriate modifications to item content.

An additional limitation concerns the language of the survey. Although most participants were native German speakers, the questionnaire was administered in English. While participants had sufficient language proficiency to complete the survey, subtle misunderstandings in wording or phrasing may have affected the interpretation of some items. Future research could employ translated versions of the scale to ensure linguistic and cultural clarity.

Finally, the sample was not fully representative. While participants came from various national backgrounds, the majority were based in Germany and the Netherlands contexts that both fall within what is commonly referred to as WEIRD (Western, Educated, Industrialized, Rich, and Democratic) societies (Wooliscroft & Ko, 2023). Since privacy perceptions are shaped by cultural norms, regulatory environments, and societal attitudes toward technology, the findings may not generalize to non-WEIRD populations. Replication in different cultural contexts is needed to assess the broader applicability of the scale.

Future Research

Building upon the contributions and limitations of the present study, several directions for future research are proposed. First and foremost, to formally validate the four-factor structure identified in the exploratory factor analysis, a confirmatory factor analysis (CFA) is essential. This would provide a more robust test of the scale's structural validity and reliability. Following methodological recommendations future studies should employ larger and more diverse samples to allow for such advanced statistical analyses.

A particular area that warrants further attention is the development of a distinct third-party concern dimension. Future research should aim to develop and pretest new items that more clearly differentiate third-party data recipients, such as advertisers or analytics firms, from manufacturers and service providers.

Additionally, future research should examine the predictive validity of the scale in relation to smart speaker adoption, specifically whether perceived privacy concerns can reliably predict decisions related to the adoption of smart home technologies. This would enhance the practical utility of the scale in both academic and applied settings. Future research should also further assess other aspects of scale validity, such as discriminant validity, in larger and more diverse samples.

To further establish the generalizability of the instrument, the scale should be tested in diverse cultural contexts and across various smart home technologies beyond smart speakers, such as smart cameras, thermostats, or wearable devices. Since privacy norms and perceptions are shaped by cultural values and the technological environment, such studies would help determine the scale's adaptability across domains.

Finally, longitudinal research designs could provide valuable insights into how privacy concerns develop and change over time, particularly in response to external factors such as data breaches, regulatory changes, or evolving public discourse around digital surveillance. Understanding these dynamics would contribute to a more nuanced view of user trust and adaptation in smart environments.

In addition to these future directions, the findings also suggest avenues for improving privacy practices in current smart home technologies. Since smart speaker owners expressed lower privacy concerns and engaged less in protective behaviours, particularly in physical and settings-based strategies, developers should consider designing default settings that maximize privacy without requiring extensive user input. Privacy tools that emphasize usability, such as pre-configured privacy modes, in-device reminders, or simplified controls, may help bridge the gap between user intentions and actual behaviour. Moreover, the scale's multidimensional structure points to the need for targeted communication strategies: developers and policymakers should address specific areas of concern (e.g., manufacturer, governmental, or interpersonal concerns) rather than treating privacy as a singular, uniform issue. These strategies may help users make more informed and confident decisions regarding their privacy.

Conclusion

This study introduced and validated a multidimensional scale to measure perceived privacy concerns in the context of smart home IoT devices, particularly smart speakers. The developed scale fills a gap in the existing literature by providing an empirically validated instrument that captures the multifaceted nature of perceived privacy concerns, distinguishing between risks associated with manufacturers, government surveillance, household dynamics and cybersecurity. Beyond establishing the scale's internal structure, additional analyses supported its predictive and discriminant validity. Perceived privacy concerns were shown to positively correlate with privacy-protective behaviours, and significant group differences were observed based on ownership status and gender. These findings offer a more nuanced understanding of how users experience and manage privacy risks in increasingly data-driven home environments and lay the groundwork for future research into the behavioural implications of privacy perception.

References

Alhija, F. (2010). Factor analysis: an overview and some contemporary advances. In *Elsevier eBooks* (pp. 162–170). https://doi.org/10.1016/b978-0-08-044894-7.01328-2

Al-Husamiyah, A., & Al-Bashayreh, M. (2021). A comprehensive acceptance model for smart home services. *International Journal of Data and Network Science*, *6*(1), 45–58. https://doi.org/10.5267/j.ijdns.2021.10.005

Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, *27*(6), 2233–2242. https://doi.org/10.1016/j.chb.2011.07.002

Berte, D. (2018). Defining the IoT. *Proceedings of the . . . International Conference on Business Excellence*, *12*(1), 118–128. https://doi.org/10.2478/picbe-2018-0013

Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quiñonez, H. R., & Young, S. L. (2018). Best Practices for developing and Validating scales for health, Social, and Behavioral Research: A primer. *Frontiers in Public Health*, *6*. https://doi.org/10.3389/fpubh.2018.00149

Bujang, M. A., Ghani, P. A., Soelar, S. A., & Zulkifli, N. A. (2012). Sample size guideline for exploratory factor analysis when using small sample: Taking into considerations of different measurement scales. *IEEE*, 1–5. https://doi.org/10.1109/icssbe.2012.6396605

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Open Access*, 1–12. https://doi.org/10.1145/3290605.3300764

Fantinato, M., Hung, P. C., Jiang, Y., Roa, J., Villarreal, P., Melaisi, M., & Amancio, F. (2018). A preliminary study of Hello Barbie in Brazil and Argentina. *Sustainable Cities and Society*, *40*, 83–90. https://doi.org/10.1016/j.scs.2018.03.006

Gaspar, C., Neus, A., Nuremberg Institute for Market Decisions e.V., & Founder and Anchor Shareholder of GfK SE. (2023). *SMART SPEAKER REPORT 2023: THE EXPERIENCES, ASSESSMENTS AND DESIRES OF USERS IN GERMANY, THE UK AND THE U.S.* https://www.nim.org/fileadmin/PUBLIC/3_NIM_Publikationen/NIM-Studien/NIM-Studien_EN/2023_Smart_Speaker_Report_0602_Eng_fin.pdf

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*, *2*(2). https://doi.org/10.1007/s42452-020-2025-8

Haug, M., Rössler, P., & Gewald, H. (2020). How users perceive privacy and security risks concerning smart speakers. *European Conference on Information Systems*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1128&context=ecis2020_rp

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management*, *21*(5), 967–988. https://doi.org/10.1177/014920639502100509

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods*, *1*(1), 104–121. https://doi.org/10.1177/109442819800100106

Howard, M. C. (2015). A review of exploratory factor analysis decisions and overview of current practices: what we are doing and how can we improve? *International Journal of Human-Computer Interaction*, *32*(1), 51–62. https://doi.org/10.1080/10447318.2015.1087664

Huang, Y., Obada-Obieh, B., & Beznosov, K. (2020). Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. *ACM*, 1–13. https://doi.org/10.1145/3313831.3376529

Huijts, N. M. A., & Haans, A. (2024). Values as causes of emotions and acceptability in the digital risk context: an extension of the values scale with privacy. *Journal of Risk Research*, 1–26. https://doi.org/10.1080/13669877.2024.2423203

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kline, P. (2014). An easy guide to factor analysis. In *Routledge eBooks*. https://doi.org/10.4324/9781315788135

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

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

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, *30*(3), 607–610. https://doi.org/10.1177/001316447003000308

Lau, J., Zimmerman, B., & 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

Lee, H., & Kobsa, A. (2016). Understanding user privacy in Internet of Things environments. *IEEE*, 407–412. https://doi.org/10.1109/wf-iot.2016.7845392

Lenhart, A., Park, S., Zimmer, M., & Vitak, J. (2023). "You shouldn't need to share your data": Perceived privacy Risks and Mitigation Strategies among Privacy-Conscious Smart Home Power Users. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2), 1–34. https://doi.org/10.1145/3610038

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

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.561011

Myers, N. D., Ahn, S., & Jin, Y. (2011). Sample size and power estimates for a confirmatory factor analytic model in exercise and sport. *Research Quarterly for Exercise and Sport*, *82*(3), 412–423. https://doi.org/10.1080/02701367.2011.10599773

Petronio, S., Child, J. T., & Hall, R. D. (2021). Communication Privacy Management Theory. In *Routledge eBooks* (pp. 314–327). https://doi.org/10.4324/9781003195511-28

Purington, A., Taft, J. G., Sannon, S., Bazarova, N. N., & Taylor, S. H. (2017, May). " Alexa is my new BFF" social roles, user satisfaction, and personification of the Amazon Echo. In *Proceedings of the 2017 CHI conference extended abstracts on human factors in computing systems* (pp. 2853-2859). https://doi.org/10.1145/3027063.3053246

Sanguinetti, A., Karlin, B., & Ford, R. (2018). Understanding the path to smart home adoption: Segmenting and describing consumers across the innovation-decision process. *Energy Research & Social Science*, *46*, 274–283. https://doi.org/10.1016/j.erss.2018.08.002

Schomakers, E., Biermann, H., & Ziefle, M. (2021). Users' preferences for smart home automation – Investigating aspects of privacy and trust. *Telematics and Informatics*, *64*, 101689. https://doi.org/10.1016/j.tele.2021.101689

Shuhaiber, A., Alkarbi, W., & Almansoori, S. (2023). Trust in smart Homes: the power of social influences and perceived risks. In *Lecture notes in networks and systems* (pp. 305–315). https://doi.org/10.1007/978-981-19-7660-5_27

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in Society*, *58*, 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

Stevic, A., Schmuck, D., Koemets, A., Hirsch, M., Karsay, K., Thomas, M. F., & Matthes, J. (2021). Privacy concerns can stress you out: Investigating the reciprocal relationship between mobile social media privacy concerns and perceived stress. *Communications*, *47*(3), 327–349. https://doi.org/10.1515/commun-2020-0037

Tifferet, S. (2018). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, *93*, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Wairimu, J., Ayaburi, E., & Andoh-Baidoo, F. (2018). Individual™s Security and Privacy Behavior on the Use of Unfamiliar Wireless Networks: Habituation Theory Perspective. *ICIS 2018 Proceedings*. 12. https://aisel.aisnet.org/icis2018/security/Presentations/12

Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. *IEEE*, 181–18109. https://doi.org/10.1109/pst.2017.00029

Wooliscroft, B., & Ko, E. (2023). WEIRD is not Enough: Sustainability Insights from Non-WEIRD Countries. *Journal of Macromarketing*, *43*(2), 171–174. https://doi.org/10.1177/02761467231169880

Yang, H., Lee, W., & Lee, H. (2018). IoT smart home adoption: The importance of proper level automation. *Journal of Sensors*, *2018*, 1–11. https://doi.org/10.1155/2018/6464036

Zeng, E., Mare, S., & Roesner, F. (2017). End User Security and Privacy Concerns with Smart Homes. *Symposium on Usable Privacy and Security*, 65–80. https://atc.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf

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

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Appendix A

During the preparation of this work the author (Sanae Akchich) used ChatGPT in order to brainstorm, clarify concepts, plan tasks, receive feedback on the structure, and improve clarity of writing. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.

Appendix B

Sociodemographic Characteristics of Participants (N=127)

Variable	Category	*n*	%
Gender	Female	52	40.9
	Male	72	56.7
	Other	3	2.4
Nationality	German	79	62.2
	Dutch	14	11
	American	8	6.3
	Turkish	4	3.1
	Other	22	17.3
Highest Education Level	High School	45	35.3
	Bachelor	58	45.7
	Master	20	15.8
	PhD	4	3.2
Student	Yes	61	52
	No	66	48
Smart Speaker Ownership	Yes	37	29.1
	No	90	70.9
Knowledge about Smart Speakers	Nothing	40	31.5
	A little	48	37.8
	A moderate amount	23	18.1
	Much	2	1.6
	Very much	14	11

Note. Percentages may not sum to 100 due to rounding.

Appendix C

Informed Consent

Project Title: Developing and Testing a Multidimensional Scale for Perceived Privacy Concerns of Smart Speakers

Researchers: Sanae Akchich (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 how individuals perceive privacy risks associated with smart home devices, with a particular focus on smart speakers. While smart speakers are used as a reference throughout the study, the aim is to create a generalizable scale for smart home IoT privacy concerns. This study aims to advance our understanding of privacy perceptions about smart speakers. You are being asked to participate in this study because you found this survey online or were asked to participate by one of the researchers or data collectors and because we are interested in these processes in a wide variety of people. We are seeking individuals who are at least 18 years old. If you are under 18, please do not participate.

Procedure:

If you agree to participate, you will begin by answering several demographic questions (e.g., age, gender, nationality, and education). You will then be introduced to the concept of smart speakers and asked to respond to a series of questions concerning your perceptions of privacy risks related to smart speakers. Additionally, the survey includes questions measuring privacy-protective behaviours. Finally, you will be provided with more information about the study and relevant contact details. Your participation will take approximately 7–10 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.

Anonymity & 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.

Questions:

For further information about this study, you may contact:

Sanae Akchich: s.akchich@student.utwente.nl

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

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

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

O I agree and consent to participating in this study and confirm that I am over 18 years old

O No, I do not agree to participating in this study

Demographics

1. What is your age? _____
2. What is your gender?
[ ] Female
[ ] Male
[ ] Other
[ ] Prefer not to say
3. What is your nationality?
[ ] German
[ ] Dutch
[ ] Other _____
4. What is your highest level of education?
[ ] Primary education
[ ] Highschool
[ ] Bachelor
[ ] Master
[ ] PhD
5. Are you a student?
[ ] Yes
[ ] No
6. Which living arrangement describes your situation the best:
[ ] Living alone
[ ] Living with partner
[ ] Living with family (e.g. parents, grandparents, etc.)
[ ] Living with friends
[ ] Living with others who I would no classify as partner, family or friend (such as living with other students, or in co-housing)

Survey Introduction

In the next part of the survey, you will be asked about your thoughts and perceptions regarding smart home devices — specifically smart speakers.
Examples of smart speakers include Amazon Echo, Google Home, and Apple HomePod. These devices typically include a built-in voice assistant (e.g., Alexa, Google Assistant or Siri), can respond to voice commands, and are often connected to other smart home devices.
Below this section you can find an example of a smart speaker.

(https://www.saga.co.uk/magazine/life/what-is-a-smart-speaker)

7. How much do you know about smart speakers?

[ ] Nothing
[ ] A little
[ ] A moderate amount
[ ] Much
[ ] Very much

8. Do you currently own or use a smart speaker (e.g., Amazon Echo, Google Home, Apple HomePod)?

[ ] Yes

If yes, follow up: Which of the following best describes your relationship with the smart speaker?

[ ] Primary user – I installed the device and manage its settings myself
[ ] Secondary user – I live in a household where a smart speaker is installed, but I didn't set it up

[ ] No

If no, follow up:

For the remainder of this survey, please imagine that you've recently received a smart speaker as a gift from a friend or family member. You have now set it up and started using it in your home.

Please indicate how much you agree or disagree with the following statements using the scale below:

1 = Strongly disagree 2 = Disagree 3 = Somewhat disagree 4 = Neither agree nor disagree 5 = Somewhat agree 6 = Agree 7 = Strongly agree

1. Dimension: Manufacturer Privacy Concerns

I am concerned that I have no control over what happens with my data once it's collected by the company.
I am concerned that people working at the manufacturer could access my personal data.
I am concerned that smart speaker companies know too much about me through the data they collect.

I am concerned that my data might be used by smart speaker manufacturers for purposes I'm not aware of.

I am concerned that smart speaker companies may share my data without my consent.

2. Dimension: Government Surveillance Concerns

I am concerned that laws do not sufficiently protect my smart speaker data from government access.

I am concerned that smart speaker technology increases the risk of government surveillance.

I am concerned that government agencies could access data collected by my smart speaker.

I am concerned that my conversations at home could be used by government agencies.

I am concerned that government agencies might not respect my privacy when it comes to data collected by my smart speaker.

3. Dimension: Household Privacy Concerns

Note: If you live alone, please imagine for this set of questions that you have a long term guest staying with you.

I am concerned that smart speakers could accidentally reveal private information to other household members during use.

I am concerned that other household members might access my personal information through the smart speaker.

I am concerned that the smart speaker records conversations I don't want others in my household to hear.

I am concerned that the smart speaker can be used to monitor my activities at home by people I live with.

I am concerned that others in my household could use the smart speaker to impersonate me or access features intended only for me.

4. Dimension: Third-Party Data Access Concerns

Note: By "third parties," we mean external companies or organizations that are not the manufacturer of the device but may receive user data for purposes such as advertising, analytics, or service delivery. Examples include marketing agencies, software vendors, or data brokers.

I am concerned that third parties could gain access to my smart speaker data.

I am concerned that third parties may use data from my smart speaker for advertising purposes.

I am concerned that my smart speaker data could be sold to unknown companies without my knowledge.

I am concerned that my smart speaker data could be shared with other companies for purposes I did not agree to.

I am concerned that companies use vague policies to justify sharing my smart speaker data with third parties.

5. Dimension: Cybersecurity Concerns

I am concerned that my smart speaker could be hacked.

I am concerned that storing my smart speaker data in the cloud increases the risk of being hacked.

I am concerned that technical vulnerabilities in my smart speaker could compromise my privacy.

I am concerned that my smart speaker may not receive important security updates to protect it from new threats.

I am concerned that my smart speaker does not have strong security measures in place.

Privacy Protective Behaviours

Gifted: Please indicate how likely it is that you perform the following actions to protect your privacy when using smart speakers using the scale below:
1 = Extremely unlikely 2 = Very unlikely 3 = Unlikely 4 = Neither likely nor unlikely
5 = Likely 6 = Very likely 7 = 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 turn off the smart speaker when I am having sensitive or private conversations.
I will unplug the smart speaker when I am having sensitive or private conversations.
I will place my smart speaker where I typically don't have sensitive or private conversations.
I will avoid placing the smart speaker in shared spaces (e.g., living room) to reduce the chance that others in my household hear or access personal interactions.
I will mute the smart speakers microphone when I am not using it.
I will review and adjust the privacy settings of my smart speaker.
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 set up multiple user accounts or voice profiles on the smart speaker to manage what other household members can access.
I will speak very quietly around the smart speaker when I don't want to be recorded.
I will moderate my language around the smart speaker to avoid recording private matters.
I will avoid sensitive or private conversations around the smart speaker.
I will avoid giving voice commands to the smart speaker when other people in the household are around.

Owned: Please indicate how often in the **last 3 month** you engaged in the following actions to protect your privacy when using smart speakers using the scale below:
1 = Never 2 = Rarely 3 = Occasionally 4 = Sometimes 5 = Frequently 6 = Very often
7 = 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 turned off the smart speaker when I was having sensitive or private conversations.
I unplugged the smart speaker when I was having sensitive or private conversations.
I placed my smart speaker where I typically don't have sensitive or private conversations.
I avoided placing the smart speaker in shared spaces (e.g., the living room) to reduce the chance that others in the household could overhear private interactions.
I muted the smart speakers microphone when I was not using it.
I reviewed and adjusted the privacy settings of my smart speaker.
I reviewed which applications/services have access to my smart speaker.
To ensure you are paying attention, please select "Always" for this statement.
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 set up multiple user accounts or voice profiles on the smart speaker to control what others in the household can access.
I spoke very quietly around the smart speaker when I didn't want to be recorded.
I moderated my language around the smart speaker to avoid recording private matters.
I avoided sensitive or private conversations around the smart speaker.
I avoided using the smart speaker when other household members were around to protect my privacy.

Debriefing
Thank you for participating in this study.

If you have any questions or would like to receive a summary of the results once the study is complete, please feel free to contact the researcher at: **[s.akchich@student.utwente.nl]**