Cultural Dimensions of Privacy Behaviours in Smart Speakers: A Systematic Review

Abdulrhman Alorini[1], Suleiman Abahussein[1], Abdullah Bin Sawad[2], Indra Mckie[1], Mohammed Althubyani[1], Afnan Bukhari[3], Noura Abdi[4], Kiran Ijaz[5], Mukesh Prasad[1], and A. Baki Kocaballi[1(B)]

[1] University of Technology Sydney, Ultimo, NSW 2007, Australia baki.kocaballi@uts.edu.au
[2] King Abdulaziz University, Jeddah 22254, Saudi Arabia
[3] Taif University, Taif, Saudi Arabia
[4] Liverpool John Moores, Liverpool, UK
[5] The University of Sydney, Camperdown, NSW 2050, Australia

Abstract. Smart speakers have proliferated globally, yet research on user privacy behaviours has largely overlooked how cultural contexts shape protection strategies. This PRISMA-guided systematic review analysed 14 empirical studies from five databases spanning the USA, UK, Netherlands, and Canada. Findings reveal significant cultural variations: users in highly individualistic cultures (USA, UK) favoured technical controls (e.g., muting, unplugging) with limited household privacy concern, while users in moderately individualistic cultures (Netherlands, Canada) adopted balanced strategies emphasising consent and collective negotiation. We propose the Cultural Privacy Protection Behaviour (CPPB) framework, extending Lutz and Newlands' three-category model (tech nical, data-related, social behaviours) to incorporate cultural dimensions as a fourth category. We offer design implications for culturallyadaptive privacy interfaces, including culture-aware defaults and crosscultural household support. This review demonstrates that effective smart speaker privacy design requires moving beyond universal solutions toward culturally-sensitive approaches.

Keywords: Privacy · Smart speakers · IoT security · user b ehaviour · systematic review

1 Introduction

Advances in technologies such as natural language processing (NLP), voice recognition, and artificial intelligence (AI) have increased the use and availability of Internet of Things (IoT) devices. A smart speaker essentially functions as a device that monitors the physical characteristics of the environment, with processors that process and analyse data, and actuators that perform the necessary actions, much like smart light bulbs and thermostats which exemplify IoT devices [1]. An intelligent speaker constantly listens for its activation keyword (such as "Alexa") to determine when users make requests. The smart sp eaker responds to requests using both audio feedback and virtual or actual actions [2]. Speechbased technologies also called conversational AI, intelligent dialogue systems, or virtual assistants include devices such as Amazon Alexa and Google Assistant, which operate through cloud-based systems [3]. Voice personal assistants (VPAs) employ Automatic Speech Recognition (ASR) to convert spoken commands into text, enabling Natural Language Understanding (NLU) to interpret intent and route r equests to relevant data sources, while Text-To-Speech (TTS) generates synthetic responses [4].

Smart speakers function as mobile, voice-controlled devices [5] that enhance human computer interaction in social and home contexts, improving usabil- ity and emotional engagement [6]. The broader ecosystem extends beyond the devices, often integrating into smart home environments, yet raises ongoing privacy and security concerns [7].

By December 2018, Amazon Alexa-enabled devices such as the Echo held (70%) of the U.S. market share [8]. With increasing media and academic attention on user privacy [9], concerns over smart speakers' "always-on" functionality have grown. These devices remain active to detect a predetermined wake word, after which live audio is transmitted over Wi-Fi to be stored and processed by corporations [10]. Microphones particularly in domestic settings represent among the most intrusive sensors [1], and some devices also include cameras.

While researchers have widely examined privacy threats, fewer studies explore how users protect themselves. Privacy lacks universal definition, varying across societies, groups, and individuals [11]. Users often decide what to share and take steps to prevent others from sharing it without consent [12]. Classic definitions include "the right to have one's own space" [13] and Westin's principle of controlling when, how, and to what extent information is disclosed [14]. Other definitions frame privacy as control over personal information distribution [15] [16].

Debate continues over whether privacy is a psychological state [17], a form of personal power [18], or the ability to refuse participation [19]. Influential frameworks, such as Westin's "notice and choice," emphasise individuals' control over data sharing [20]. This study systematically reviews literature on smart

speaker users' privacy protection behaviours to clarify the state of the art and identify future research directions.

However, existing research has largely overlooked how cultural contexts shape privacy protection behaviours in smart speaker use. Cultural dimensions theory suggests that cultural values fundamentally shape privacy perceptions and behaviours [21]. For instance, individualistic cultures may prioritize personal control over data, while collectivistic cultures might e mphasize group privacy and social harmony [22]. This cultural lens becomes particularly crucial as manufacturers deploy smart speakers globally across diverse cultural contexts, yet their privacy features often reflect Western-centric assumptions about privacy
[23].

While several systematic reviews have examined smart speaker privacy, none have investigated how cultural contexts shape user protection behaviours. [24] comprehensively reviewed privacy concerns, vulnerabilities, and countermeasures but analysed these through a universal lens without considering cultural variations in privacy perceptions or protection strategies. Similarly, [25] focused on algorithmic implementations and technical countermeasures, while [26] investigated security challenges and authentication vulnerabilities both providing valuable technical insights but overlooking how users from different cultural back- grounds might perceive and respond to these threats differently.

This review highlights that while prior studies identify low privacy awareness, convenience privacy trade-offs, and limited use of controls, they overlook cultural variations in these behaviours. This review addresses this gap by systematically examines how cultural dimensions (e.g., individualismcollectivism, power distance, uncertainty avoidance) shape smart speaker users' privacy protection strategies across societies. The paper consolidates fragmented findings, emphasizes the need for culturally aware privacy design, and contributes by (1) categorizing privacy behaviours (technical, data-related, social), (2) revealing cultural influences on privacy perceptions, and (3) offering design and research recommendations for more transparent and context-sensitive voice-enabled IoT systems.

While this review adopts a cultural lens, it is important to note that the included studies are predominantly situated in Western contexts. Accordingly, the findings reflect cultural variations within and across Western societies and should not be interpreted as representative of global smart speaker use.

The remainder of this paper is structured as follows. Section2 presents the theoretical background underpinning our cultural analysis. Section3 describes the PRISMA-guided systematic review methodology. Section4 reports the results, including a narrative synthesis of included studies and quantitative anal- ysis of privacy behaviours across cultures. Section5 discusses theoretical

contributions, the proposed CPPB framework, and design implications. Section6 concludes with future research directions.

2 Theoretical Background

This review integrates Hofstede's Cultural Dimensions Theory [21], Petronio's Communication Privacy Management (CPM) Theory [27], the Privacy Calculus Theory [28], and Altman's environmental psychology of privacy [29] to form a comprehensive framework for understanding culturally embedded privacy behaviours. Hofstede's dimensions particularly individualism, collectivism, power distance, uncertainty avoidance, and long-term orientation provide a macro-cultural lens through which privacy attitudes and behaviours toward smart speakers can be interpreted. Petronio's CPM theory complements this by explaining how individuals manage privacy boundaries and negotiate information disclosure within their cultural and social contexts.

The Privacy Calculus Theory adds a decision-making perspective, emphasizing that users weigh perceived benefits and risks differently across cultures Western users often prioritizing individual autonomy, while Eastern users account for family and collective considerations. Finally, Altman's environmental psychology situates privacy as a dynamic, culturally relative process, where boundary regulation, privacy mechanisms, and definitions of privacy violations vary across societies. Together, these theories highlight that privacy is neither universal nor static but shaped by cultural norms, social structures, and contextual interpretations of acceptable information sharing.

3 Method

3.1 Reporting Standards

A systematic literature review was conducted based on the PRISMA checklist [30]. The review protocol was registered on OSF Preregistration, with DOI: [10.17605/OSF.IO/PC9RW].

3.2 Selection of Primary Studies

A systematic search was conducted in May 2025 in the ACM digital library, IEEE, PubMed, Web of Science, and Scopus databases. The timeframe was set from January 31, 2014, as the start date, because Amazon's Echo became the first smart speaker with a built-in intelligent personal assistant, and the term "smart speaker" began to be used this year. The timeframe ended on April 31, 2025. The following search terms were used:"smart speaker","‌ smart assis- tant","voice assistant","virtual assistant","digital assistant","digital personal assistant","virtual personal assistant","amazon Alexa","amazon echo","google home","Siri" And"privacy". Screening also included Gray literature identified in the ACM digital

library, IEEE, PubMed, Web of Science, and Scopus databases (such as conference proceedings, theses, and dissertations).

3.3 Inclusion and Exclusion Criteria

The criteria included primary research studies, written in English, that investigated privacy concerns regarding smart speaker users and their privacy protection behaviour from a user-centred approach. According to the exclusion criteria, reviews, perspectives, opinion papers, and news articles were excluded due to lack of primary data, subjectivity, variable quality and focus on secondary interpretation. Additionally, studies that considered privacy from a security perspective (e.g. profiling, access control or hacking) were excluded.

3.4 Screening and Data Extraction

Search results were downloaded for all references identified. Following that, Rayyan AI was used to remove duplicates. By providing a platform for downloading articles and analysing data, Rayyan AI [31] enables researchers to conduct systematic reviews with increased transparency and efficiency by facilitating collaboration among multiple reviewers. Rayyan AI was then used to screen titles and abstracts of each paper. Two independent reviewers conducted the abstract and full-text screenings. Three reviewers extracted the following data from each study: authors, year of publication, study location, study aims, type and methods of study, participant characteristics, and main findings.

4 Results

The initial search criteria identified 1376 studies in the five databases. After removing duplicates, 852 articles remained. Following the screening of abstracts and titles, 58 articles remained. There was a dramatic decrease in articles due to a number of studies that examined privacy from an algorithmic security perspective, as well as any topics related to it, such as profiling, access control or hacking. Forty-six articles were excluded during the full-text screening. The primary reason for the exclusions at this stage was the majority of the studies either did not incorporate user perspectives [32] or did not concentrate specifically on the privacy of smart speakers [33] rather, they broadly touched upon the p rivacy of IoT devices [34].

The review ensured concentration on understanding smart speaker users and their privacy-related practices and experiences. Searching the references of the included studies identified one additional study. The Cohen's kappa coefficient was used to assess the level of agreement between two independent reviewers involved in this review process [35]. Two stages of screening were performed: the screening of titles and abstracts and the screening of full-text articles. The kappa statistic for the title and abstract screening was 0.39 (fair

agreement) and 0.57 (moderate agreement) for the full-text screening before consensus agreement was reached [36]. The relatively low kappa scores can be associated with highly varying and poor reporting practices in the published pap ers in this area. The Mixed Methods Appraisal Tool (MMAT) [37] was applied to assess the quality of included studies. Each study was evaluated based on five key criteria reflecting methodological quality and relevance to the research objectives, with scores ranging from 0–5. Two reviewers independently assessed quality, with disagreements resolved through discussion. The Study Design criterion assessed the appropriateness of the chosen methodology, accounting for 15% of the total weight. The Cultural Context criterion, which carried the highest weight of 30%, examined the extent to which each study explicitly considered cultural factors in its design and analysis. The Sample Diversity criterion represented 20% of the evaluation and focused on the level of geographic and demographic representation among participants. The Privacy Behaviour criterion, also weighted at
20%, evaluated the depth of behavioural analysis in relation to privacy protection practices. Finally, the Theoretical Grounding criterion, weighted at 15%, assessed the use of relevant privacy and cultural theories to frame and interpret the study findings. Fourteen articles were considered eligible for inclusion in the systematic literature review as shown in Fig.1.

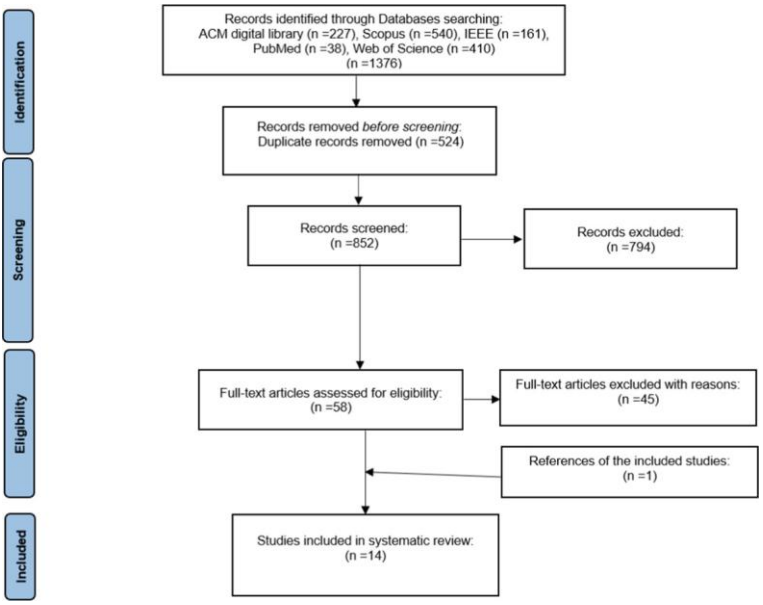

Fig. 1. Flow diagram.

Several findings and user recommendations emerged from our investigation, shedding light on the complexities of using smart speakers and privacy concerns.

In the review, all studies involved participants who used smart speakers, except for one study that compared users of smart speakers with those who did not. A narrative summary of the included studies is presented below, outlining their aims, methods, participant characteristics, and key findings. Choi et al. (2021) conducted a feasibility study in the USA to investigate older adults' perceptions of IoT smart home devices. The study spanned two months and included three research visits involving 37 participants (8 males and 29 females) with an average age of 77. The results showed that smart speakers helped participants maintain independence and supported memory functions. However, participants also expressed concerns about eavesdropping and the sharing of healthcare information. Meng et al. (2021) in the UK explored both visitors' and residents' perceptions of intelligent personal assistants through semi-structured interviews with 19 participants (8 males, 9 females, 1 non-binary, and 1 agender) aged around 26. The sessions lasted between 40 and 65 minutes. Findings revealed that smart speakers were more accepted in shared spaces, but participants lacked awareness of privacy protections and raised concerns about informed consent and data handling. Lutz and Newlands (2021) investigated users' privacy concerns with smart speakers through an online survey of 367 participants (152 males, 214 females, and 1 other) with an average age of 36. The study found that users were least concerned about other household members and more concerned about institutional privacy issues, contractors, and third-party developers accessing their smart speakers. Most participants were particularly worried about Amazon and Google contractors listening to private conversations, yet 72% never turned off their devices during private discussions, and over half left them on when not in use. Lin and Parkin (2020) examined privacy behaviours in relation to older and newer smart devices in the UK using an online survey of 100 participants (38 males and 62 females, average age 35). Their findings indicated low transfer of privacy behaviours from previous devices and limited use of privacy controls for smart assistants. Huang et al. (2020) from Canada investigated the sharing of smart speakers among multiple users through online surveys and semistructured interviews with 26 participants (14 males, 12 females) aged around 31. The study revealed concerns about housemates accessing personal information and company data usage, as well as a tendency toward all-or-nothing privacy strategies. Chalhoub and Flechais (2020) in the UK conducted semistructured interviews with 13 participants (10 males, 3 females) using grounded theory to understand how user experience factors influence perceptions of security and privacy in smart speakers. The results showed that users often traded security for convenience and found existing privacy features difficult to use. Pridmore et al. (2019) compared user perspectives on intelligent personal assistants between the Netherlands and the USA using surveys and focus groups. Although participant characteristics were not detailed, the study revealed that American users were more tolerant of in-home surveillance, whereas Dutch participants expressed

more critical views. Abdi et al. (2019) in the UK explored users' perceptions of security and privacy in smart home personal assistants through semi-structured interviews with 17 participants (8 males, 9 females) averaging 28years old. The findings indicated widespread misunderstandings about data processing locations, with users viewing smart speakers as central data hubs that build behavioural profiles. Many found it difficult to protect their devices effectively. Chhetri and Motti (2019) analysed online reviews from Amazon and Best Buy between October 2016 and October 2017 to understand users' privacy concerns regarding smart home devices. Participants' demographics were not specified. The analysis revealed strong user preferences for local control, data deletion, and encryption, alongside concerns about cloud-based data security. The authors recommended improvements in device programming and accuracy. Lau et al. (2018) in the USA conducted a diary study and semi-structured interviews with 17 smart speaker users and 17 non-users to understand adoption factors and privacy perceptions. Users seldom used privacy controls, mainly due to limited perceived utility and ongoing privacy concerns. Non-users expressed similar worries, while users developed brand loyalty toward their smart speakers. Manikonda et al. (2018) examined privacy concerns surrounding intelligent personal assistants in the USA using sen-timent analysis of online reviews and a survey of 51 participants, primarily students aged 1820. Although most participants acknowledged privacy issues, they maintained positive attitudes toward the devices. Many took protective actions such as muting microphones, restricting usage, or returning their devices. Belanger et al. (2021) in the USA conducted a longitudinal grounded theory study to explore family members' evolving privacy views when sharing technology. The study included 12 families (42 participants in total), with 24 adults aged 3454 and 19 children aged 717. The research identified various privacy concepts and proposed a three-stage lifecycle model describing how families adopt and manage shared devices over time. Malkin et al. (2019) in the USA surveyed 116 participants (44% female, average age 34) to explore beliefs and concerns about smart speaker recordings. Among them, 69% owned Alexa and 31% owned Google Home. Many users were unaware that recordings were permanently stored or reviewable, and only a few used privacy features such as microphone muting. Participants criticized manufacturers' data retention practices and expressed unease about recordings involving children's voices.

Finally, Major et al. (2021) in the USA assessed how Amazon Alexa's interface design affected users' understanding of native versus third-party applications. Their survey of 237 participants (103 students and 134 Mechanical Turk workers) revealed a widespread lack of awareness that third parties could develop Alexa skills. Participants struggled to distinguish between official and third-party functionalities, highlighting significant gaps in transparency and user comprehen- sion. The review of the 14 included studies highlights several aspects related to smart speaker usage. More specifically, four studies [5,38–40] examined

the role of smart speakers in the context of IoT smart home ecosystems. Three studies [41–43] investigated the shared usage of smart speakers among multiple users. Two studies [44,45] focused on considerations related to privacy in the design process. Five studies [46–50] explored users' privacy perceptions regarding smart speaker usage. Regarding the methodologies employed, the majority of studies(N=8) utilized surveys as their primary research method, followed by semistructured interviews. The remaining studies adopted various other research methods. A quantitative synthesis of privacy protection behaviours across different cultural contexts was conducted. To analyse cultural variations in privacy protection, this review adopts Lutz and Newlands' framework, which categorises behaviours into three types: technical p rivacy protection behaviours (TPPB), such as muting or unplugging the device; data privacy protection behaviours (DPPB), such as deleting or reviewing recordings; and social privacy protection behaviours (SPPB), such as refraining from discussing sensitive topics near the device. Table1 presents the distribution of these behaviour types across countries, revealing significant cultural variations.

Note: Percentages indicate proportion of participants reporting each behaviour type. Users have expressed similar concerns regarding their data privacy when using smart speakers within IoT smart homes. In particular, these

Table 1. Cultural Differences in Privacy P rotection Behaviours

Country	N Studies	N Participants	TPPB (%)	DPPB (%)	SPPB (%)
USA	8	453	72	28	45
UK	5	216	65	35	52
Netherlands	1	~25	45	55	68
Canada	1	26	60	40	70

concerns arose when information relating to healthcare and personal information was involved [38]. In the context of shared usage of smart speakers among multiple users, participants generally preferred placing s mart speakers in shared spaces rather than private areas [41]. Furthermore, a serious issue with roommates' access to personal data surfaced [42]. Users' privacy perceptions regarding smart speaker usage revealed profound anxiety about institutional privacy breaches. Notably, this included the concern that contractors from companies like Amazon or Google might have access to private conversations [46]. On the other hand, a notable lack of understanding among participants about third parties creating skills for Alexa was found [45]. Many participants were not aware that other parties could develop skills and make them available on the A lexa network, independent of Amazon. According to [45], over sixty-two percent of all participants incorrectly believed that "all the commands Alexa makes are created by Amazon." This indicates a lack of knowledge about third-party developers who create skills for Alexa. The study also found that about one quarter of the participants understood that third-party skills were capable of

accessing personal information directly. Other users believed that their interactions were exclusively with Amazon, or remained uncertain.

4.1 Privacy Protection Behaviour in the Included Studies

The analysis of the included studies revealed various privacy protection behaviours adopted by users in relation to smart speakers. These behaviours encompassed a range of actions aimed at safeguarding personal information and maintaining privacy. Table2 summarizes the identified privacy protection behaviours and their corresponding studies.

4.2 Cultural Patterns in Privacy Protection

The analysis indicates that cultural orientation shapes privacy protection behaviours. Highly individualistic countries (e.g., USA, UK) prioritize technical controls and exhibit all-or-nothing approaches focused on personal autonomy, with limited concern for household privacy. In contrast, moderately individualistic cultures (e.g., Netherlands, Canada) adopt more balanced strategies, combining technical and social approaches that emphasize consent, negotiation, and collective privacy management. Power distance relationships with

Table 2. Summary of All Privacy Protection Behaviours in the Included Studies

Privacy Protection Behaviour	Studies
Turn off the smart speaker	[41,45,46,50–52]
Muting the smart speaker	[46,49,51]
Unplugging the smart speaker	[38,46,49,53,54]
Avoidance (talking about sensitive data, using data collection services, purchasing features, returning the device, limiting u sage, speaking quietly near the smart speaker)	[38,41,42,46,49,53]
Deleting recordings	[46,47,52–54]
Changing settings (setting a new password)	[46,47,54]
Others (reviewing recordings, covering the smart speaker, using other devices, acceptance of privacy risk, using multiple profiles, trusting vendors who advocate for data privacy)	[41,46,51–53,55]

privacy behaviours proved complex. Countries with low Power Distance Index (PDI) scores tend to exhibit stronger scepticism toward corporate data practices, greater resistance to surveillance, and higher adoption of privacy protection to ols. However, the USA presents an intriguing paradox: despite its low PDI score of 40. [39] found American users developed“ surveillance tolerance,” suggesting cultural factors beyond Hofstede’s dimensions influence privacy acceptance. Uncertainty avoidance emerged as another significant factor shaping privacy strategies. High Uncertainty Avoidance Index (UAI) cultures showed clear preferences for binary privacy settings, avoiding ambiguous features and

favouring complete device disconnection over partial controls. This pattern reflects these cultures' need for clarity and predictability in privacy protection, preferring definitive actions over nuanced approaches.

Across the reviewed studies, two main user types were identified: primary users, who owned or most frequently used the smart speaker, and secondary users, such as visitors, family members, or ro ommates, who interacted with the device occasionally. Primary users were generally experienced, except for those in study [38], who were older adults using the device for the first time. Most studies examined both user types within shared domestic spaces, revealing that controlling other smart appliances via IoT commands was the most frequently reported task, followed by entertainment (e.g., listening to music or streaming radio content) and information-related activities, such as searching for weather or time updates.

Studies [42,46], and [47] consistently highlighted entertainment as the dominant activity among co-users, emphasizing its social and shared nature, while studies [5,41] observed a broader range of engagement, including IoT control, entertainment, purchasing, and information retrieval. Similarly, studies [39,48], and [49] emphasized IoT commands and entertainment but did not specify user type or environment, indicating a generalized b ehavioural focus. Research on primary users, particularly older adults [38,40], underscored functional use and independence through IoT interactions, whereas a few studies ([43–45,50]) offered limited contextual details yet reinforced the centrality of shared usage and entertainment-driven b ehaviours in smart speaker engagement.

5 Discussion

This review contributes to Human-Computer Interaction (HCI) by proposing a culturally informed understanding of privacy protection behaviours among smart speaker users. Unlike previous research focusing on technical vulnerabilities or privacy perceptions, these findings reveal how cultural dimensions fundamentally shape privacy strategies, offering a comprehensive framework to guide culturally-sensitive design interventions. The discussion will focus on the theoretical contributions, design implications, and future research directions arising from our cultural analysis.

5.1 Theoretical Cont ributions

Cultural Privacy Protection Behaviour (CPPB) Framework. This review extends [46] three-category model by introducing Cultural Privacy Protection behaviours (CPPB) as a fourth dimension, recognizing that privacy behaviours are not merely technical, data-related, or so cial, but fundamentally cultural. American users' "surveillance tolerance" reflects cultural narratives of technological

progress [56], while Dutch users' emphasis on consent reflects European privacy culture shaped by GDPR [57], and UK users' balanced approach reflects moderate individualism with social awareness.

The findings suggest the"privacy paradox" [58] manifests as culturally constructed, appearing differently across contexts. In high-individualism cultures, the paradox appears as a gap between stated concerns and individual inaction, while moderate-individualism cultures show less paradoxical behaviour due to social negotiation mechanisms. The Cultural Privacy Protection Behaviour (CPPB) framework is intended as a descriptive and interpretive synthesis, rather than a predictive or fully validated model. It consolidates observed patterns from existing empirical studies to explain how cultural values shape users' selection and enactment of privacy protection strategies in smart speaker contexts. While the framework may inform research on other voice-enabled or domestic IoT technologies, its scope in this paper is limited to smart speakers and shared household environments. Empirical validation and extension of CPPB across non-Western contexts and additional device categories remain important directions for future work.

5.2 Cultural Differences in Smart Speaker Privacy Design

The review reveals significant cultural variations in privacy attitudes toward smart speakers, shaped by differences in technology integration, societal norms, and regulatory frameworks. [39] found that American users were more likely to accept home surveillance over time, often prioritizing convenience and expressing the belief that they had" nothing to hide," while Dutch users exhibited greater privacy consciousness with a more cautious approach toward smart devices. Similarly, an analysis of online reviews revealed that privacy concerns regarding Internet of Things (IoT) devices were more prevalent among users in the United States compared to those in the United Kingdom and India [59].

5.3 Comparison with Previous R esearch

The findings align with and extend previous studies in several ways. [26] reported that users' concerns about privacy and security significantly influenced their decisions to use virtual assistants, an observation that aligns with our results. Similarly, research on smart speaker trustworthiness found that despite widespread adoption of Direct Voice Input (DVI), users remained uncomfortable sharing sensitive information through voice commands, preferring key-boards or touchscreens on computers or smartphones [60]. [26] also highlighted privacy challenges posed by third-party applications, reflecting our finding that many participants were unaware that third parties could develop Alexa skills. That study also noted compensatory behaviours among users to manage privacy risks, a theme consistently reported across the studies in our review.

However, our review differs from prior work by focusing on how cultural contexts shape users' interpretation of privacy protection behaviours and how such insights can inform smart speaker design. This approach emphasizes the importance of considering cultural differences during the design stage to ensure privacy features are appropriate and effective across diverse user populations. In contrast, [24] primarily addressed technical vulnerabilities, proposing solutions such as advanced traffic analysis techniques and machine learning methods to detect threats within the software development lifecycle. Similarly, [25] examined specific types of attacks targeting smart speakers, including Voice Command Injection, Voice Squatting, Masquerading, Traffic Analysis, and Adversarial Machine Learning. While these technical perspectives are valuable, this review highlights the need for further empirical research examining user behaviours and privacy concerns through a cultural lens, aligning with recommendations from [25] for more detailed investigation into user interactions and privacy management strategies. Such insights are essential for guiding the development of user centric smart speaker systems that prioritize culturally-sensitive privacy by default.

5.4 Perceptions and Usage of Smart Speakers, Ownership, Control, and Trust

Smart speakers can enhance users' independence, particularly by assisting individuals with memory decline through features such as alarms, reminders, and problem-solving tools [38]. Some participants subsequently purchased a device, indicating increased perceived utility. However, concerns over eavesdropping and sharing healthcare information hinder adoption [27,61]. Addressing these concerns involves user education on privacy settings [22] and alternative strategies such as embedding privacy-by-design principles [62], providing tangible or wearable privacy controls [5], implementing contextual consent models [63], and designing culturally sensitive interaction modes [23]. Participatory design has proven effective in aligning device functions with user expectations, especially in healthcare contexts [64,65].

Across studies, participants preferred placing smart speakers in shared rather than private spaces, indicating discomfort in intimate settings [41]. They also stressed informed consent, seeking clear warnings about the presence of smart speakers and other data-collecting devices. These findings highlight the need for transparency and control features, such as visible on/off indicators, accessible privacy settings, and clear activity notifications. Given the predominance of studies from the United States and United Kingdom, further research should explore perspectives from other regions, especially regarding device placement and privacy expectations [62]. In shared environments, users often developed a c omplex sense of ownership. [41] reported that frequent users formed attachments despite lacking control or decision-making authority. Many

relied on external protections such as government regulations and provider policies rather than direct actions, yet felt uninformed and ill-equipped to manage personal data. Addressing these gaps requires clearer guidelines and agreements defining ownership, shared use b oundaries, and privacy responsibilities. Personalization options such as userspecific profiles and adjustable privacy settings could further empower users to manage interactions while safeguarding data [66].

5.5 Concerns About Privacy and How Participants Act

Lutz and Newlands identified seven types of privacy concerns in smart speaker use: the device, household members, strangers, companies, contractors, thirdparty developers, and government entities. Institutional concerns were most prominent, with anxiety over Amazon or Google contractors accessing private conversations. Despite this, (72%) never turned off their devices during private conversations, and (51%) never deactivated them when unused [46].

Experience with shared devices influenced privacy behaviours. [47] found that users with prior shared-device experience were more likely to use privacy controls. However, many lacked knowledge of formal settings, relying instead on informal strategies like muting or avoiding sensitive topics. Thus, privacy concerns were widespread, but effective management mechanisms were often absent, leading to extreme approaches such as always leaving devices active or completely avoiding privacy features.

Privacy behaviours often reflected adaptive responses to perceived surveillance and inadequate controls. [38] reported that many viewed smart speakers as constant surveillance tools, prompting unplugging or disconnection. In shared environments, visitors withheld personal information and avoided data services to reduce exposure [41]. Engagement with protective measures was typically sporadic. Turning off the device was the most common technical action, while more proactive steps reviewing logs, changing passwords, or providing misleading information were rare [40,41,46]. Other actions included disabling voice purchases, clearing histories, limiting interconnections, and avoiding sensitive data storage [47,48,53].

Some users were unsure how to protect devices effectively. noted misconceptions, such as believing antivirus software for computers could secure smart speakers. Concerns over hacking and unauthorised access also led some to avoid certain features or restrict connectivity [67]. Overall, tension exists between smart speaker convenience and privacy concerns. Participants valued functionality and often traded some privacy for convenience, yet desired stronger control and greater transparency over device behaviour and data use [68]. Some users were unsure how to protect devices effectively. [48] noted misconceptions, such as believing antivirus software for computers could secure smart speakers. Concerns over hacking and unauthorised access also led some

to avoid certain features or restrict connectivity [67]. Overall, tension exists between smart speaker convenience and privacy concerns. Participants valued functionality and often traded some privacy for convenience, yet desired stronger control and greater transparency over device behaviour and data use [68].

5.6 Design Implications for Culturally-Sensitive Smart Speakers

The proposed design implications can be directly mapped to the cultural patterns identified in the review. For example, in highly individualistic contexts where users favour technical, all-or-nothing strategies, privacy interfaces should prioritise fast, device-level controls (e.g., one-tap mute or disconnect). In moderately individualistic contexts, where privacy is negotiated socially, interfaces should support shared controls, consent cues, and transparent activity indicators. In contexts characterised by higher uncertainty avoidance, users prefer clear and decisive actions; thus, privacy settings should minimise ambiguity by offering explicit modes (e.g., "private," "shared," "guest") rather than granular but opaque options.

Based on our cultural analysis, three key design directions emerge for culturally-sensitive privacy interfaces. First, adaptive privacy interfaces should incorporate culture-aware defaults that align with local expectations. Multicultural households demand privacy negotiation tools for shared spaces that can accommodate different cultural expectations within the same device ecosystem. Privacy warnings must also be culturally contextualized: individualistic cultures respond to messages emphasizing personal data access ("Your personal data may be accessed"), collectivistic cultures need family-oriented warnings ("Your family's conversations may be recorded"), and uncertainty avoidant cultures require clear, specific risk descriptions.

Design patterns for cross-cultural households present unique challenges as many homes contain members from different cultural backgrounds. These environments require privacy negotiation interfaces that support consensus-building [69], cultural mediation tools that explain different privacy expectations [70], flexible boundary management supporting multiple privacy models [71], and guest modes with cultural presets for visitors [72]. Such features become essential as globalization increases the prevalence of multicultural living arrangements. Privacy localization must extend beyond simple language translation to encompass deeper cultural adaptations. Information architecture should adapt to cultural mental models [73], default settings must align with regional privacy norms [74], local privacy regulations and cultural values need integration [75], and data visualizations should be culturally appropriate [76]. This comprehensive localization approach ensures privacy features resonate with users' cultural e xpectations rather than imposing foreign privacy concepts

5.7 Research Contributions and Future Directions

This systematic review advances understanding of privacy protection behaviours in smart speaker use through theoretical, empirical, methodological, and practical contributions. It introduces the Cultural Privacy Protection Behaviours (CPPB) framework, integrating cultural dimensions into existing privacy models to explain cross-cultural variations in privacy practices. Empirically, it provides the first systematic synthesis of cultural influences on smart speaker privacy, while methodologically, it offers a cultural coding framework to support future IoT privacy research. Practically, it proposes design guidelines for culturally sensitive privacy interfaces. The cultural patterns identified in this review are derived primarily from studies conducted in Western countries, which limits the generalisability of the findings to non-Western contexts. Future research should examine privacy protection behaviours in underrepresented regions to validate, extend, or challenge the patterns identified here.

Building on these insights, six propositions are outlined for future research: (1) users in highly individualistic cultures will favour technical privacy solutions; (2) the privacy paradox will be weaker in moderately individualistic contexts; (3) culturally aligned interfaces will achieve greater adoption; (4) users in low power-distance cultures will more actively resist surveillance; (5) cross-cultural households will exhibit hybrid privacy strategies; and (6) the effectiveness of privacy protection will depend on the alignment between cultural values and protection strategy type. Together, these contributions and propositions establish a foundation for culturally responsive privacy research and design.

6 Conclusion

This review underscores the complex relationship between cultural norms and the privacy protection behaviours of smart speaker users. The analysis reveals that existing privacy features often fall short of user expectations, particularly in culturally diverse settings where norms and sensitivities vary significantly. To address these gaps, the development of culturally responsive smart speaker designs that reflect the privacy values of different user groups becomes essential. The studies reviewed highlight the value of innovative strategies such as contextual privacy controls, user education, and participatory design in addressing privacy concerns more effectively. This review also identifies critical avenues for future research, including the need for deeper empirical exploration of privacy behaviours in underrepresented regions and the development of adaptive, context-aware privacy frameworks. A holistic, culturally aware approach to pri- vacy design therefore proves essential for building trust and supporting safer, more inclusive adoption of smart speaker technologies worldwide.

References

1. Bugeja, J., Jacobsson, A., Davidsson, P.: On privacy and security challenges in smart connected homes. In: Proceedings of the IEEE European Intelligence and Security Informatics Conference. IEEE (2016)
2. Lopatovska, I., et al.: Talk to me: Exploring user interactions with the amazon Alexa. J. Librariansh. Inf. Sci. **51**(4), 984–997 (2019)
3. Luger, E., Sellen, A.: "Like having a really bad PA": the gulf between user expectation and experience of conversational agents. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. ACM (2016)
4. Popovic, I., Culibrk, D., Mirkovic, M., Vukmirovic, S.: Automatic speech recognition and natural language understanding for emotion detection in multi-party conversations. In: Proceedings of the IEEE Conference. IEEE (2020)
5. Lau, J., Zimmerman, B., Schaub, F.: Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In: Proceedings of the ACM on Human-Computer Interaction, vol. 2, no. CSCW, pp. 1–31 (2018)
6. Porcheron, M., Fischer, J.E., Sharples, S.: "Do animals have accents?" talking with agents in multi-party conversation. In: Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing. ACM (2017) 7. Tabassum, M., et al.: Investigating users' preferences and expectations for alwayslistening voice assistants. In: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 3, no. 4, pp. 1–23 (2019)
8. Feiner, L.: Apple's smart speaker is struggling against rivals from amazon and google. CNBC.com (2019)
9. Alepis, E., Patsakis, C.: Monkey says, monkey does: security and privacy on voice assistants. IEEE Access, vol. 5, pp. 17 841–17 851 (2017)
10. Liao, Y., Vitak, J., Kumar, P., Zimmer, M., Kritikos, K.: Understanding the role of privacy and trust in intelligent personal assistant adoption. In: Proceedings of the International Conference on Information. Springer (2019)
11. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science **347**(6221), 509–514 (2015)
12. Ramokapane, K.M., Misra, G., Such, J., Preibusch, S.: Truth or dare: understanding and predicting how users lie and provide untruthful data online. In: Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing. ACM (2021)
13. Warren, S., Brandeis, L.: The right to privacy. Philosophical Dimensions of Privacy. Columbia University Press (1989)
14. Houghton, D.J., Joinson, A.N.: Privacy, social network sites, and social relations. J. Technol. Hum. Serv. **28**(1–2), 74–94 (2010)
15. Tavani, H.T., Moor, J.H.: Privacy protection, control of information, and privacyenhancing technologies. ACM SIGCAS Comput. Soc. **31**(1), 6–11 (2001)
16. Moor, J.H.: The ethics of privacy protection. Library Trends (1991)
17. Kokolakis, S.: Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput. Secur. **64**, 122–134 (2017)
18. Nissenbaum, H.: Protecting privacy in an information age: the problem of privacy in public. Privacy and Social Media. Routledge (2020)

19. Parker, R.B.: A definition of privacy. Rutgers L aw Rev. **27**, 275 (1973)
20. Martin, K.: Understanding privacy online: development of a social contract approach to p rivacy. J. Bus. Ethics **137**(3), 551–569 (2016)
21. Hofstede, G.: Dimensionalizing cultures: the Hofstede model in context. Online Readings Psychol. Cult. **2**(1), 8 (2011)
22. Li, Y.: Cross-cultural privacy differences. Advances in Information Security. Springer International Publishing, Cham (2022)
23. Sun, H.: Cross-Cultural Technology Design: Creating Culture-Sensitive Technology for Local Users. Oxford University Press (2012)
24. Maccario, G., Naldi, M.: Privacy in smart speakers: a systematic literature review. Secur. Priv. **6**(1), e274 (2023)
25. Edu, J.S., Such, J.M., Suarez-Tangil, G.: Smart home personal assistants: a security and privacy review. ACM Comput. Surv. (CSUR) **53**(6), 1–36 (2020)
26. Bolton, T., Dargahi, T., Belguith, S., Al-Rakhami, M.S., Sodhro, A.H.: On the security and privacy challenges of virtual assistants. Sensors **21**(7), 2312 (2021)
27. Ebbers, F., Karaboga, M.: Influencing factors for users' privacy and security protection behavior in smart speakers: insights from a Swiss user study. In: Proceedings of the International Conference on Information Systems Security and Privacy. Springer (2022)
28. Dinev, T., et al.: Privacy calculus model in e-commerce - a study of Italy a nd the united states. Eur. J. Inf. Syst. **15**(4), 389–402 (2006)
29. Altman, I.: The Environment and Social Behavior: Privacy. Territory, and Crowding. Bro oks/Cole Publishing Company, Personal Space (1975)
30. Liberati, A., et al.: The Prisma statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: explanation and elaboration. BMJ, vol. 339 (2009)
31. help.rayyan.ai. Understanding Rayyan: a comprehensive overview (2024)
32. Sivaraman, V., Gharakheili, H.H., Vishwanath, A., Boreli, R., Mehani, O.: Network-level security and privacy control for smart-home IoT devices. In: Proceedings of the IEEE Conference on Wireless and Mobile Computing, Networking and Communications. IEEE (2015)
33. Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karliychuk, T.: Smart IoT devices in the home: security and privacy implications. IEEE Technol. Soc. Mag. **37**(2), 71–79 (2018)
34. Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M.: IoT privacy and security: challenges and solutions. Appl. Sci. **10**(12), 4102 (2020)
35. P´erez, J., D´ıaz, J., Garcia-Martin, J., Tabuenca, B.: Systematic literature reviews in software engineering - enhancement of the study selection process using Cohen's Kappa statistic. J. Syst. Softw. **168**, 110657 (2020)
36. To, S.H.: Cohen's kappa statistic (2024)
37. Hong, Q.N., et al.: The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers. Educ. Inf. **34**(4), 285–291 (2018)
38. Choi, Y.K., Thompson, H.J., Demiris, G.: Internet-of-things smart home technology to support aging-in-place: older adults' perceptions and attitudes. J. Gerontol. Nurs. **47**(4), 15–21 (2021)

39. Pridmore, J., et al.: Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. Surveill. Soc. **17**(1/2), 125–131 (2019)
40. Chhetri, C., Motti, V.G.: Eliciting privacy concerns for smart home devices from a user centered perspective. In: Pro ceedings of the International Conference on Human-Computer Interaction. Springer (2019)
41. Meng, N., Keku¨ll¨uog˘lu, D., Vaniea, K.: Owning and sharing: privacy perceptions of smart speaker users. Pro c. ACM Hum. Comput. Interact. **5**(CSCW1), 1–29 (2021)
42. Huang, Y., Obada-Obieh, B., Beznosov, K.: Amazon vs. my brother: how users of shared smart speakers perceive and cope with privacy risks. In: P roceedings of the CHI Conference on Human Factors in Computing Systems. ACM (2020)
43. B´elanger, F., Resor, J., Crossler, R.E., Finch, T.A., Allen, K.R.: Smart home speakers and family information disclosure decisions. In: Proceedings of the Hawaii International Conference on System Sciences (2021)
44. Chalhoub, G., Flechais, I.: "Alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In: Proceedings of the International Conference on Human-Computer Interaction. Springer (2020)
45. Major, D., Huang, D.Y., Chetty, M., Feamster, N.: Alexa, who am i speaking to?: understanding users' ability to identify third-party apps on amazon Alexa. ACM Trans. Internet Technol. (TOIT) **22**(1), 1–22 (2021)
46. Lutz, C., Newlands, G.: Privacy and smart speakers: a mu lti-dimensional approach. Inf. Soc. **37**(3), 147–162 (2021)
47. Lin, V.Z., Parkin, S.: Transferability of privacy-related behaviours to shared smart home assistant devices. In: Proceedings of the IEEE European Symposium on Security and Privacy Workshops. IEEE (2020)
48. Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Proceedings of the Fifteenth USENIX Conference o n Usable Privacy and Security. Santa Clara, CA, USA: USENIX Association (2019)
49. Manikonda, L., Deotale, A., Kambhampati, S.: What's up with privacy? user preferences and privacy concerns in intelligent personal a ssistants. In: Proceedings of the AAAI Conference on Artificial Intelligence (2018)
50. Malkin, N., et al.: Privacy attitudes of smart speaker users. Pro c. Priv. Enhancing Technol. **4**, 2019 (2019)
51. Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Proceedings of the Fifteenth USENIX Conference o n Usable Privacy and Security. Santa Clara, CA, USA: USENIX Association (2019)
52. Chhetri, C., Motti, V.G.: Eliciting privacy concerns for smart home devices from a user centered perspective. In: Pro ceedings of the International Conference on Human-Computer Interaction. Springer (2019)
53. Chalhoub, G., Flechais, I.: "Alexa, are you spying on me?": Exploring the effect of user experience on the security and privacy of smart speaker users. In: Proceedings of the International Conference on Human-Computer Interaction. Springer (2020)
54. B´elanger, F., Resor, J., Crossler, R.E., Finch, T.A., Allen, K.R.: Smart home speakers and family information disclosure decisions. In: Proceedings of the Hawaii International Conference on System Sciences (2021)

55. Pridmore, J., et al.: Intelligent personal assistants and the intercultural negotiations of dataveillance in platformed households. Surveill. Soc. (2019)
56. Lyon, D.: The Culture of Surveillance: Watching as a Way of Life. John Wiley & Sons (2018)
57. Strycharz, J., Ausloos, J., Helberger, N.: Data protection or data frustration? Individual perceptions and attitudes towards the GDPR. Eur. Data Protect. Law Rev. **6**, 407 (2020)
58. Barth, S., De Jong, M.D.T.: The privacy paradox - investigating discrepancies between expressed privacy concerns and actual online behavior - a systematic lit- erature review. Telematics Inform. **34**(7), 1038–1058 (2017)
59. Liu, W., Lee, S.Y., Yao, M.: Acceptance and self-protection in government, commercial, and interpersonal surveillance contexts: an exploratory study. Comput. Hum. Behavior (2024)
60. Wells, A., Usman, A., McKeown, J.: Trusting smart speakers: Understanding the different levels of trust between technologies. Int. J. Comput. Sci. Secur. **14**(2), 72–81 (2020)
61. Haug, M., R¨ossler, P., Gewald, H.: Identification and influence of perceived risks on smart speaker use b ehavior. In: WI2020 Zentrale Tracks, pp. 1325–1331 (2020)
62. Zheng, S., Apthorpe, N., Chetty, M., Feamster, N.: User perceptions of smart home IoT privacy. Pro c. ACM Hum. Comput. Interact. **2**(CSCW), 1–20 (2018)
63. Emami-Naeini, P., Agarwal, Y., Cranor, L.F., Hibshi, H.: Ask the experts: what should be on an IoT privacy and security label? In: Proceedings of the IEEE Symposium on Security and Privacy. IEEE (2020)
64. Hu, X., Desai, S., Lundy, M., Chin, J.: Beyond functionality: co-designing voice user interfaces for older adults' well-being. In: Proceedings of the CHI Conference on Human Factors in Computing Systems (2025)
65. Mahmood, A., Cao, S., Stiber, M., Antony, V.N., Huang, C.M.: Voice assistants for health self-management: designing for and with older adults. In: Proceedings of the CHI Conference on Human Factors in Computing Systems (2025)
66. Palenio, H.: Privacy in the age of IoT: an experimental study investigating the attitude towards smart speakers of non-users through voice activation and data evaluation as intrusive features. Master's thesis, University of Twente (2020)
67. Meng-Schneider, N., Yasa Kostas, R., Vaniea, K., Wolters, M.K.: Multi-user smart speakers - a narrative review of concerns and problematic interactions. In: Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing (2023)
68. Acosta, L.H., Reinhardt, D.: "Alexa, how do you protect my privacy?" a quantitative study of user preferences and requirements a bout smart speaker privacy settings. Comput. Secur. **151**, 104302 (2025)
69. Dourish, P., Bellotti, V.: Awareness and coordination in shared workspaces. In: Proceedings of the ACM Conference on C omputer-Supported Cooperative Work. ACM (1992)
70. Irani, L., Vertesi, J., Dourish, P., Philip, K., Grinter, R.E.: Postcolonial computing: a lens on design and development. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. ACM (2010)
71. Palen, L., Dourish, P.: Unpacking "privacy" for a networked world. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. ACM (2003)

72. Barkhuus, L.: The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In: Proceedings of the CHI Conference on Human Factors in Computing Systems. ACM (2012)
73. Marcus, A., Gould, E.W.: Crosscurrents: cultural dimensions and global web userinterface design. Interactions **7**(4), 32–46 (2000)
74. Reinecke, K., Bernstein, A.: Knowing what a user likes: a design science approach to interfaces that automatically adapt to culture. MIS Quarterly, pp. 427–453 (2013)
75. Suchman, L.: Located accountabilities in technology production. Scand. J. Inf. Syst. **14**(2), 7 (2002)
76. Setlur, V., Stone, M.C.: A linguistic approach to categorical color assignment for data visualization. IEEE Trans. Visual Comput. Graphics **22**(1), 698–707 (2015)