“Alexa, How Do You Protect My Privacy?” A Quantitative Study of User Preferences and Requirements about Smart Speaker Privacy Settings

Luca Hernández Acosta[1 [0000−0002−9696−3180]] and Delphine Reinhardt[1 [0000−0001−6802−2108]]

University of Göttingen, 37073 Göttingen, Germany

Abstract. Voice assistants are becoming increasingly popular. While users may benefit from the convenience of voice interactions, the use of voice assistants raises privacy issues. To address them, existing voice assistants propose some privacy settings. However, we are lacking knowledge about (1) which privacy settings are important to users, (2) what are their preferences about their application, and (3) what are their requirements beyond existing privacy settings. Gaining such knowledge is important to understand why users may not use these settings and to identify which settings should be introduced to allow users to better protect their privacy. To this end, we have conducted a quantitative online study with 1,103 German smart speaker owners. In addition to partly replicating findings obtained with different samples, the results show that the currently available privacy settings do not fully cover user requirements and indicate a general desire for more transparency and control over the collected data. Our results hence serve as basis for designing future privacy-preserving solutions.

Keywords: Smart speakers · Voice assistants · Privacy · Survey.

1 Introduction

The use of voice assistance has increased in recent years and is expected to grow in the future with the expansion of both smart homes and workplaces [13,9]. Its usage can, however, threaten users’ privacy according to different dimensions [14]. For example, user recordings processed and stored on servers controlled by manufacturers and third-party developers have already been unknowingly accessed and the resulting personal information sold or leaked [26,27]. Moreover, the analysis of the voice itself, such as tonal pitch, speech patterns, and intonation, can reveal sensitive information about the users, such as health issues [14,19]. To protect their privacy, manufacturers often provide privacy settings. Using them, users can, e.g., review and delete past interactions with the smart speaker as well as manage the access of third-party applications to their personal information (incl. e-mail, name, or place of residence [15]). Nevertheless, these settings are only accessible when users register their device with the

respective manufacturer. Most users, however, often do not know about those settings or perceive them as too complex [21,24]. As a result, they do not use them [21,24]. Furthermore, in multi-user environments, only the smart speaker owners (or people who installed the device) have full control and access to all privacy settings. In contrast, secondary users (i.e., family members or roommates) and tertiary users (i.e., visitors) do not have this control. They hence depend on the primary users to both respect their privacy by, e.g., not accessing stored data about them, as well as to protect their privacy against the device manufacturers [16]. While studies conducted in the US [21,24] and UK [1] show that existing solutions are either unused or unusable, we are missing knowledge about their validity in other cultures and with a representative sample. Privacy perceptions can, however, vary between cultures, often influenced by societal norms, individualistic or collectivistic values, and regional legal frameworks, impacting attitudes towards personal data sharing and control [22,32]. To bridge this gap, our contributions are as follows: We conducted a comprehensive survey of 1,103 German smart speaker owners, a study that extends beyond the usual focus on the US [21,24] and UK [1], thus exploring a different cultural context. We offer insights into (1) the differences in user profiles regarding privacy settings, (2) the relevance of existing privacy controls, (3) user preferences in their application usage, and (4) the demand for new privacy-preserving solutions. Our findings challenge the assumption of cultural differences in privacy perceptions and underline the universal importance of enhanced privacy controls among smart speaker users. Ultimately, this study indicates that current privacy settings on smart speakers do not fully meet user requirements, highlighting a significant desire among users for enhanced privacy controls and increased transparency in data handling.

Our manuscript is structured as follows: Sec. 2 presents related work. In Sec. 3, we elaborate on our methodology and sample in Sec. 4. Our findings are presented in Sec. 5 and discussed in Sec. 6. Finally, Sec. 7 concludes this paper.

2 Related Work

Several studies have explored privacy concerns and mental models of smart speaker users. As summarized in Tab. 1, Lau et al. interviewed both users and non-users to identify privacy concerns and found that current controls often do not meet users' needs [21]. Abdi et al. conducted interviews and a survey to investigate users' perceptions of smart speaker architectures and associated privacy risks [1,2]. Similarly, Kröger et al. investigated users' awareness of possible privacy-relevant inferences based on recordings [19], and Malkin et al. studied the attitudes and privacy behaviors of users using a browser extension in an online study [24]. Our study, while replicating some of these results, differs primarily in methodology, the German-based participant sample, and our focus on designing future privacy-preserving solutions, in contrast to studies primarily based in the US [21,24] and the UK [1].

Table 1. Comparison of Different Studies on Smart Speaker Privacy

Reference	Methodology	Participants	Differences from our study	Key findings
Lau et al. [21]	Diary study & interviews	34	US participants; privacy perceptions, behaviors	Privacy role in adoption, user interactions
Abdi et al. [1]	Interviews	17	UK participants; Security and privacy perceptions	Incomplete mental models, privacy coping strategies
Kröger et al. [19]	Online questionnaire	683	UK participants; focus on privacy awareness levels	Low awareness in voice data privacy, demographic variations (age, professional experience)
Malkin et al. [24]	Online questionnaire	116	US participants; beliefs on smart speaker recordings	Data retention unawareness, third-party concerns
Our Study	Online questionnaire	1,103	German participants; cultural differences, privacy control requirements	Need for enhanced privacy controls, transparency emphasis

In addition to the aforementioned studies we've incorporated individual solutions proposed and evaluated by users into our study to conduct a cross-analysis of these novel concepts, which haven't been implemented in existing smart speakers. In more details, Jin et al. have explored privacy behaviors in smart home environments and proposed some new privacy concepts evaluated in a speed-dating session [18]. Thakkar et al. have proposed privacy notices to inform users about data practices [30], and Ahmad et al. have designed physical and software-based controls to mute the assistant [4]. While studies in the broader field of smart homes have explored cultural and socio-economic privacy differences [6,5], this work specifically focuses on privacy issues in the context of smart speakers. Our study thus relies on existing works but explores further dimensions incl. another culture and comparing existing, proposed, and future solutions.

3 Methodology

3.1 Study Design

Our questionnaire (available here) is structured as follows. It first collects demographics and smart speaker model information, then assesses usage patterns and beliefs about data processing and storage. We then explore user interactions with current privacy settings. Additionally, some questions are informed by enhanced solutions and countermeasures for smart speaker privacy as discussed in related work [14] to assess participants' familiarity with and attitudes towards these emerging privacy protection methods. Next, the questionnaire includes the Affinity for Technology Interaction (ATI) scale [11] to gauge participants' comfort with technology. It finally uses constructs like Privacy Awareness (PA), Disposition to Value Privacy (DVP), and Privacy Experience (PE) to understand participants' general privacy attitudes [19]. The questionnaire, based on prior work for comparability, includes open-ended questions for qualitative insights and was refined through a pilot study to enhance flow and correct errors.

3.2 Study Distribution

The participants were recruited via a panel provider certified according to ISO 26362 [17] that ensures reliable and unbiased participant sampling. The study was approved by our Data Protection Officer (DPO). Although our institutions do not have a formal Institutional Review Board (IRB) process, we conducted our study in strict adherence to the Standards of Good Scientific Practice to ensure ethical compliance and integrity in our research. The sample representativeness for the Germany-based population was ensured via quotas applied during the participants' selection including gender, age, level of education and managed by our panel provider [7]. The questionnaire was implemented in LimeSurvey hosted on our server and respected the participants' anonymity. A total number of 1,103 smart speaker users contributed to the study between 09.08.2022 and 17.08.2022. The survey took participants approximately 15-20 minutes to complete, and they were compensated for their time.

3.3 Statistical Analysis

Since demographics and user profiles may influence the participants' answers [31,28,20], we divide our participants into independent groups. According to the Kolmogorov-Smirnov and the Shapiro-Wilk test, the answers are not normally distributed. We hence apply Mann-Whitney U tests to investigate the significance of differences between two independent groups and Kruskal-Wallis tests for more than two independent groups. Statistical significance is defined at the $p < 0.05$ level. If the applied Kruskal-Wallis test shows a significant difference, we perform a pairwise comparison using Mann-Whitney U tests to identify groups that significantly differ. Our analysis was conducted using SPSS, ensuring rigorous and standardized data evaluation.

4 Demographics and User Profiles

Fig. 1 shows the balanced distribution of our participants according to age group and gender. Most participants have a high-school diploma (32%) followed by a basic secondary schooling certificate (27%) and a secondary school certificate (21%). 6% resp. 4% have a bachelor's resp. master's degree, while $< 1\%$ have a PhD. Most participants are either full-time (53%) or part-time (17%) employees, while 2% are job-seeking and 14% not working (retired, maternity leave...). Moreover, 7% are students and 4% self-employed.

4.1 Smart Speaker Ownership and Utilization

All participants own a smart speaker. 77% own an Amazon Echo, 19% a Google Home/Google Nest, and Apple HomePod with 11%. A minority (4%) own other smart speaker models, such as Bose, Sonos, or Magenta. For participants owning multiple devices, the distribution of the most used smart speaker is the same

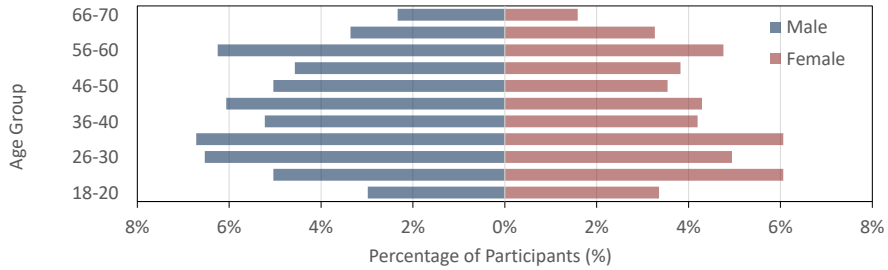

Fig. 1. Distribution among age groups for male and female participants

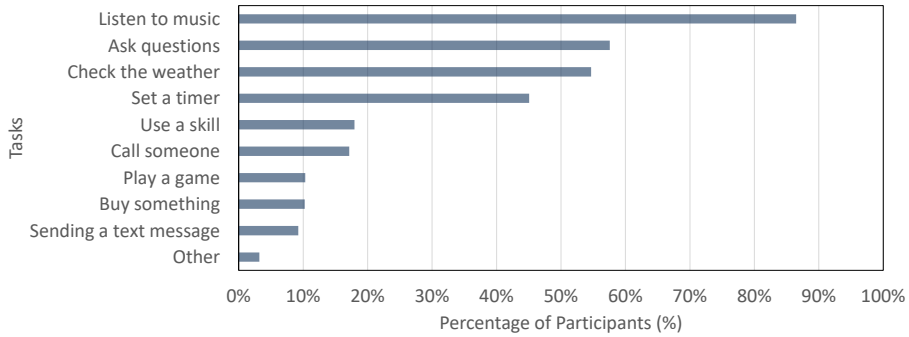

Fig. 2. Activities performed by the participants with their smart speaker(s)

as for the ownership. 75% interact with their device(s) at least daily (only 18% weekly, 5% monthly, and 1% yearly) for different activities, the top-10 being displayed in Fig. 2. These interactions mainly happen in a private context (90%).

4.2 Beliefs about Data Handling Practices

When asked about where their data are processed, only 29% of the participants gave the correct answer for the brand of their smart speaker as shown in Fig. 3 and 24% indicated that they do not know. For the data storage: 34% gave the correct answer and 23% said that they do not know. Fig. 4 also shows the answers for the data retention periods with only 14% of the participants providing the correct answer (i.e., indefinitely). Moreover, 40% participants agreed that their data could be viewed by employees. The same percentage further agreed that their voice could be analyzed to derive personal characteristics, while 46% agree that other family members or people in their household could review past interactions. Overall, many participants misunderstand how their smart speakers handle data, which influences their perceptions of privacy threats [21,24,1]. Apple now processes some voice commands offline. We compared responses from HomePod users with others and found no major differences, except more Ama-

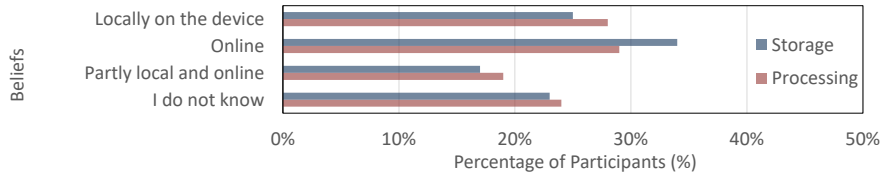

Fig. 3. Participants' beliefs on data processing and storage

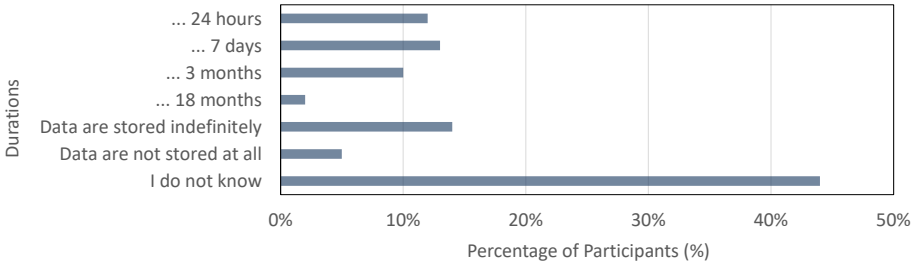

Fig. 4. Distribution of participants' answers with respect to data retention duration

zon Echo and Google Home/Nest users were unsure about data storage duration. While the applied methodology and sample are different, our results confirm the ones obtained in [21,24,1] and extend them by comparing smart speaker models.

4.3 Usage of Existing Privacy Settings

Fig. 5 provides a comparison of the different used (or not) privacy settings. For all settings, the majority of participants did not use them. The two main cited reasons for all users independently of the brand of their smart speakers are: (1) they do not know that they exist (32%) and (2) they do not care about them (20%). Complexity and time are also cited, but by fewer participants (9% resp. 7%). Note that these results are consistent with the findings of other works [21,24,1] based on interviews and smaller surveys. On the other hand, participants who had already interacted with privacy settings indicated that they agree or partially agree that it is both easy to find (23%) and (24%) interact with the settings. These participants interact with privacy settings on a weekly (8%) or monthly (7%) basis, except for changing the retention period when setting up the device (11%). Among the privacy settings, they interact most with: (1) review past voice recordings (32%), (2) review past smart home interactions (31%), and (3) delete past voice recordings and transcripts (29%). Like in Sec. 4.2, we explore the impact of smart speaker brands on user awareness of privacy settings. Our results indicate that Google Home/Nest users are better informed about managing data retention and third-party permissions than Amazon Echo users, likely due to Google's user-friendly app design.

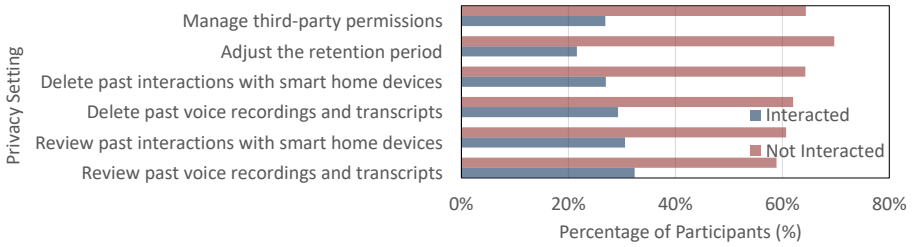

Fig. 5. Distribution of participants who have already interacted with specific privacy settings in contrast to those who have not

4.4 Affinity for Technology Interaction

With an average score of 3.19 (1 being the lowest score, i.e., a low affinity), our participants are hence not particularly tech-savvy. Indeed, only 12% show a very high affinity for technology interaction.

4.5 Privacy Attitudes

We finally analyze the participants' privacy attitudes based on [19]. The obtained average scores are: 3.26 for PA, 3.28 for DVP, and 2.80 for PE (see Sec. 3). This results in an average privacy score of 3.11. Hence, our participants are not particularly concerned about their privacy. In summary, our sample is diverse according to different dimensions including privacy attitudes. In addition to partially reproduce results obtained in qualitative studies, we observe significant differences between users of different brands not studied before.

5 Results

5.1 Importance of Privacy Settings for the Participants

Fig. 6 displays participant responses on various privacy settings using a 5-point Likert scale. All settings are deemed important, but storing only text transcripts and reviewing past interactions are rated slightly less crucial than others, with no significant difference among them. When comparing the means, the most important settings are (1) muting the smart speaker, (2) managing skill permissions, and (3) reviewing and deleting interactions with smart home devices. This preference for physical over software controls is supported by existing research on usability [4]. Privacy preferences vary significantly across genders, user types, technical affinity, privacy attitudes, and speaker models. Males prefer reviewing past interactions and storing text transcripts more than females ($N_{males} = 580$, $N_{females} = 492$; $Z < -3$, $p < 0.001$ and $Z < -2$, $p = 0.004$, respectively), while females more often choose to mute the speaker ($Z < -2$; $p = 0.018$). Further research is needed to understand the reasons behind these differences. Partici-

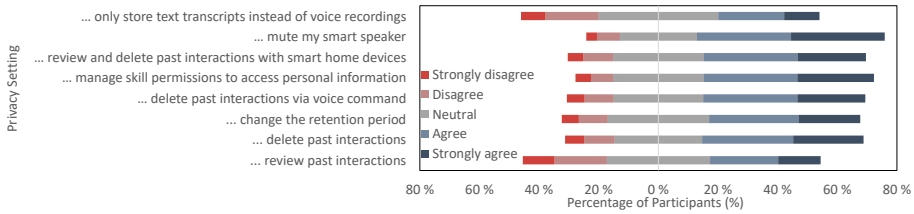

Fig. 6. Distribution of the answers to the question "It is important for me to have the option to ..." completed by different privacy settings

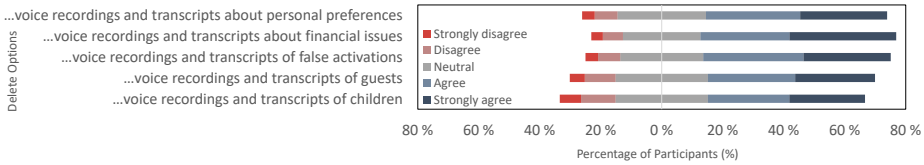

Fig. 7. Distribution of the answers to the question "I would tend to delete..." completed by different interactions

pants experienced with privacy settings rated all options higher in importance ($N_{not-interacted}$ = 547, $N_{interacted}$ = 556; Z < -2, p < 0.05), except for the muting option, which was equally important to both groups. Tech-savvy individuals also valued these settings more ($N_{non-tech-savvy}$ = 968, $N_{tech-savvy}$ = 135; Z < -2, p < 0.05), except for storing only text transcripts. The preference for storing only text transcripts is significantly different between users of major models like Amazon Echo, Google Home/Nest, and others (N_{amazon} = 817, N_{google} = 155, N_{apple} = 96, N_{others} = 35; Z < -2, p < 0.05). This suggests that users of these popular brands might have a different level of awareness about voice analysis privacy risks compared to others. As expected, participants with higher privacy scores indicated a significantly higher importance for all options ($N_{low-privacy}$ = 968, $N_{high-privacy}$ = 135; Z < -6, p < 0.05). Most participants view the privacy settings as important, especially the mute function of smart speakers. Our findings thus confirm that the importance of these settings varies with user profiles, underlining the need for more user-centric privacy options in future developments, tailored to diverse user needs.

5.2 Preferences

Deleting Interactions Our initial focus is on supporting users in identifying interactions for deletion [15,16]. Based on studies [21,24] that identified sensitive topics, we observe in Fig 7 that our participants are likely to delete interactions in this order: (1) financial issues, (2) false activations, (3) personal preferences, (4) guests, and (5) children. Again, there exist significant differences among our considered participant groups, except for users of various speaker models. Fe-

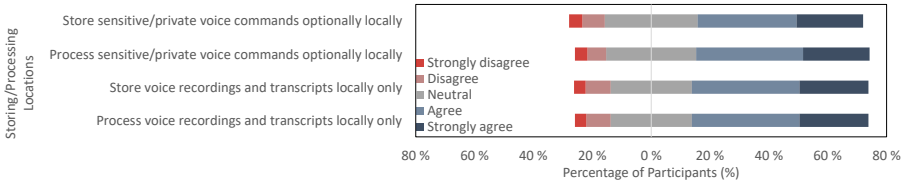

Fig. 8. Distribution of the answers to the question "I would prefer/like to have..." completed by different locations for processing and storage

males were notably more likely to delete recordings and transcripts (N_{males} = 580, $N_{females}$ = 492; Z < -2, p < 0.05), except in scenarios involving guests, suggesting a gender-based difference in privacy awareness [31]. Users that already interacted with privacy settings frequently opted to delete guest interactions ($N_{not-interacted}$ = 556, $N_{interacted}$ = 547; Z < -2, p = 0.021). In contrast tech-savvy users generally chose to delete interactions ($N_{non-tech-savvy}$ = 968, $N_{tech-savvy}$ = 135; Z < -2, p < 0.05), barring those with children, possibly valuing memory preservation over privacy [12]. This aligns with "sharenting" trends, despite privacy risks [3]. Participants with higher privacy concerns consistently showed a greater propensity to delete all interaction types ($N_{low-privacy}$ = 968, $N_{high-privacy}$ = 135; Z < -2, p < 0.05).

Local Processing and Storage Our participants prioritize (1) process voice recordings and transcripts locally only, (2) local storage of voice recordings and transcripts, and (3) local processing of sensitive/private commands (see Fig.8). This preference for local handling aligns with previous findings in the dimension of sensor data collected by robots [29], indicating a broad preference for local data processing. Those familiar with privacy settings show a significant higher interest in locally storing sensitive/private commands ($N_{not-interacted}$ = 556, $N_{interacted}$ = 547; Z < -2, p = 0.049), but not necessarily in processing them. This suggests a preference for customizable storage based on content sensitivity, though processing location seems less important to them, as indicated in Sec. 4.2.

Transparency and Control Participants' key preferences for future privacy-enhancing solutions include (1) being informed about what personal information can be derived from an audio recording, (2) activating a private mode where no recordings are stored, and (3) muting the smart speaker via voice command, although currently only button muting is available (see Fig. 9). Participants favor being informed about data extraction over voice obfuscation to protect against manufacturers, possibly due to misunderstandings about voice obfuscation or beliefs in offline data processing. This highlights the need for more research on user understanding of these privacy features. Again, differences in privacy preferences emerge among participant groups. Those experienced with privacy settings show a significantly higher interest in voice obfuscation, indicating a desire for increased control ($N_{not-interacted}$ = 556, $N_{interacted}$ = 547; Z < -3, p < 0.001). Tech-savvy participants also have a significantly higher interest for

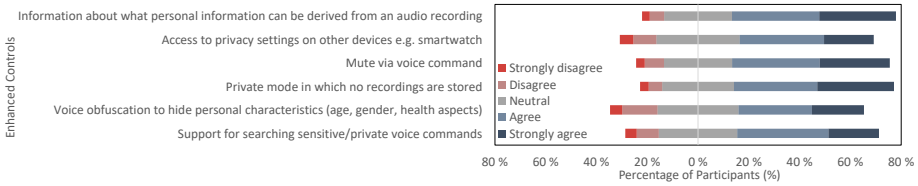

Fig. 9. Distribution of the answers to the question "I would prefer/like to have..." completed by different locations for processing and storage

Table 2. Further mentioned future options to improve privacy

Category	Response
Transparency	Periodic data report and automatic reminders before data are deleted
	Notification when unknown devices try to interact with the smart speaker
	Notifications as soon as personal data are accessed
	Informing guests about smart speakers in proximity
Deletion	Improvement of deletion options to easier find sensitive information and delete it
	Deletion via voice command
Control	Private mode similar to incognito browsing
	Controlling privacy settings via voice command
	Self-defined wake words
	Manual approval of recordings, e.g. with smartwatch
	Anonymous requests and decoupling of registered account with the manufacturer
	More individual options for specifying personal privacy preferences
Authentication	Stricter voice authentication
	Support voice authentication with password and fingerprint

privacy features ($N_{non-tech-savvy} = 968$, $N_{tech-savvy} = 135$; $Z < -2$, $p < 0.05$), though voice obfuscation is not significant. Participants who value privacy generally prefer all options presented ($N_{low-privacy} = 968$, $N_{high-privacy} = 135$; $Z < -6$, $p < 0.05$). Notably, Apple HomePod users are more interested in accessing privacy settings through additional devices, like smartwatches, compared to other brand users ($N_{amazon} = 817$, $N_{google} = 155$, $N_{apple} = 96$, $N_{others} = 35$; $Z < -2$, $p < 0.05$). This raises the question of whether privacy settings should be standardized across platforms or tailored to specific user groups.

Requirements for New Privacy Controls Participants' individual open answers to privacy settings or functionalities that they are currently missing can be categorized into transparency, deletion, control, and authentication, further detailed in Tab. 2. In the transparency category, one participant (P1) wishes for periodic data reports, and participants P2-5 seek automatic reminders before data deletion. For transparency improvement, participant P6 proposes notifications for interactions from unknown devices with the smart speaker. P7 prefers alerts when personal data, such as recordings, are accessed, while P8 suggests an app to alert guests about nearby smart speakers. These functionalities, however, are not available yet. For the deletion of recordings, P9 and P10 mentioned that deleting options should be improved to easily find sensitive content. Moreover, P11-14 wish to delete all data at once via a voice command. This is currently only possible using the app. To gain more control, P15-19 advocate for a private

mode where no data is stored, akin to a browser's incognito mode. P20 recommends voice navigation through privacy settings for ease and speed. P21-24 propose creating custom wake words and approving interactions manually, perhaps via a smartwatch. P25 suggests anonymous requests not linked to the user's account with the manufacturer, an idea present in academic research but not yet implemented [16]. Lastly, P26 believes current privacy controls are too generic, advocating for adaptive solutions as discussed in related studies [21,24,1]. In the last category, P27-29 request improved authentication with voice recognition that limits access to personal information to specific users, excluding others like children. P27 and P30-35 also propose combining voice authentication with passwords and biometrics, such as fingerprints. Currently, while voice authentication and passwords are common, the use of fingerprints in smart speakers is not yet implemented. In summary, 35 participants proposed various options to enhance their privacy protection, reflecting a broad range of interests in advanced privacy controls. Related studies like Lau et al. [21] and Malkin et al. [24] highlight interest in features like automatic deletion at set intervals and sensitive content filtering. While these studies focus on specific areas, our work confirms interest in automatic filtering and deletion but also allows participants to freely suggest ideas for advanced privacy controls. Notably, besides filtering and deletion, participants primarily proposed new methods in transparency and control for privacy protection. Overall, the participants' emphasis on wanting more transparency and control aligns with GDPR principles, highlighting a shared priority between user desires and regulatory standards in data privacy. The limited functionalities of current privacy settings suggest that the insights in Tab. 2 could guide future enhancements in privacy setting design and implementation.

6 Discussion

6.1 Similarities and Differences with other Studies

Recognizing that previous studies observed privacy perception differences by nationality and culture with different technologies [22,23,32], we explored similar patterns with smart speakers. We examined three aspects: beliefs about operations and data storage, interactions with privacy settings, and deletion behaviors in sensitive scenarios [21,24,1]. Our participants' beliefs align with previous findings on data processing misconceptions [21,24,1]. Many think their data are processed offline or are unsure about data handling. Like earlier studies, most participants avoid privacy settings due to unfamiliarity, though privacy-concerned individuals try to use them but remain misinformed about data management. Overall, misconceptions and privacy setting usage in our sample match those in US or UK groups [21,24,1]. Existing studies that explore control and transparency solutions [18,30,4] often address broader smart home contexts, not solely smart speakers, focusing on solutions like device muting or enhanced privacy notifications (Sec.2). Our study, however, specifically targets improved privacy settings for smart speakers, incorporating ideas from these and our own research

(Sec.3). We also encourage participants to contribute their own ideas for additional privacy improvements through an open-ended text response.(Sec. 5.2). While our study focused on smart speakers and differences in privacy concerns among user groups, our results complete those obtained in different areas. For example, Dawn Branley-Bell et al. found that older users are less likely to secure devices but more proactive in password security [8]. Sathasivam Mathiyalakan et al. discovered gender differences in privacy attitudes on Facebook [25]. J. Cho et al. identified differences in privacy concerns with wearable fitness devices based on exercise frequency [10]. These studies hence show that privacy concerns vary significantly across domains and demographics, including age, gender, and usage patterns. To address user requirements, we propose improving smart speaker interfaces with a user-friendly dashboard and color-coded filters to identify sensitive content. Additional features could include filters for interaction history and automatic reports to assist users in reviewing and deleting sensitive information. The interface could also offer verbal feedback on privacy settings to simplify navigation. These enhancements could guide policymakers in updating privacy standards to increase transparency, user control, and trust in smart technologies.

6.2 Limitations

We have chosen to conduct an online quantitative study to obtain a representative sample and hence be able to explore potential differences between users based on their characteristics, such as gender, affinity for technology interaction, privacy attitude, and used speaker models. As all findings are based on the participants' answers and not on direct observations, the usual limitations of quantitative online questionnaires apply. In this study, we have only included people who own a smart speaker. Moreover, we have only considered participants located in Germany to explore potential differences. Our choice for Germany is due to its distinctive cultural perspective on privacy, contrasting significantly with e.g. UK perceptions and influencing practices and attitudes towards data control and privacy [28,20].

7 Conclusion and Future Work

We have conducted an online questionnaire-based study with 1,103 participants about their privacy preferences when interacting with smart speakers, their privacy requirements, and their interest in novel privacy controls. We have shown that our participants indicate an overall interest in enhanced privacy controls for their smart speakers. They also ask for features to improve transparency about data handling practices and provide mechanisms to conduct data collection. Although we have specifically considered smart speaker users about privacy settings, non-users, guests, and bystanders should also be considered in the future. Nonetheless, we encourage designers and developers to use our findings in future work to develop usable enhanced privacy controls that are aligned with users' needs and wishes highlighted in our results.

References

1. Abdi, N., Ramokapane, K.M., Such, J.M.: More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In: Proc. of the 15th Symposium on Usable Privacy and Security (SOUPS) (2019)
2. Abdi, N., Zhan, X., Ramokapane, K.M., Such, J.: Privacy Norms for Smart Home Personal Assistants. In: Proc. of the 40th Conference on Human Factors in Computing Systems (CHI) (2021)
3. Adawiah, L.R., Rachmawati, Y.: Parenting Program to Protect Children's Privacy: The Phenomenon of Sharenting Children on Social Media. Jurnal Pendidikan Usia Dini (2021)
4. Ahmad, I., Akter, T., Buher, Z., Farzan, R., Kapadia, A., Lee, A.J.: Tangible Privacy for Smart Voice Assistants: Bystanders' Perceptions of Physical Device Controls. Proc. of the ACM on Human-Computer Interaction (2022)
5. Albayaydh, W., Flechais, I.: Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households. In: Proc. of the 32nd USENIX Security Symposium (USENIX Security) (2023)
6. Bernd, J., Abu-Salma, R., Choy, J., Frik, A.: Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. In: Proc. of the 18th Symposium on Usable Privacy and Security (SOUPS) (2022)
7. Bilendi und Respondi: Best for planning (2023), [Online]. `https://www.bilendi.de/`, accessed in 2023-08-21
8. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., Briggs, P., et al.: Exploring Age and Gender Differences in ICT Cybersecurity Behaviour (2022)
9. Chan, Z.Y., Shum, P.: Smart Office: A Voice-Controlled Workplace for Everyone. In: Proc. of the 2nd International Symposium on Computer Science and Intelligent Control (ISCSIC) (2018)
10. Cho, J.Y., Ko, D., Lee, B.G.: Strategic Approach to Privacy Calculus of Wearable Device User Regarding Information Disclosure and Continuance Intention. KSII Transactions on Internet & Information Systems (2018)
11. Franke, T., Attig, C., Wessel, D.: A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. International Journal of Human–Computer Interaction (2019)
12. Goggin, G., Ellis, K.: Privacy and Digital Data of Children With Disabilities: Scenes From Social Media Sharenting. Media and Communication (2020)
13. Han, S., Yang, H.: Understanding Adoption of Intelligent Personal Assistants. Industrial Management & Data Systems (2018)
14. Hernández Acosta, L., Reinhardt, D.: A Survey on Privacy Issues and Solutions for Voice-Controlled Digital Assistants. Pervasive and Mobile Computing (PMC) (2021)
15. Hernández Acosta, L., Reinhardt, D.: Enhanced Privacy for Voice-Controlled Digital Assistants. In: Proc. of the 20th IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) (2022)
16. Hernández Acosta, L., Reinhardt, D.: Multi-User Privacy with Voice-Controlled Digital Assistants. In: Proc. of the 20th IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) (2022)
17. ISO: ISO 20252:2019 (2019), [Online]. `https://www.iso.org/obp/ui/#iso:std:iso:20252:ed-3:v1:en`, accessed in 2023-08-21

18. Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y., Hong, J.I.: Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In: Proc. of the 41st Conference on Human Factors in Computing Systems (CHI) (2022)
19. Kröger, J.L., Gellrich, L., Pape, S., Brause, S.R., Ullrich, S.: Personal Information Inference From Voice Recordings: User Awareness and Privacy Concerns. Proc. on Privacy Enhancing Technologies (PoPETs) (2022)
20. Kühtreiber, P., Pak, V., Reinhardt, D.: Replication: The Effect of Differential Privacy Communication on German Users' Comprehension and Data Sharing Attitudes. In: Proc. of the 18th Symposium on Usable Privacy and Security (SOUPS 2022) (2022)
21. Lau, J., Zimmerman, B., Schaub, F.: Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. Proc. of the ACM on Hum.-Comp. Interact. (CSCW) (2018)
22. Li, Y.: Cross-Cultural Privacy Differences. In: Modern Socio-Technical Perspectives on Privacy. Springer, Cham (2022)
23. Lukács, A.: What Is Privacy? The History and Definition of Privacy (2016)
24. Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., Wagner, D.: Privacy Attitudes of Smart Speaker Users. Proc. on Privacy Enhancing Technologies (PoPETs) (4) (2019)
25. Mathiyalakan, S., Heilman, G., White, S.: Gender Differences in Student Attitude Toward Privacy in Facebook. Communications of the IIMA (2013)
26. Mozilla: Amazon Echo Dot (2021), [Online]. `https://foundation.mozilla.org/en/privacynotincluded/amazon-echo-dot/`, accessed in 2023-08-21
27. Mozilla: Google Nest Mini (2021), [Online]. `https://foundation.mozilla.org/en/privacynotincluded/google-nest-mini/`, accessed in 2023-08-21
28. Murmann, P., Beckerle, M., Fischer-Hübner, S., Reinhardt, D.: Reconciling the What, When and How of Privacy Notifications in Fitness Tracking Scenarios. Pervasive and Mobile Computing (2021)
29. Reinhardt, D., Khurana, M., Hernández Acosta, L.: "I Still Need My Privacy": Exploring the Level of Comfort and Privacy Preferences of German-Speaking Older Adults in the Case of Mobile Assistant Robots. Pervasive and Mobile Computing (2021)
30. Thakkar, P.K., He, S., Xu, S., Huang, D.Y., Yao, Y.: "It Would Probably Turn Into a Social Faux-Pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In: Proc. of the 41st Conference on Human Factors in Computing Systems (CHI) (2022)
31. Tifferet, S.: Gender Differences in Privacy Tendencies on Social Network Sites: A Meta-Analysis. Computers in Human Behavior (2019)
32. Wilkowska, W., Offermann-van Heek, J., Florez-Revuelta, F., Ziefle, M.: Video Cameras for Lifelogging at Home: Preferred Visualization Modes, Acceptance, and Privacy Perceptions Among German and Turkish Participants. International Journal of Human–Computer Interaction (2021)