Multi-User Smart Speakers - A Narrative Review of Concerns and Problematic Interactions

Multi-User Smart Speakers - A Narrative Review of Concerns and Problematic Interactions

Nicole Meng-Schneider
nicole.meng@ed.ac.uk
School of Informatics, University of Edinburgh
Edinburgh, United Kingdom

Rabia Yasa Kostas
School of Informatics, University of Edinburgh
Edinburgh, United Kingdom

Maria K. Wolters
School of Informatics, University of Edinburgh
Edinburgh, United Kingdom

Kami Vaniea
School of Informatics, University of Edinburgh
Edinburgh, United Kingdom

ABSTRACT

Smart speakers in multi-user spaces, such as Amazon Echos, introduce risks to both owners and anyone sharing the space. They store voice recordings of user requests, and anyone in range can potentially interact with the device. As smart speakers are usually bound to a single account, despite being shareable by design, it introduces potential tensions between users. We systematically searched the literature for findings on concerns and scenarios in which problems may arise and synthesised the resulting 20 papers in a narrative review. Owners were concerned about other users', potentially malicious, interactions, device faults, and third party sharing. In contrast, bystanders worried about "being listened" to and a lack of awareness and protections. Our findings show a clear gap in literature on the privacy concerns of regular and incidental secondary users of smart speakers.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing →** *Ubiquitous and mobile devices.*

KEYWORDS

smart speaker, voice assistant, multi-user, bystander, incidental user

ACM Reference Format:
Nicole Meng-Schneider, Rabia Yasa Kostas, Maria K. Wolters, and Kami Vaniea. 2023. Multi-User Smart Speakers - A Narrative Review of Concerns and Problematic Interactions. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3544549.3585689

1 INTRODUCTION

Smart speakers are internet-connected speakers with built-in microphones, hosting a smart voice assistant [3]. Prominent products are Amazon Echos or Google Nest speakers, previously Google Home. They are often found in smart homes alongside smart TVs, door bells, and thermostats. They are very versatile and can be programmed to interact with services from accessing entertainment to controlling smart home appliances.

Compared to other smart home devices, smart speakers pose unique security and privacy risks. Smart speakers are typically placed in shared locations like kitchens and living rooms, hence such devices are expected to be shared [15, 17, 22], and they can control communal smart devices like smart lights. Different than general smart home devices, smart speaker interactions, requests as well as responses, are audible to anyone in the room. This has lead to privacy issues such as revealing calendar entries or items from an online order [19, 32]. Smart speakers also accept voice request from anyone in the range of audibility, leading to further security risks such as unauthorised purchases or unlocking of doors [19, 24, 32, 36].

Smart speakers also collect and store voice recordings of anyone who interacts with them [1, 5, 18]. People worry about having their voice recorded [11, 12], especially in a private environment like a home. Even if people do not wish to interact with the smart speaker, there is a risk that their voice is recorded, processed and reviewable by the owner. If a smart speaker hears anything remotely resembling their wake word (e.g. 'Alexa'), it records and sends the request off for processing [18]. This happens regardless of whether the request was made intentionally or not [7, 27, 32, 37, 39].

Prior work shows that for smart homes and smart speakers alike, typically one motivated, tech-savvy user makes the decision, accepts the risks, and sets up the smart speaker with their account [17, 35]. Other people living in the same space like family members and cohabitants are often not consulted [17, 27]. Bystanders visiting the space have even less notice [27, 39]. These secondary users may have concerns and not understand the data handling procedure and risks, less even accept them [17, 22, 27]. The clear differences between account owners and secondary users in terms of control, device awareness and risk acceptance [23, 27] have led to tensions between users in smart homes [17, 21, 35, 40].

In this narrative qualitative review, we examine what is known about security and privacy concerns regarding smart speakers in shared spaces to identify gaps in the literature. Specifically, we answer the following research questions:

RQ1: What concerns do users have about multiple people using smart speaker technology?
RQ2: Which scenarios/anecdotes have users experienced involving multiple people that made them feel worried or awkward,

CHI EA '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3585689

or where the desired level of security or privacy was not possible to achieve?

Our review shows a clear gap in work on concerns of cohabitants and visitors to smart speakers in shared spaces. Existing work either focused on concerns of account owners of smart speakers, or looked at the different user groups in smart homes. Most studies looking at cohabitants focus on young children, but not adults. We conclude that there is a clear need to better understand the concerns of adult cohabitants and bystanders.

2 BACKGROUND

Typically, interactions with smart speakers are entirely voice-based, aided by LED indicators for when the device is "listening" to the user' request [18][1]. An interaction begins when a user says the wake word. The device begins to record the request, which is then sent to the manufacturer's cloud service for speech and request processing [3, 5, 10, 18]. Abdi et al. define two types on interactions: built-in skills such as information retrieval or weather, where the request is handled by the manufacturer, and third-party skills such as Spotify music or smart home control, where the request is passed on to the third party [1]. Due to the nature of a smart speaker, anyone within audible range can interact with it. Manufacturers offer mechanisms such as voice recognition and authentication pins for additional security, however they are not often utilised due to a lack of awareness [1, 20, 27].

2.1 Not just any smart home device

While smart speakers are often part of a smart home, used as a hub to control smart home devices by voice [17, 40], they stand out from other kind of smart home devices due to their potential for data collection and interaction type. People are usually comfortable with the collection of environmental data such as room temperature, however they worry about the collection of personally identifying data such as video and audio [11, 12], especially data collection in a private space [11]. However, smart speakers need to record and store voice recordings to offer their hands-free service [1, 5, 18]. By installing the device, owners, who may also have concerns regarding data collection and potential data leakage [1, 23, 27], are making a privacy-convenience trade off and decide to accept the data collection. Other users often have to accept the situation [17, 22, 27]. Some bystanders directly interact with smart speakers when visiting, while others report being accidentally recorded when the device activates [23, 27, 38, 39].

Smart speakers not only differ from other sensory smart home devices because of the data they are collecting, but also in how they are delivering their services. Since requests and responses are given in a voice-based manner, they can be overheard by anyone close enough. Therefore, interactions that used to be private, such as reading emails or checking the calendar, can be shared with other people in the room [8, 19].

[1]While there are smart speakers which also feature screens and cameras, such as Echo Show, in this review, we focus on voice-based interactions only.

2.2 Multi-user smart homes

Smart speakers and smart homes are rarely used only by one person. In both cases, there is typically a tech-savvy user, who drives the installation [1, 17, 21, 34]. This person has administrative power over the devices, thus more control than other users, but is also often responsible for dealing with faults and setting up security [17, 35]. Cohabitants of the owner were often not consulted upon adoption and were found to be more passive and less motivated to use it [17, 21, 34]. Account owners were also often not aware of concerns other users may have [22], despite having privacy concerns themselves [40–42]. Although some installers are aware of risks, they have limited understanding of smart home systems and their concerns are shaped by their experience in other domains like internet browsing [34]. These factors lead to gaps in threat models [40]. Research has also mapped out bystander privacy concerns in smart homes [17, 21, 26, 38, 39], but it is not clear to what extent these findings translate to the specific setting of shared smart speakers as they differ considerably in their heterogeneous data collection and interaction type.

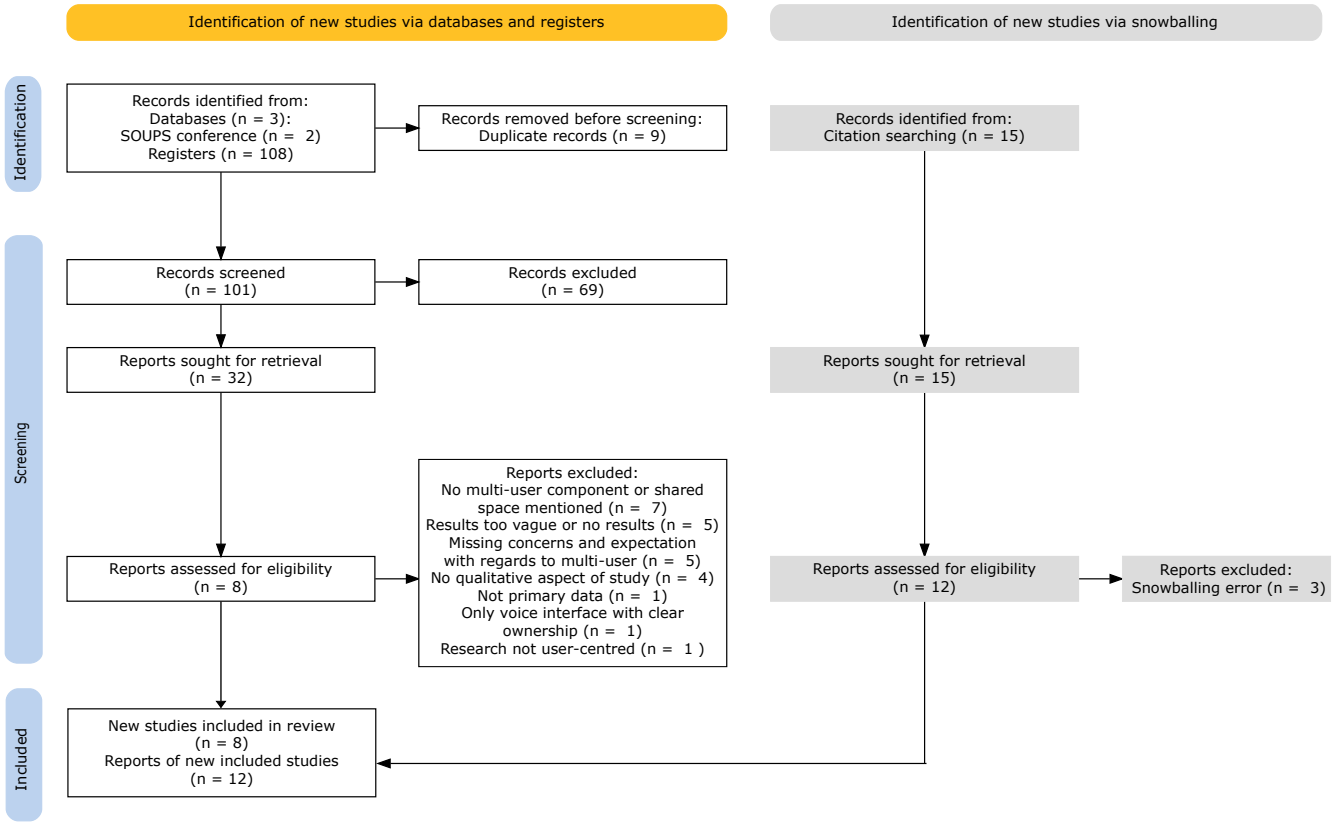
3 METHODOLOGY

We conducted a qualitative narrative review [13] of the literature in computer science and adjacent areas, using the databases Web of Science, ACM Digital Library, and IEEE Xplore. The query for the initial literature review was created using the SPIDER tool [28] and covered the following components: (1) synonyms for smart speakers or product names, (2) terms that cover worries and attitudes, (3) terms for the multi-user aspect (e.g. secondary users, shared devices), and (4) list of qualitative research methods. The search terms used for the review are provided in Table **??** in Appendix A.

Additionally, the lead researcher reviewed all Symposium on Usable Privacy and Security (SOUPS) publications between 2012 and 2022 based on title and abstract as not all papers are included in the selected three databases, and two papers were added for further review. Two reviewers independently screened all 110 titles and abstracts, then the full texts of 32 papers that passed abstract screening. Conflicts among the reviewers were resolved by discussion. An additional 15 papers were included based on manual search of references found in the initial systematic review process. A publication was considered if: (1) it focused on smart speakers or other interaction-based voice assistants, (2) the study had a qualitative aspect, and (3) it suggested findings on concerns or potential scenarios regarding shared smart speakers. We required a qualitative component as we extracted quotes and findings on a participant basis rather than large scale summaries. The final analysis was conducted on 20 papers. Figure 1 summarises the described methodology.

To answer RQ1, we extracted any findings which could be interpreted as a concern or worry or a lack thereof regarding sharing smart speakers. We then categorised these extracts to identify who the user is concerned about. For example, if the extract mentioned that owners are concerned about visitors overhearing their interaction, it was categorised as *owners concerned about visitors*. Since little differentiation was made between related and unrelated cohabitants, the two categories were combined. To answer RQ2, we extracted any situation that was quoted or described in the results and used inductive thematic analysis to discern common patterns.

Figure 1: PRISMA flow chart, detailing the various steps as well as exclusion criteria to choose papers for our review.



The analysis was conducted by the lead researcher and revised in discussion with the remaining authors of the paper.

4 RESULTS

As shown in Table 1, 12 (60%) of all papers cover smart speakers or other voice interfaces, while 8 (40%) papers contain valuable insights gained as part of a smart home study. Most studies (17 papers, 85%) focus on owners, while only 6 (30%) include information from the perspective of bystanders or non-users, and 7 (35%) cover cohabitants who are not family. Methodologically, interviews dominate (16 papers, 80%) , followed by diary studies (7 papers, 35%).

4.1 RQ1: Concerns about multi-user scenarios

Our first research question focuses on the concerns and worries that smart speaker users have in regards to sharing a device. Unsurprisingly, the majority of concerns extracted from the set of papers were mentioned by account owners. Account owners and cohabitants were mostly concerned about other potential users. In contrast, visitors seem to worry about the device and the manufacturer rather than other people. While most concerns were about their own privacy, safety, or security, we came across participants worrying about other people's comfort and privacy.

4.1.1 Concerns about 'other people'. Most concerns were mentioned by owners and related to potential other users within the smart speaker's proximity. Owners were often afraid that 'other people' may overhear their interactions [15, 20, 23, 29, 33]. *There were concerns about housemates overhearing phone conversations conducted over the speaker.[. . .] "I do not want other people in the household to hear me talking about work, and my wife does not want everyone else to hear her talking to her friends."* [20]. One person was even worried about being judged for the kind of tasks they use their smart speaker for [29]. Owners also mentioned other possibilities for unexpected privacy invasion, for example, similar voices leading to mismatched voice authentication or calling the account owner's contacts [9, 20]. Another major concern of owners as well as of some cohabitants was 'other people's' inappropriate behaviour [9, 14, 20, 27, 29]. They mention rudeness, accessing improper content, or causing annoyance through pranks. *When we asked participants about the possible motivation of insider threat actors, they suspected that friends and children would prank them.* [29].

A number of owners were afraid that strangers may use their smart speaker to gain access to their house or their data, or use it to get on their network for other malicious purposes [20, 29]. They were also afraid of strangers overhearing the authentication pin, thus bypassing the security mechanisms for sensitive actions [29]. A few participants feared malevolence by close acquaintances such as

Table 1: Overview of studies, their examined user group, method and sample size, grouped by investigated device. [30]† focused on a single use case. [25]†† looked at a fictional service, while similar to smart speakers, included hypothetical scenarios.

	Author/Year	Study	Owner	Family	Cohabitant	Bystander	Non-User	Interview	Diary Study	Focus Group	Survey	Sample Size	Comment
Smart Speakers Only	Meng et al. [2021]	[27]	•	•	•	•	•	•				19	
	Huang et al. [2020]	[20]	•	•	•			•				26	from 21 households
	Porcheron et al. [2018]	[30]†	•	•					•			5	single case study reported
	Garg [2020]	[14]	•	•				•	•			20	
	Beneteau et al. [2020]	[6]	•	•				•	•			10	Log analysis
	Ponticello et al. [2021]	[29]	•					•				16	
	Chalhoub and Flechais [2020]	[7]	•					•				13	
	Lau et al. [2018]	[23]	•				•	•	•			34	17 from each group
	Davitt and Brown [2022]	[9]								•		16	Staff in care facility
SS + Voice	Luria et al. [2020]	[25]††	•	•				•				54	18 families
	Garg and Sengupt [2019]	[16]	•	•				•	•			40	parents
	Storer et al. [2020]	[33]	•	•				•				12	6 mixed-visual ability pairs
Smart Homes	Shank and Gott [2020]	[32]	•	•	•	•	•				•	158	
	Garg and Moreno [2019]	[15]	•	•	•	•		•	•			20	
	Geeng and Roesner [2019]	[17]	•	•	•			•	•			18	
	Tabassum et al. [2020]	[35]	•	•	•			•			•	176	
	Zeng et al. [2017]	[40]	•	•	•			•				15	
	Wright and Shank [2022]	[37]	•					•				10	
	Yao et al. [2019]	[39]				•	•			•		18	Co-design sessions
	Ahmad et al. [2020]	[2]					•	•				19	

an ex-partner misusing their access after the relationship ends [29], or a housemate going through contacts and call history on purpose [20]. We found that cohabitants and visitors mentioned fewer concerns regarding 'other people'. Cohabitants mostly worried about inappropriate behaviour. Surprisingly, we did not find bystanders concerned about account owners seeing or hearing their interaction. Their concerns mainly related to the device nature, which is discussed in subsection 4.1.3.

4.1.2 Concerns for 'other people'. In a few cases, participants were concerned about 'other people's' privacy rather than their own. They worried about the amount of their children's data captured and stored [16] or about intruding upon privacy themselves; either by interacting with another person's smart speaker [27], or by overly monitoring their teenager's request history [25].

Some participants actively sought to protect 'other people's' privacy. They mentioned warning their visitors and offering to mute or unplug the device to avoid causing discomfort to their clients and coworkers [7]. *"We never discussed the matter. But whenever clients [they] are in my home, I make sure to plug off all the smart assistants"* [7]. Davitt and Brown found that nursing homes did not allow smart speakers in shared rooms to preserve the roommate's privacy [9].

4.1.3 Concerns about Device Infrastructure / Nature. Account owners, cohabitants, and bystanders all reported worries regarding the nature or functionality of smart speakers. Surprisingly, only Meng et al. reported that visitors were concerned about intruding on the owners privacy or the owner seeing the interaction [27]. More commonly, visitors were concerned about not knowing what data might be collected or how it is being used [2, 27, 39]. They worried about 'being listened to' and not even knowing of the device in the room [2, 27, 39]. Ahmed et al. discovered the need for tangible privacy mechanisms as visitors worry about protecting themselves, but do not know what being 'protected' actually looks like. *[We] observed that our participants understood the 'on' state with a high level of certainty. However, they often were not clear about the characteristics of the 'off' state.* [2]. They also worry about the lack of protection mechanism available and feel awkward asking for protection in a social situation [27].

Owners also had concerns about their device, but of a different nature. First, they mentioned unwanted sharing of their personal data with third parties [17, 20, 27]. *Almost half of all participants mentioned a loss of privacy as a risk when data they expect to be private is disclosed to a third party either through a data leak, sharing between companies or users.* [27]. The second concern is related to device faults. Findings show concerns regarding faulty authentication method, lack of granular permissions for different users, and wrong outcomes due to misinterpreting requests [15, 20, 32]. A participant noted: *"I do not feel the [purchasing feature is] secure enough because my younger brother has a similar voice. Sometimes when we talk [to] the speaker, it recognizes him as me. So [the speaker] may mess things up"* [20].

4.2 RQ2: Scenarios

With our second research question, we explored multi-user smart speaker situations which made users uncomfortable. From our set of papers, we were able to extract over 66 scenarios, which illustrate concerns or show the root of a concern. In our analysis, three themes emerged: intentional misuse, unexpected behaviour, and device sharing.

4.2.1 Intentional Misuse. The clearest cluster of scenarios involved malicious or naïve misuse. Misuse included a variety of minor annoyances like pranks [6, 17, 30, 40], children's obsessive repetition of a certain interaction [6, 17], disrespect towards device [27], and cheating in homework [16, 33]. In Geeng and Roesner's study on smart homes, a participant said: *When P14 had guests over, they [playfully] tried to use Amazon Echo voice commands to place orders from Amazon. P14 was annoyed about that, but had the ordering functionality disabled.* [17].

More serious situations described intentional privacy invasion [23, 25, 35] and unauthorised purchases [7, 20, 33]. In Storer et al. participant Ryan vents: *"I had no intention on buying him a new [freaking] MacBook . . . the next thing I know is—it's comin'. [. . .] That [ticked] me off, because I felt that that was stealing from me . . ."* [33]. An example of privacy invasion is presented in Tabassum et al.: *Travis [He] does not like his aunt having access to the audio logs because "(she) keeps looking through what's been said . . . just comes to a point where it's just a little nosy."* [35].

4.2.2 Unexpected Behaviour. Most papers reported scenarios in which a smart speaker behaved differently than the user expected and caused discomfort, distress, or even unintended data leakage. Some users were frustrated by being unable to get the smart speaker to do what they wanted [17, 30]. For example, *P1 logged that his girlfriend was annoyed she could not use the voice command 'turn off TV' to turn off the TV, since P1 has Apple, Chromecast, and Fire TV, each requiring a specific command, e.g., 'turn off Fire TV'.* [17].

In situations when a smart speaker mistakenly activates, participants reported feeling uncomfortable. [7, 27, 32, 37, 39]. *"It is kind of annoying when he [my father] isn't there, I unplug it because it is kind of weird like if we are talking just amongst ourselves and he says something vaguely like 'okay Google' which is the activation thing, it will start listening and it is kind of weird."* [39].

Participants also reported unease and embarrassment when requests were misinterpreted [16, 32, 33]. A participant in Shank and Gott's survey on AI leaking private information describes *"One of the children in my family was asking a device to play a certain song. Apparently, the device didn't 'hear' correctly. The information that came out was very disturbing and should have not been heard by anyone under the age of 18. [. . .]"* [32].

Unexpected smart speaker behaviour may also cause for private information to be leaked [9, 14, 27, 32, 37, 40]. In some situations, the revelation was unprompted, such as the case where Amazon Echo repeated conversations verbatim [37]. In another case, a teenager in an Asian Indian family describes an awkward situation: *"I once thought I was alone in the room, so I asked for some sensitive information from the speaker instead of searching the info on my phone. It blasted the response on full volume, which led my mom to come to the room"* [14].

4.2.3 Device Sharing. Sharing devices naturally lead to the need to coordinate with co-users. Situations ranged from tensions at adoption [27, 33] and coordination of sharing [15, 16, 23, 30] to controlling the speakers [6, 17, 30, 40]. Two participants in Meng et al. interview study described being uncomfortable when not being consulted before adoption; one explaining: *"There was nothing like 'Hey, there is going to be a potential spy in the house'. There was no foreknowledge on my part. I remember being remotely annoyed by that"* [27].

From the scenarios collected from the selected set of papers, we found differences in how sharing smart speakers is coordinated in a home. For unrelated cohabitants, ownership is the clear and decisive factor in prioritisation [16, 23]. Deciding on who gets to use the device is more complex in a family setting as smart speakers are considered 'family' devices [15]. Some described following a 'first come, first serve' approach [15], while others used task priority, social hierarchy or prior communication to decide who got to control the device [14, 30]. Tensions arise when rules are broken or misinterpreted, or the speaker is used in a way that bothers other users [14, 15].

5 DISCUSSION AND CONCLUSION

Based on our findings to answer RQ1, our work revealed that account owners of smart speakers worry about 'other people' with regards to their smart speakers. They are also concerned about device faults, which can cause unwanted privacy intrusion, and third party data sharing. This pattern agreed with Luria et al.'s findings on the hierarchical difference in social roles regarding smart speakers between 'insiders' and 'outsiders' [25]. In contrast bystanders were found to worry about being 'listened to', being unaware of the presence of a smart speakers, and the lack of protection mechanisms available to them. While there was little differentiation between related and unrelated cohabitants, children emerged as a separate user group. With over half of the reviewed papers including families, the amount of concerns related to children is unsurprising. Reporting entities were usually parents, not split into account owners and non-owner.

For RQ2, we identified three groups of scenarios which caused discomfort. The first cluster covers *misuse*, which aligns well with owners' concerns about other users. Participants also reported cases of *unexpected smart speakers behaviour*, such as unprompted activation or misheard request, which lead to revealing sensitive

information to bystanders. The last set of scenarios evidenced tensions arising from *sharing smart speakers*. Ranging from adoption to coordination of usage, some cases showed cohabitants being annoyed when they lacked the knowledge of how to operate the device.

We found substantial gaps in understanding of privacy concerns of cohabitants, bystanders, and non-users. Although previous work on secondary users showed them to be less motivated and rather passive towards smart devices [17, 27, 34], there are still concerns and privacy threats that are specific to this group and need to be addressed in future smart speaker technology. Work on addressing those concerns is underway for smart homes [4, 31, 38, 39], exploring design alternatives such as mobile apps [4] or tangible sensor controls [31], but there is little work for smart speakers.

When establishing models of perceived and actual threats, concerns and example scenarios need to be analysed together. Sometimes, there is overlap. For example, the cluster of misuse related situations mapped onto owner concerns of 'other people' misusing their device, and cases of a smart speaker activated without prompting matched what visitors are afraid of when they say they are being 'listened to'. However, most of the scenarios we analysed complement reported concerns. For example, while many situations reported children being exposed to inappropriate content or traumatised by the device behaviour, concerns mainly focusing on children behaving in a harmful way. Looking at scenarios where non-owners struggled to get the device to fulfil their request, we see a connection to owners' reports of their cohabitants' annoyance with interacting with a smart home device [17, 21]. However, this annoyance is not reflected in the explicit concerns reported.

Limitations. In order to ensure a manageable size, we did not search the grey literature or articles written by journalists. While other databases with better coverage of the social sciences could have been included, the databases we chose covers most of the relevant literature in computing (ACM Digital Library), engineering (IEEE Xplore), and related fields from the humanities, sciences, and social sciences (Web of Science). We also included two papers published at SOUPS. Due to space constraints, we only presented high level findings from our in-depth thematic analysis.

Future Work. We found a clear need for a better understanding of the privacy needs of related and unrelated cohabitants, bystanders, and visitors. We believe that such an understanding is crucial for the development of smart speakers and indeed their survival as a product category. In future work, we plan to conduct a deeper analysis of involved users and interaction types, which will allow to identify threat vectors and tailor protection mechanisms.

Acknowledgements

We thank Farid Bin Abdol Ghani for his assistance in paper screening, and the members of the TULiPS and Catalytics lab for their feedback throughout the process. This work was supported in part by the UKRI Centre for Doctoral Training in Natural Language Processing (grant EP/S022481/1) and the University of Edinburgh. Rabia Yasa Kostas was supported by the Ministry of National Education, Republic of Türkiye.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 451–466.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2 (2020), Article 116.

[3] Amazon Alexa. 2023. *How Does Alexa Work?* https://www.amazon.com/how-does-alexa-work/b?ie=UTF8&node=21166405011

[4] Leena Alghamdi, Mamtaj Akter, Cristobal Sepulveda Cardenas, Diego A. Cruces, Jason Wiese, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2022. Mi Casa Es Su Casa ("MiSu"): A Mobile App for Sharing Smart Home Devices with People Outside The Home. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing* (Virtual Event, Taiwan) *(CSCW'22 Companion)*. Association for Computing Machinery, New York, NY, USA, 184–187. https://doi.org/10.1145/3500868.3559709

[5] Amazon. 2021. *Alexa Terms of Use.* https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201809740

[6] Erin Beneteau, Ashley Boone, Yuxing Wu, Julie A. Kientz, Jason Yip, and Alexis Hiniker. 2020. Parenting with Alexa: Exploring the Introduction of Smart Speakers on Family Dynamics. Association for Computing Machinery, 1–13. https://doi.org/10.1145/3313831.3376344

[7] George Chalhoub and Ivan Flechais. 2020. "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. Springer-Verlag, 305–325. https://doi.org/10.1007/978-3-030-50309-3_21

[8] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. Alexa, Can i Trust You? *Computer* 50, 9 (2017), 100–104. https://doi.org/10.1109/MC.2017.3571053

[9] Joan K. Davitt and Jocelyn Brown. 2022. Using Voice and Touchscreen Controlled Smart Speakers to Protect Vulnerable Clients in Long-Term Care Facilities. *Innovation in Aging* 6, 4 (2022), igac024. https://doi.org/10.1093/geroni/igac024

[10] Jide S. Edu, Jose M. Such, and Guillermo Suarez-Tangil. 2020. Smart Home Personal Assistants: A Security and Privacy Review. *ACM Comput. Surv.* 53, 6, Article 116 (dec 2020), 36 pages. https://doi.org/10.1145/3412383

[11] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 399–412.

[12] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. 2022. Transparency for Bystanders in IoT regarding audiovisual Recordings. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. 649–654. https://doi.org/10.1109/PerComWorkshops53856.2022.9767212

[13] Rossella Ferrari. 2015. Writing narrative style literature reviews. *Medical Writing* 24 (Dec. 2015), 230–235. https://journal.emwa.org/writing-for-lay-audiences/writing-narrative-style-literature-reviews/ Publisher: European Medical Writers Association (EMWA).

[14] Radhika Garg. 2022. Supporting the Design of Smart Speakers to Foster a Sense of Ownership in Asian Indian Families. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), Article 167. Publisher: Association for Computing Machinery.

[15] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 2 (2019). https://doi.org/10.1145/3328915

[16] Radhika Garg and Subhasree Sengupta. 2019. "When You Can Do It, Why Can't I?": Racial and Socioeconomic Differences in Family Technology Use and Non-Use. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (2019). https://doi.org/10.1145/3359165

[17] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. Association for Computing Machinery, 1–13. https://doi.org/10.1145/3290605.3300498

[18] Google Nest Help. 2023. *Data security and privacy on devices that work with Assistant.* https://support.google.com/googlenest/answer/7072285?hl=en-GB

[19] Matthew B. Hoy. 2018. Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants. *Medical Reference Services Quarterly* 37, 1 (1 2018), 81–88. https://doi.org/10.1080/02763869.2018.1404391

[20] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. Association for Computing Machinery, 1–13. https://doi.org/10.1145/3313831.3376529

[21] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing

Machinery, New York, NY, USA, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598
[22] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further Exploring Communal Technology Use in Smart Homes: Social Expectations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3334480.3382972
[23] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (2018), Article 102.
[24] Andrew Liptak. 2017. *Amazon's Alexa started ordering people dollhouses after hearing its name on TV*. https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse
[25] Michal Luria, Rebecca Zheng, Bennett Huffman, Shuangni Huang, John Zimmerman, and Jodi Forlizzi. 2020. Social Boundaries for Personal Agents in the Interpersonal Space of the Home. Association for Computing Machinery, 1–12. https://doi.org/10.1145/3313831.3376311
[26] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM '20)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464
[27] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1 (2021), Article 45.
[28] Abigail M. Methley, Stephen Campbell, Carolyn Chew-Graham, Rosalind McNally, and Sudeh Cheraghi-Sohi. 2014. PICO, PICOS and SPIDER: a comparison study of specificity and sensitivity in three search tools for qualitative systematic reviews. *BMC Health Services Research* 14, 1 (Nov. 2014), 579. https://doi.org/10.1186/s12913-014-0579-0
[29] Alexander Ponticello, Matthias Fassl, and Katharina Krombholz. 2021. Exploring Authentication for Security-Sensitive Tasks on Smart Home Voice Assistants. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (soups 2021)* (2021), 475–491.
[30] Martin Porcheron, Joel E. Fischer, Stuart Reeves, and Sarah Sharples. 2018. Voice Interfaces in Everyday Life. Association for Computing Machinery, 1–12. https://doi.org/10.1145/3173574.3174214
[31] Sarah Delgado Rodriguez, Sarah Prange, Pascal Knierim, Karola Marky, and Florian Alt. 2022. Experiencing Tangible Privacy Control for Smart Homes with PriKey. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 298–300. https://doi.org/10.1145/3568444.3570585
[32] Daniel B. Shank and Alexander Gott. 2020. Exposed by AIs! People Personally Witness Artificial Intelligence Exposing Personal Information and Exposing People to Undesirable Content. *International Journal of Human–Computer Interaction* 36, 17 (2020), 1636–1645. https://doi.org/10.1080/10447318.2020.1768674
[33] Kevin M. Storer, Tejinder K. Judge, and Stacy M. Branham. 2020. "All in the Same Boat": Tradeoffs of Voice Assistant Ownership for Mixed-Visual-Ability Families. Association for Computing Machinery, 1–14. https://doi.org/10.1145/3313831.3376225
[34] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. 2019. "I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 435–450.
[35] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart Home Beyond the Home: A Case for Community-Based Access Control. Association for Computing Machinery, 1–12. https://doi.org/10.1145/3313831.3376255
[36] Aaron Tilley. 2016. *How A Few Words To Apple's Siri Unlocked A Man's Front Door*. https://www.forbes.com/sites/aarontilley/2016/09/21/apple-homekit-siri-security/
[37] David Wright and Daniel Shank. 2022. Rejecting and Restricting Smart Home Technology. *2022 IEEE International Professional Communication Conference (ProComm)* (2022), 352–357. https://doi.org/10.1109/ProComm53155.2022.00072
[38] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428
[39] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (2019). https://doi.org/10.1145/3359161
[40] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. USENIX Association, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
[41] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and in-Home User Study. In *Proceedings of the 28th USENIX Conference on Security Symposium* (Santa Clara, CA, USA) *(SEC'19)*. USENIX Association, USA, 159–176.
[42] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469

A SEARCH TERMS

The terms in each theme cluster were combined with an 'OR' Boolean operator, which each theme cluster itself was concatenated with 'AND' Boolean operator to create the whole search strategy.

Terms for Smart Speakers and Brands. Smart Speaker*, Intelligent Personal Assistant*, Voice Assistant*, Smart Home Assistant*, Smart Assistant*, Smart Agent*, Smart Personal Assistant*, Conversational Agent*, Conversational Interface*, Voice Assistant*, Voice-Based, Voice-Controlled, Voice Interface*, Amazon Echo, Alexa, Google Home, Apple HomePod, Siri, Google-Nest, Google-Nest-Audio, Bose, Asus, Eufy, Harman Kardon, Huawei, Lenovo, MarQ, Marshall, Polk Audio, Qubo, Redmi, Skoss, Sonos, Sony, Xiaomi, Zebronics, Bang and Olufsen, B&O, Cortana

Synonyms for Concerns. Disadvantag*, Worr*, Issue*, Percept*, Attitud*, View*, Perspect*, Prefer*, Aware*, Concern*, Experience*, Interact*, Tension*, Expect*, Consent*, Control*

Terms for Multi-User Aspect. Multi-user, Multiple User*, Bystander*, Passenger*, Secondary User*, Cohabitant*, Incidental User*, Visit*, Shared Device*, Shared Household*, Shared Space*, Indirect User*, People In The Home, Resident*, Co-occupant*, Co-resident*

Terms for Qualitative Research. Interview*, Workshop*, Diary stud*, Focus Group*, Home Tour*, Survey*, User Stud*, Questionnair*, Mixed Method*, Secondary Data Analysis, Qualitati*, Thematic Analysis, Qualitative Analysis, Cod*, Affinity Diagram*, Quot*, Co-Design

Received 19 January 2023; accepted 26 February 2023