

THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Owning and Sharing: Privacy Perceptions of Smart Speaker Users

Citation for published version:
Meng, N, Kekulluoglu, D & Vaniea, KE 2021, 'Owning and Sharing: Privacy Perceptions of Smart Speaker Users', *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW1, 45. https://doi.org/10.1145/3449119

Digital Object Identifier (DOI):
10.1145/3449119

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Proceedings of the ACM on Human-Computer Interaction

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.



Download date: 28. Mar. 2024

Owning and Sharing: Privacy Perceptions of Smart Speaker Users

NICOLE MENG, University of Edinburgh, UK
DILARA KEKÜLLÜOĞLU, University of Edinburgh, UK
KAMI VANIEA, University of Edinburgh, UK

Intelligent personal assistants (IPA), such as Amazon Alexa and Google Assistant, are becoming increasingly present in multi-user households leading to questions about privacy and consent, particularly for those who do not directly own the device they interact with. When these devices are placed in shared spaces, every visitor and cohabitant becomes an indirect user, potentially leading to discomfort, misuse of services, or unintentional sharing of personal data. To better understand how owners and visitors perceive IPAs, we interviewed 10 in-house users (account owners and cohabitants) and 9 visitors from a student and young professionals sample who have interacted with such devices on various occasions. We find that cohabitants in shared households with regular IPA interactions see themselves as owners of the device, although not having the same controls as the account owner. Further, we determine the existence of a smart speaker etiquette which doubles as trust-based boundary management. Both in-house users and visitors demonstrate similar attitudes and concerns around data use, constant monitoring by the device, and the lack of transparency around device operations. We discuss interviewees' system understanding, concerns, and protection strategies and make recommendation to avoid tensions around shared devices.

CCS Concepts: • **Security and privacy → Privacy protections**; *Social aspects of security and privacy*; • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**.

Additional Key Words and Phrases: smart speakers, voice assistants, multi-user, bystanders/visitors, privacy perceptions, protection mechanisms, social rules

ACM Reference Format:
Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 29 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Intelligent personal assistants (IPAs) – such as Amazon Alexa – are increasing in popularity, which has positive implications for convenience but also raises important questions around awareness and consent of the end users they interact with. IPAs are popular in part because a user can initiate a wide range of actions using only their voice. They support activities like searching the Internet, setting a timer, playing music, or interacting with other smart home technology such as light bulbs. Like their title indicates, they are intelligent voice assistants meant to fade into the background when not needed, but still be readily available when called.

Providing such a variety of services requires a lot of user data which includes sharing personal details with third parties, e.g. log-in details with Spotify to play back music, the user location for weather services, or recording the voice of the users and uploading it to Amazon or Google for

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Woodstock '18, June 03–05, 2018, Woodstock, NY
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

speech recognition [1, 4, 5, 17, 24]. While people who purchase IPAs and install them in their homes may be willing to accept the data usage aspects of the devices, that is not necessarily true for other people who encounter the devices. For example, when being gifted an IPA, the user might miss out on the chance to make the decision to accept the risks that come with IPAs [38]. Some may use the devices despite privacy concerns to please the gift giver, although privacy concerns are one of the main reasons for non-adoption [37].

People living with the device's legal owner such as flatmates, partners, or children often interact with the device on a regular basis and can see themselves as having ownership of the device. We therefore refer to them as *resident owners* of the device. These resident owners and *visitors* become secondary users when they enter the space [21]. By design [52], IPAs will interact with anyone they perceive to be speaking to them, thus, making everyone within vocal range a user. But these visitors or resident owners of IPA spaces have not explicitly consented to data usage and may have a poor understanding of the privacy implications of the device. Due to not being the account holder, their abilities to take actions against any of their concerns are subject to the given situation and the relationship to the account owner. Visitors may not even realise that an IPA is present since they are typically designed to fit in with other home decor.

Visitors and resident owners can also use their access to IPAs to (un)-intentionally breach the privacy of owners. Previous research has demonstrated potential security and privacy issues with IPAs reading out sensitive information like calendar entries [27], or allowing anyone in the range of audibility to express commands, e.g. purchases or unlocking doors [27, 39, 61]. Although security preserving options such as adding multiple accounts for shared devices were introduced, these measures are rarely known by owners, less even applied [21].

In this work, we are looking at the various kinds of users of smart speakers such as Google Home or Amazon Echo and their feeling of ownership. We aim to understand how visitors and resident owners perceive IPAs in shared spaces and how they act on it. In particular, we aim to compare emerging themes of in-house users of IPAs (account and resident owners) and visitors in terms of: 1) their understanding of how these devices function, 2) their concerns about data usage, 3) protection behaviours they use, and 4) social norms around non-owners using IPAs. To explore these issues, we conducted semi-structured interviews with 9 visitors and 10 in-house users, including drawing and free listing exercises to probe their understanding of how IPAs fulfil different types of user requests. Most of our participants were students and young professionals, who live in shared households or share devices with other family members.

We find that people who regularly interact with an IPA in their home consider themselves to be owners, even if they have no direct access to associated accounts. However, regular interaction with an IPA does not seem to result in either a better understanding of its functions, or a difference in concerns. Participants identifying as owners and visitors have similar levels of awareness and worries around IPA usage. Protection strategies were also similar ranging from just accepting the risks to non-usage of all or certain types of features. Similar to other smart home technology, people are worried about social boundaries around using someone else's IPAs. We found participants expressed these social boundaries as a social etiquette issue where they wanted to respect owners but were unsure about acceptable behaviour. However, despite existing social rules and protection strategies, we found tensions arising from mismatched expectations and existing defaults.

Contributions.

- We explore privacy perceptions and concerns of a range of users of IPAs, including visitors, in shared spaces. Our findings confirm existing research [1, 30, 37] in terms of concerns and system understanding as well as show that the differences between account owners, resident owners, and visitors are minimal.

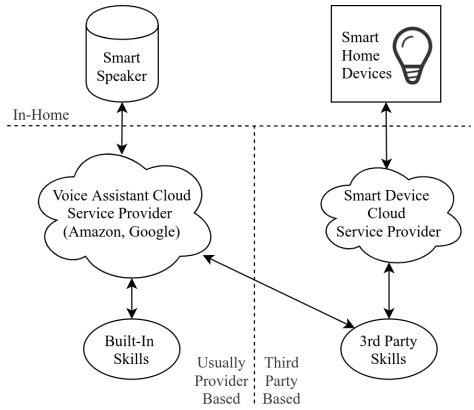


Fig. 1. Smart speaker services and data flows. Graphic inspired by [17].

- We provide insights into unwritten social expectations around IPA interactions of in-house users and visitors and discuss how they function as a privacy boundary.
- Our findings that the relationships between owners and towards the device are rather complex confirm prior work [21, 68]. However, we also find novel evidence that the concept of ownership of IPAs is not binary. Regular users, who do not have their account connected or purchased the device, often identify as owners despite the lack of control.
- We make recommendations on how to mitigate user concerns, integrate various user groups in a shared smart home, and fulfil users' desire for transparency and control of shared devices.

2 BACKGROUND

To operate seamlessly, IPAs are built on a multi-organisation infrastructure and can be in a variety of hardware devices including smart phones and speakers. Smart speakers, e.g. Amazon Echo or Google Home, consist of a microphone and a speaker, which act as the interface for the virtual assistant. IPAs like the Google Assistant and Alexa continuously operate in a "passive listening mode" where they listen for a user to say a *wake word* such as "Alexa" or "Hey Google", ideally disregarding all other audio [6, 18, 25, 33]. Upon hearing the word, the device activates, records the user's request, and uploads it to the provider's cloud to perform speech recognition [4, 6, 25] as shown in Figure 1. User requests are then mapped to predefined behaviours that Amazon calls "skills", a term we use throughout the paper for simplicity. There are two skill types: 1) built-in skills offered by the provider and 2) third-party skills designed by a third party and processed on their server [1, 4, 5, 17, 24]. For example, a user might say: "Alexa, turn on the living room light". That request is then uploaded to Amazon's Alexa cloud for processing, and forwarded to the smart light bulb provider's servers, which then sends a turn on request to the light bulb in the user's home.

The result of the interconnectivity of smart speakers is that a previously in-home action, such as turning on a light, now involves audio recording and data being sent to at least two companies. That behaviour may not be obvious to the device owner, and possibly even less obvious to other people who may only occasionally visit a space containing an IPA.

Fulfilling requests also requires the use of specific user data. For example, the weather skill needs a location to provide the user with accurate weather predictions. Third-party skills such as playing back a song from Spotify require an associated user account to gain access to their service [6, 25].

Correctly understanding user voices also requires data. Most IPAs retain audio data which may then be labelled by humans [12, 13, 18] for training the speech recognition systems. Such

training helps the system better recognise the vast array of accents and voice patterns used by real humans [32]. Finally, any developer can create skills, but Amazon Alexa skill developers are not required to provide a privacy policy disclosing how they use the data [2, 5].

3 RELATED WORK

Previous research has focused on smart home device adoption, personification and privacy perceptions [1, 30, 37, 40, 41, 58, 70]. Researchers have also explored the potential future design space of voice controlled interfaces [54] as well as health applications [9] and anxiety control [63]. These devices, specifically smart speakers, are placed in a central, main living location where they provide the most convenience such as helping with daily tasks or playing back music [7, 19, 37]. Convenience as well as an early-adopter mentality [37] are reasons for adoptions, whereas some decide against it due to a lack of perceived utility and privacy concerns [31, 35, 37]. Most smart home devices are purchased and set up by a tech-enthusiastic home member, who finds pleasure in exploring new technology [21, 37, 58].

Users have also been found to underestimate security and privacy risks of smart home devices due to an incomplete mental model and a lack of understanding how components of smart homes work together [1, 30, 37, 59, 67, 69, 70], such as assuming that all data is processed locally and not shared [1]. Users feel vulnerable when using technology they do not understand [15]. Prior work also shows that smart home users are concerned about unwanted data access, data misuse and unethical data collection [30, 46, 59, 67, 70]. For smart speakers, these concerns extend to misuse by unintended visitors, inappropriate access to personal information or voice match false positives [30]. Users' understanding of privacy and data practices is heavily based on their experience with social media and other companies [30, 44, 59].

3.1 Employed Protection Mechanisms

Prior research has shown that smart home users avoid certain features of devices for their safety or because they are unaware of existing protections [19, 30, 59, 67]. For example, we see a lack of awareness of the devices' history and the ability to view and delete recordings [10] or disabling the shopping feature as a protection from other users [59]. Both Google and Amazon are offering the option of adding multiple accounts to one device or recognising voices [4, 23], however, this strategy is rarely known to users, even less employed [19, 30]. While some users are concerned and engage in protections themselves, existing work also finds users accepting risks and not actively engaging in risk mitigation strategies [30, 37, 59]. These IPA users see their own data as not worth hiding or that they "have nothing to hide" [37, 57]. Or they trust their IPA provider to protect their privacy and do not engage in further protection strategies [1, 37]. Some other prefer the convenience of the service [47, 69] and "mindlessly consent" to sharing their data [48, 50].

3.2 Use of IPAs by Non-Owners

Smart home devices are commonly used by people other than the owner. Personal devices like phones, tablets and PCs [45, 60] or Internet of Things and smart home devices are shared among various parties in a home [19, 21]. Reasons for sharing may be to provide key access for a smart door lock or using the Amazon Echo's drop-in feature to check in with elderly relatives [21, 60]. There are a variety of relationships in a multi-user smart household including: partners, flatmates, family members, or visitors [21, 68]. While most users have positive attitudes towards sharing devices and expect cohabitants to use smart devices in the home [34], not all devices are considered safe or appropriate for sharing [34, 60]. For example, users seem uncertain whether smart speakers should be considered shared devices [34]. While they are established as a shared "family device" [19], they can cause tensions when sharing expectations are unmatched. Geeng and Roesner also found a

lack of knowledge or abilities in co-users, an imbalance of control, varying preferences, or device inflexibility can provoke unease at different points in time [21]. The relationship between the owner and any co-occupants influences how these tensions are resolved, how sharing is coordinated and what kind of protection mechanisms are employed [19, 21, 34, 65].

3.3 Adoption and Maintenance of Shared Devices

The home member who *drives* the installation of the device tends to also be the sole account holder resulting in a concentration of knowledge and control [21, 37, 67]. Device maintenance and error management fall to the driver in shared smart homes as co-users have been found to be more passive towards these device [21]. Geeng and Roesner show that drivers do not consult with cohabitants before installation due to a passivity of co-users or inequality in their relationship [21], however, other work shows that partner and flatmates expect consultation [34]. This situation creates an imbalance in control, knowledge, concerns, and interest in these devices, which may change power dynamics in the home and create further tensions between co-users [21, 37, 67]. Even for "family devices", there is a clear distinction between the account holder and other users [19]. For example, most co-occupants are not aware of certain features [21] or the ability to view or delete previous requests [10, 21, 43], but have similar concerns about data handling and monitoring as smart home owners [30, 37, 59].

3.4 Privacy Perception of Visitors

Visitors may become temporary users when visiting a smart home, have their own concerns, and can cause tensions and risks [21]. Concerns of bystanders were explored in the context of audio or video capture of wearable Augmented Reality [14], surveillance cameras [56], or lifelogging [11, 28, 29]. Visitors have been found to understand less of the risks of smart devices and have even less control in smart homes [67]. In their study, Yao et al. found that privacy perceptions of smart home bystanders are shaped through norms, device awareness and their own privacy seeking behaviour [66], they propose a privacy design to address privacy concerns [65, 66]. Kraemer et al. found that most users are happy to share their devices with guests and accommodate their wishes, but need to balance politeness and security [34]. Owners also seem unaware of privacy concerns of co-users and visitors [21].

3.5 Research Aims

We find that the concerns of visitors, their needs and perceptions of smart speakers require further investigation to understand how to support them in multi-user smart homes. And not only visitors, but we find resident owners such as flatmates and family members and their perception of shared devices as well as expectations in need of further exploration. We are interested to understand the concept of ownership, control, attitudes, and sharing expectations of those users who do not have the same controls as the account holders but use the device on a regular basis. Similarly, although the view of owners on visitors of smart speakers and on cohabitants of smart home devices have been looked at in terms of concerns and potential tensions, the way they handle expectations when sharing is still unclear. We see the value of comparing the social expectations, concerns, and attitudes of owners and other groups.

4 METHODOLOGY

We conducted semi-structured interviews with 19 participants to shed light on the situation in which they encountered smart speakers, existing privacy perceptions, and utilised protection mechanisms. Further, we aim to understand whether their feeling of ownership influences their system understanding and the existence of a social rules regarding IPA interaction. Designing the

study was an iterative process including feedback from security experts in our research group at the University of Edinburgh. The study design was approved by the Informatics ethics procedure with number #3465.

4.1 Recruitment

We recruited participants who owned or have encountered an Amazon Echo or Google Home by emailing different groups at the University of Edinburgh and posting on the university's internal career platform. We used these methods to target young professionals and students as they are more likely to be in shared living environments and may use spaces like bedrooms to host visitors, so bedroom-based speakers may have visitor interactions. We were open to other groups, but our recruitment strategy resulted in participants that were mainly PhD students and young professionals.

Participants signed up by filling out a demographics questionnaire hosted on Qualtrics where they also self-identified as owning a smart speaker or not, and selecting a suitable time for the interview. Of the 26 people who signed up, 19 scheduled and completed an interview and were compensated with £10 in cash. To limit participant priming, the words "privacy" and "risk" were not used in any of the advertisements. The questionnaire also avoided them with the exception of Westin's Privacy Index questions [36]. We are aware of the lack of correlation between Westin categories and the actual behaviour of participants [64], however, decided to use Westin's privacy scale for simplicity to get a broad sense of our participants' general privacy attitudes, which we can gain from their responses towards the three questions.

4.2 Participants

Of the 19 participants, 9 identified as female, 8 as male, one as non-binary, and one as agender. Their ages ranged from 20 to 34 years old, with an average of ~26 years. Fifteen were students (mainly Masters or PhD students), three were employed full-time, and one was self-employed. Ten participants held bachelor degrees, six had completed master degrees. One participant self-described as having previously worked in a high tech job involving AI. As expected, most participants were privacy pragmatists. Although not being representative of all IPA users, many of our participants were indeed in shared living arrangements with non-family.

Table 1 shows all participants, their self-identification as owning or not, and what devices they had interacted with. Eleven participants had interacted with an Amazon Echo, six participants with a Google Home and two with both. The popularity of the Echo makes sense since it has been on the market the longest.

4.3 Interview Protocol

All 19 interviews were conducted by the lead researcher in the UK with sessions lasting between 40 and 65 minutes. We stopped hearing new themes after the 15th participant but interviewed four more for certainty. The themes were similar for owners and visitors, so saturation was reached for all groups. The protocol was the same for all participants. Appendix A provides a detailed list of the primary interview questions and scenarios.

The session was composed of five parts which engage participants in a combination of question answering, drawing, and free listing. We began with *informed consent*, including permission to audio record. Consent avoided the terms "privacy", "security", and "risk" while still being clear that we were interested in their experiences and understanding of smart speakers. We then asked questions about their *prior interactions* with IPAs including what kinds of devices, types of interactions, and how they came into contact with them. We also asked them to recall a recent interaction with a smart speaker and draw the room the interaction occurred in. The drawing task was partially

	ID	Smart Speaker	Identification as Owner	Device Location	Account Holder	Non-Owner Interactions
Acc. Own.	**AO3**	Google Home	Owner	Bedroom	-	Twice
	AO9	Google Home	Owner†	Kitchen	-	Regular
	AO17	Google Home	Owner†	Bedroom	-	None
	AO19	Amazon Echo	Owner†	Living Room	-	Regular
Resident Owners	**RO1**	Amazon Echo	Owner	Kitchen	Father	None
	RO2	Amazon Echo	Owner	Kitchen	Flatmate	Regular
	RO4	Amazon Echo	Owner	Living Room	Father	Rarely
	RO10	Google Home	Not Owner	Living Room	Partner	Twice
	RO11	Amazon Echo	Owner	Kitchen	Flatmate	Rarely
	RO18	Amazon Echo	Owner	Dining Room	Father	Rarely
Visitors	**V5**	Google Home	Not Owner	Shared Office	CEO	Once
	V6	Amazon Echo & Google Home	Not Owner	Living Room	Friends	Often
	V7	Amazon Echo	Not Owner	Living Room	Relatives	Observation
	V8	Amazon Echo	Not Owner	Living Room	Relatives	Extensively††
	V12	Amazon Echo	Not Owner	Living Room	Relatives	Regular††
	V13	Amazon Echo & Google Home	Not Owner	Living room	Parents / Friends	Rarely
	V14	Amazon Echo	Not Owner	Dining Room	Acquaintances	Rarely
	V15	Amazon Echo	Not Owner	Living Room	Friends	Often††
	V16	Google Home	Not Owner	Kitchen	Acquaintances	Observation

Table 1. Almost all owners were gifted their device†. Most visitors were unsure who the exact device owners are, so the general party is indicated. For account owners (AO) and resident owners (RO) we show how often guests interacted with their devices and for visitors (V) we indicate how often they had interacted with the IPA during their stay††.

intended to get them thinking about a specific past interaction and used to drawing. For visitors we also enquired about their reaction when becoming aware of the device in the room.

By using and interacting with a complex system, users form a model of how the system works, which is plausible to them and allows them to reason about it. This representation is called a *mental model* and depends on the user's technical knowledge and experience with such systems [22, 49, 71]. To understand their mental models, we presented participants with *three scenarios* described below, which were selected based on the results of Abdi et al. who identified four categories of use cases for smart speakers [1]. We excluded the category of "shopping" given our focus on visitors and because of prior work, which shows that the shopping feature is rarely used even by owners [1, 7]. We therefore deemed it unlikely that a visitor would use a feature that even owners use rarely. The three scenarios were:

(1) **Built-In.** Services provided by Google or Amazon, such as weather forecasts, music from the provider's own service, creating lists, and calendar entries.
Task: *get tomorrow's weather forecast.*
(2) **Third Party.** Services provided by external third parties. These can range from well recognised companies like Spotify (music) to individual developer services.
Task: *play a specific song from Spotify.*

(3) **Smart Home Device.** Services provided by third parties to control smart home devices such as light bulbs, thermostats, and coffee machines [4, 24].
Task: *turn on a light in the living room.*

For each of the above scenarios, we asked participants to imagine asking the smart speaker to perform the task. If the participant had never heard of the feature before, an example interaction was presented as a hint. Resident owners and visitors required examples for the light scenario and in some cases even for Spotify.

We then asked them to draw the underlying processes that happen when the smart speaker engages in the task and talk us through. This type of drawing exercise has been previously used to draw smart home systems [67], data flows [59], and smart speaker architectures [30].

Next, the participant was asked to engage in a *free listing* exercise, naming all the parties or people who were involved in the interaction and could potentially record that it happened. Brewer and Ryan recommend free listing as a suitable method to gain insight into a participant's understanding of a domain and learn more about their categorisation [8, 55]. When they were done with listing, we asked them about how these parties are involved and what they would see. If the participant brought up any perceived threats, benefits, or mitigation strategies, the interviewer would ask clarifying questions. To avoid a bias, we only used the term 'privacy' once the participants themselves mentioned it.

The last part of the interview focused on their *comfort and acceptance* of smart speakers located in shared spaces. Here we aimed to understand the extent smart speakers were accepted in shared spaces and what privacy boundaries exist in regards to smart speakers. We concluded the session with a short debrief of the participants, where we answered questions that they had off-record.

4.4 Data Analysis

Analysis was done in several phases. As a first pass, the lead researcher, who also conducted the interviews, used NVivo to open code the interview audio. Then they met with the research team and discussed the codes in relation to their research questions. Some codes were then combined such as trust and protection mechanisms. The research team decided to focus further qualitative analysis on the following main points: 1) context of interactions 2) mental models of device interaction 3) concerns and protections 4) social norms. Two coders then focused on these points as described in the paragraphs below. To ensure consistent interpretation, coders discussed their codes and memos after every two interviews. After two such iterations, their interpretations were similar and no further adjustments to codes and definitions were made. The lead researcher then coded all remaining interviews and the second researcher coded 2/3 of them. The research team created affinity diagrams of the resulting codes to determine more detailed themes for concerns, protections, and social norms.

Interaction context. Analysis focused on how participants obtained or learned about the devices they interact with, including how they saw themselves (owner vs. visitor). Answer ranges were fairly narrow. So the two researchers agreed on a code book, and individually coded it.

Mental models. Our choice of scenarios represents a varying level of data being transferred outside the local network to other parties. Thus, after reviewing all the drawing and free lists, the research team decided on three categories based on who the data was shared with: 1) in-home only 2) provider and Spotify only (Spotify scenario) 3) third parties. Two researchers then went through the drawings and audio and assigned each participant to one of the three categories. The free lists were analysed separately. Disagreements were handled by discussion.

Concerns and protections. Two researchers open coded the sections of the audio where participants discuss issues of concerns, risks, threats, strategies, and potential protections. As

	Account Holder		Not Account Holder	
	Bought	**Gifted**	**Shared**	**Espied**
Reported as Owning	1	3	5	-
Reported as Not Owning	-	-	1	9

Table 2. Count of self-identification compared with how they gained access to the IPA. *Bought* and *gifted* users legally own the device and typically have control of the account. *Shared* users regularly access a device in a shared space, and *espied* users encountered a device that they do not use regularly.

stated above, they discussed definitions for the first four interviews, in particular what constituted concerns or protections, then open coded the remaining interviews with 2/3 overlap. The research team then constructed an affinity diagram using the open codes. Through sorting and discussion, these were then clustered into themes.

Social norms. This analysis followed the exact same process as concerns and protections.

5 RESULTS

We investigated the system understanding, concerns, and protection strategies of in-house users and visitors of IPAs. We compared their perceived social rules when sharing and visiting IPAs. The numbers mentioned below are provided only to illustrate how often certain themes occurred in our sample. We refer to participants by their ID from Table 1. Generally, we found that in-house users and visitors have similar privacy concerns and attitudes, opposed to prior work [37, 38]

5.1 Device Usage and Encounters

Most participants used both built-in and third party skills such as fact requests or music playback. Two visitors reported playing a trivia game with the owners and two other visitors did not interact with the device at all but observed the owner using skills. Confirming prior work [7, 19, 37], account and resident owners reported using the device for built-in features such as cooking timers, weather requests, and alarm clocks. None of the participants used their speaker for shopping.

AO17 explained that they enjoy Google Home's "Good Night, Google" feature as it combines actions such as setting the alarm clock, checking the weather for the next day, and playing soothing rain sounds for falling asleep. Only AO3 used their Google Home to control smart lights that they had bought and set up in their bedroom. Half of the in-house users mentioned a change in their daily routines since getting a smart speaker such as relying on its timers for cooking or being able to retrieve facts using their voice as was also found by Ammari et al. [7].

Device Location. Most smart speakers were placed in a main living space such as a kitchen or living room where occupants spend a great deal of time and welcomed guests, which was expected as already shown in prior research [19, 37]. Two owners kept their device in their bedroom as they use it to play music in the morning when getting up. Consequently, most visitors also encountered smart speakers in shared living areas in places they did not frequent often, such as a friend's or family member's house. The shared nature of the space naturally brought up issues of awareness of the device, who got to decide if it would be added, and what spaces were considered acceptable for IPAs to occupy.

Reactions. Half of visitors encountered or interacted with devices located in prominent places, such as in a shelf or near the television, where it could immediately be seen by anyone visiting the space. When not placed in an obvious space, visitors described becoming aware of the device when the owners interact with it over the course of their stay. V13 describes visiting their parents:

"*I think I was just around one time after they got it. They just randomly said 'Alexa' and it just picked up*". The usual visitor reaction was excitement and curiosity as they had not seen or interacted with smart speakers before. V14 says: "*I guess I was a bit excited. I haven't used it before and it seemed sort of cool to me*". In contrast, three visitors mentioned annoyance rather than enthusiasm and were disinclined to interact with the device. For example, V5's reaction when the speaker was installed in their office was: "*It was just there one day, so I was like 'Oh, okay, great. Now all of our conversations are recorded.' [..] That's why I don't use this stuff*".

Interestingly, none of the participants mentioned either telling a visitor about an IPA, or being told about the IPA by an owner. Although, two visitors did explain that their visit was planned to "meet" the owner's new device. Devices were also sometimes hidden. RO1 stated that their visitors are kept unaware of their IPA due to its position in the room. As a visitor, V16 wondered whether the notification responsibility should be with the manufacturer or the owner: "*It's difficult. Is it the job of Amazon and Alexa to say it will collect the data of the people around you or is it the role of the consumer to be responsible to say 'oh I have this in my house and it will pick up on things'? I don't know who the responsibility necessarily lies with*".

5.2 Adoption and Ownership

For this study, we allowed participants to self-identify as owning the device or not (See Table 1). However, we found that the difference between ownership and visiting was often not binary (See Table 2) as suggested by the complex relationships in a home [21]. Only one participant (AO3) both purchased and setup their own device. More common was receiving the device as a gift or having someone else purchase and setup the device in a common shared space. Interestingly, participants viewed themselves as owners of shared devices even if they had no login access to the associated account. RO1 explains: "*My Dad bought it for my Mum. [...] But everyone loves it. [...] It's linked to my Spotify account [..] because I have Spotify Premium"* and it is a "*Family Alexa*". The notion of "family devices" in multi-user smart homes was found by Garg and Moreno [19].

Two participants showed irritation when a smart speaker was placed into their shared living space. RO2 explains how they became aware of their device: "*We were sat in the kitchen, having dinner one night and suddenly it turned on. We hadn't said anything, but it just turned on and music started playing from it. But it was actually our other flatmate who turned her Spotify on that was connected to Alexa. We were like 'Whoa, that's weird' and asked her. I was like 'I don't want one in the kitchen. You should have asked before you put it there.' [Why?] Because I hear all the rumours that they are listening to you. Not that I am doing anything wrong, but I don't want someone listening to my conversations. But then it turned into a kind of joke that she is listening to our conversations*" and "*now we all use it*". RO2 expressed growing fond of it and feeling like an owner themselves. When RO10's partner bought and placed the device into their living room without consultation, they said "*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*". RO10 continued to voice discomfort around the IPA in their living room and did not consider themselves an owner even though the device was located in their shared living room. AO9 and AO19 who set up their gifted speaker in a shared space did not mention having any tensions with their cohabitants in regards to the location, however, also did not talk about it with their cohabitants. This behaviour reflects findings by Geeng and Roesner showing tensions around a lack of consultation [21].

Acceptable Spaces. We found a divide between shared and private spaces as a boundary for being comfortable encountering a smart speaker. Except for V7, who felt uncomfortable in any space with an IPA unless clearly advertised as such with promises not to use the data and V12, who would feel comfortable if they did not have to pay for the service. Generally, smart speakers were more

accepted in shared spaces than private ones. Areas like an office, where people might normally filter what they say and where in the case of a privacy breach everyone would be impacted. University or shared living spaces were mentioned as acceptable as well as areas that were not used very often. On the other hand, participants showed a clear dislike of encountering smart speakers in private areas such as the bedroom, bathroom, or a hotel or guest room as they did not know "*who else is listening*" (V16). Further, some participants expressed not wanting to have a smart speaker in a productive environment such as a work place or classroom as it is an entertainment device and could distract from important work. As a business owner, AO19 says: "*I wouldn't have it in a work environment, not because I'd be afraid of Alexa listening in to anything particular, but more it's an entertainment product and it shouldn't really be used in work environments*".

5.3 Smart Speaker Interaction Etiquette

We asked all participants how comfortable they would be interacting with another person's smart speaker and what kind of visitor interaction they would find acceptable with a device they owned or might potentially own. We found no difference in the expected social behaviour between groups except that account and resident owners seemed more careful with permissions.

5.3.1 Being an Owner. None of the participants were uncomfortable with a visitor using their IPA, but half the participants wanted to be able to limit the commands available to guests. RO11, for example, "*wouldn't want them to change the temperature [or] open locked doors*".

No Restriction. Nearly half of each group explained that they "*do not really have any restrictions*" (AO17) for what visitors are allowed to do as they were curious what visitors would use IPAs for or did not believe that anything could go wrong. Similar to prior work, we saw limited concerns regarding other users [42]. Two visitors would not put any restrictions despite being aware that their unique user experience might be affected.

Basic Entertainment. Most other participants found it difficult to express what acceptable behaviour was. "*Basic entertainment*" functions such as asking facts, playing music or changing the TV channel were considered acceptable. However, as the owner of the device, participants would not feel comfortable for visitors to change home settings such as temperature or blinds, requesting personal information, or use it at all in a private room. RO11 hoped that their device does not allow visitors to delete their account, update their information or make purchases.

Tensions. We also found tensions or potential for discomfort when sharing devices in line with Geeng and Roesner's findings on tensions arising from mismatched expectations in multi-user smart homes [21]. AO3 described a situation where a flatmate accidentally connected to AO3's device and played back their horror movie audio in AO3's bedroom. The incident happened because the IPA default allowed audio playback from Google Chromecast on the same local network. It took AO3 a long time to understand why their device made noises and how to stop it. This situation made AO3 deeply uncomfortable, saying: "*It made both of us uncomfortable. [My flatmate is] quite embarrassed. I am also quite embarrassed. Although we are friends, and that's fine. But still, that's unintended sharing. Even as friends and family, we do not share everything. We have a boundary and we do not want Google to cross that boundary*". In another example, RO2 describes being annoyed when visitors interact rudely with their device and telling them off: "*I can be snappy with it cause she is in my flat but you cannot be snappy, say thank you*".

And AO19 explains they would be uncomfortable if a visitor requested inappropriate services such as "*a racist joke*" or do anything criminal. V12 and V8 mentioned that access control and authentication would avoid some of these tensions and make them more comfortable as both owner

Scenario	Weather		Spotify		Light	
	O	V	O	V	O	V
Third-Parties	10	9	3	5	1	3
Provider and Spotify	-	-	6	5	-	-
In-Home	-	-	-	-	8	7

Table 3. Categorisation of visitors'(V) and owners'(O) drawings and descriptions for the three scenarios.

and guest of smart speaker in shared spaces. We, however, cannot confirm prior findings of owners being concerned with data sharing with co-users or visitors [30].

5.3.2 Being a Visitor. Participants had divided opinions about interacting with other peoples' smart speakers. Visitors were more hesitant for their own protection while account and resident owners felt uncomfortable as they did not want to disrespect the other owner's property.

Basic Entertainment. Over half of the participants were comfortable interacting with another person's smart speaker for basic entertainment services just as they would be happy for their own visitors to do. For other participants, their willingness depended on permission or the social situation. V16 explained not having interacted with the device at all because of the social dynamics of visiting a friends' parents and the need to be polite.

Permission. We found permissions emerged as a stronger theme for in-house users than visitors. Three account and resident owners expressed reluctance in engaging with another person's smart speaker for fear of being intrusive and rude. They compared interacting with another owner's smart speaker to a violation of existing social norms such using their phone. AO19 explains their discomfort: "*At the end of the day it's their machine and I think if you start using it to whatever thing you want, it's a bit rude. If you ask them 'Can I see what the news is?' then that's fine. But I wouldn't feel comfortable just going in and saying 'Alexa tell me this or tell me that' without asking first. I don't know why exactly, but it's almost like going into someone's house and helping yourself to their cupboards and grabbing their food. At the end of the day it's their property. You can obviously share it, but it's theirs and if they don't give you permission, you shouldn't really be using it*". RO18 agreed that "*if it's not my gadget, it's not my gadget*" and stayed away from another person's property unless permitted.

Own Protection. Four visitors described being uncomfortable using the device for anything personal such as health related queries or making calls as they would feel uncomfortable with the owner or bystanders having a record of the interaction. V15 says: "*I guess I would not ask it to make phone calls for me with close friends. [...] And I would not use it for purchases as it is quite personal*". V7 said they were uncomfortable just being around IPAs: "*I don't like that someone is listening to me. Yes, I just asked it to do a simple function, but at the same time, my voice has been recorded. It knows a bit about me already*". They would not interact for fear of an external party listening into their private conversations.

5.4 System Understanding and Awareness of Third Parties

Generally, we observed that all users had a limited understanding of how smart speakers work which has also been found by prior work [1, 30, 37, 59, 67, 69, 70]. Our participants show critical misconceptions and missed security risks such as the involvement of third parties or how accounts are shared [30, 37, 45]. We asked participants to draw and describe what the IPA does in each of three scenarios (weather, Spotify, light bulb) which were then assigned to one of three categories

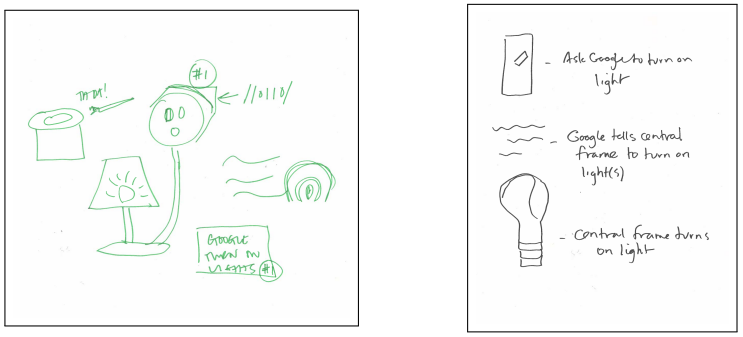


Fig. 2. Drawings of participants AO17 (left) and AO9 (right) for the scenario of turning on a smart light in the room. Both participants own a Google Home. (Images cropped.)

depending on the involvement of third parties (See Table 3). We also had them free list entities that might know about the interaction.

For the weather scenario, all participants recognised that a third party must be involved, typically the group providing the weather data. They expected their IPA to search the internet and draw data from weather providers like 'Metoffice' or 'BBC' just as they would do themselves. However, during free listing they also included groups like other people in the room (bystander), the provider (Alexa, Google), as well as the provider's staff.

The Spotify scenario was similar with all participants being aware that a third party would be involved, contrasting findings by Abdi et al. [1]. However, they were more divided on if Spotify was the only third party, or if there were others. Some participants believed that their IPA connects to the Spotify App on another device, while others thought that it requested the song directly from Spotify. During free listing, participants included bystanders and the provider, but they also included music artists, Spotify third parties, and advertisers, expecting them to play a role in the request for statistics and advertisements, respectively. Interestingly, none of these groups were included in the drawings, suggesting that participants are aware of potential third party sharing, but are not clear on how it happens as part of a specific action like playing a song. When describing the IPA actions in this scenario, RO2 was surprised when they realised that the music they requested from their shared device was played from the account holder's Spotify and not their own account, even when it was them requesting it.

For the light bulb scenario, most participants thought that the interaction happened entirely within the home, as found previously [1]. They thought that the IPA connected to the light switches or central wiring via Bluetooth or directly through their home network, as AO9 and AO17's sketches show in Figure 2. Because the connection was seen as direct, they did not believe that any third parties were involved. The free listing showed a similar result, with third parties rarely mentioned.

When V13 was asked to do free listing for the light bulb, they said: "*that surely shouldn't be too much*" and then named the IPA provider, people in the room, and the electricity provider who can observe the energy being used. The light bulb manufacturer was only mentioned by five participants in free listing, and only two of them included it in their drawing. Similar to the Spotify scenario, some participants seemed aware that such sharing was possible but did not see how it fit into a typical interaction.

5.5 Concerns and Benefits

The collection and use of data was a common point of concern which is in line with prior work [1, 30, 37, 46, 59, 67, 70]. There was also a strong sense of feeling uninformed about how the device worked, making it challenging to know what they should be concerned about.

5.5.1 Data Collection. Participants were aware that the device provider was likely recording their interaction data, including their requests and audio recording; however, only a few brought up the request history which stands in contrast to Ammari et al. [7], but is in line with other work [19, 21]. Roughly half the participants also acknowledged the need for involving third parties in order to provide services. For example, a weather service might need to be contacted to retrieve the weather. For those aware of third parties, we asked what a third party with access to requests could learn about users. Participants mentioned: daily routines, habits, and music preferences similar to [59]. They were also aware that using features like shopping or smart light bulbs might allow the associated parties to know information like what they shopped for or when they were home.

Monitoring. A consistent concern emerging in most interviews and in prior work [7, 20, 30, 37, 42] was that the device is always recording. Almost all visitors and half of in-house users were sure that a smart speaker "*hears everything that people actually say*" (RO10) and is "*spying on everyone*" (RO1). Two owners were not sure whether it is listening when not activated through a wake word, but AO19 was convinced that their device always listens out for keywords. A main concern was that the device will intrude on private conversations. For V16 "*it crosses a line that they could be listening and could potentially see what you do*". Whereas V7 was concerned that they as a user do not know exactly "*who else is monitoring, listening*" and that "*there isn't any sort of privacy anymore without big brother listening*". V13 wonders "*if it is listening all the time where is that information, the data that it has got*" and whether "*people [can] tap into people's Alexa*", eavesdropping on their conversations. Our results show that participants felt uncomfortable with potential audio recording and the uncertainty of what happens with the data.

5.5.2 Data Use. Both groups showed an equal understanding that their data is used to improve their services, but also expressed a concern about not knowing what exactly their data is being used for beyond that. Concerns about data use have also been found in prior work [30, 44, 59]. Our participants showed the general trend of projecting their experience in social media on smart IPAs as also seen in Tabassum et al. [59]. For example, RO11 says that "*If I put something out online, I understand that it's going to come back to me in some sort of Facebook ad*".

Improve and Provide Services. When asked about why certain parties have access to the interaction, all participants agreed that they require access to improve the services or fulfil the request. As the provider of RO1's speaker, "*Amazon is listening in, checking that it's all working*". And V13 understands that the speaker "*must be listening all the time or it would not know when you said the [wake] word*". In detail, they mentioned that the data is used for customer feedback, trouble shooting, market research, and improving voice recognition. This purpose was accepted by most participants and seen as a beneficial use of their data as it improved their interaction. V7 found it acceptable as long as it is only used to improve their own user experience while RO10 did not want humans to be involved in the process: "*I'm perfectly alright with that [...] provided this data is fed into a machine and it's not being manually reviewed by some person at the other end. [Where is the boundary?] I think if humans are interacting with it and can see you, see what you do, that's where the boundary is. [...] I am not concerned that it has gone through a machine. But I [will be] with the human element, because that brings in the element of self-disclosure to a person I don't want to disclose to*".

Targeted Advertisements. All participants also mentioned tailored ads as a use for their data as was found in related work [1, 30, 37, 59, 62]. Most participants acknowledged the benefits of this kind of personalisation in how it can improve their user experience and help them find features and elements they like. AO3 explains that the provider earns money through ads and can thus offer their services and devices cheaply: "*There must be an incentive for them to [cut prices for smart speakers]. So they have to sell you something through their services or collect your data to sell you other services or other users*". Conversely, and similar to Ur et al.'s work on behavioural advertisements [62], targeted ads were often mentioned as a "*negative side of the data*" (RO10) as they pose privacy risks and require a lot of personal information, but users are not told what data exactly. All user groups mentioned the dangers of manipulating peoples' opinions and attitudes or buying decisions. RO11 explained that showing certain content only to a group of people can manipulate what people think and create unequal opportunities. Similarly, AO9 felt that personalisation restricted his exploration options and "*has the potential to [push people into decisions] without giving them the full information*".

Selling Data. Another use mentioned by all participants equally is sharing data with third-parties as a benefit for the company. According to RO18 the provider "*can sell that information to whoever wants to buy it*" and "*would pay a lot of money*" (V14). They believe that there are "*legal ways of selling*" (V16) data, i.e. sharing data with other parties in return for other data instead of money, as they believe that the actual act of selling data is prohibited. This concern was also found by Huang et al. [30]. RO11 was fine with it as long as no sensitive information was shared.

5.5.3 Dangers of Data Access. The mentioned risks of unexpected data access showed no significant differences between visitors, account owners, and resident owners and is in line with worries found in other work [1, 7, 37, 45]. 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. Leaked data can also be linked between different accounts, which would lead to a much more detailed level of personal information. The data holders could use it for better targeted ads. V16 is convinced that "*Facebook and Amazon probably do work together because they are huge, multi-pound businesses and can both thrive from the data they collect and share with each other*". Almost all participants mentioned a risk of financial and physical harm such as credit card fraud or identity theft if this data ends up in the wrong hands. AO19 explains that knowledge of the owner's whereabouts or holiday plans can help burglars to find the right moment to break in.

5.6 Protection Mechanisms

In general, our data shows that both groups feel uncertain of how to protect themselves. This finding is in line with other work that shows that smart home owners feel unable to protect themselves as they are unaware of existing protection mechanisms [1, 19, 21, 30]. Instead, they rely on traditional strategies for the web and external protections. Themes of avoidance and acceptance emerged strongly for both groups. Except the ability to turn off the device and not use it, they express feeling powerless and without an option to protect their data. Existing protection strategies such as voice recognition or the addition of multiple accounts were not mentioned by our participants.

5.6.1 Traditional Safe Browsing Advice. When asked about what they actively do to protect themselves from unwanted data access, the replies suggest that three participants of each group consider smart speakers as part of their general internet usage. Their protection strategies corresponded to traditional online protection advice such as not sharing, saving or writing down bank details or using different passwords. This finding corresponds to what non-advanced users mentioned as protection strategies in Tabassum et al.'s study on data perceptions of smart home users [59].

Primarily visitors also mentioned staying away from data collecting services or devices in general and avoiding giving unnecessary information.

5.6.2 Informed Consent. We found two notions of informed consent: the need to (1) inform guests about the device and (2) understand the policies accepted as part of device setup.

(1) Informing Guests. A small number of participants expressed the importance of being made aware of smart speakers. V7, who expressed clear discomfort around smart speakers explained they wish for clear warnings for areas with data-collecting devices. Although not concerned themselves, V16 mentioned why visitors should be informed about existing devices: "*As I am quite relaxed about my data, and I probably shouldn't be this relaxed, I am fine [for IPAs to learn facts about me]. [...] But, even if it's not a product that you own, just being in the same space with it, it can pick up details about you. I think, in abstract that is quite a distressing thing, because you haven't necessarily consented to have your data collected in the same way if you had your own speaker and speaking to it, you know it's collecting data*". However, they could not tell us who they find responsible for delivering the information: the provider or the owner.

(2) Transparency of Policies. Most participants mentioned a lack of knowledge of what is happening with their data and that they were not given a chance to give informed consent. Some participants felt that it is the provider's responsibility to ensure that information on data collection and use is understood by their users and that they have failed to be transparent enough. V16 explained that "*Amazon should make people aware of how and who and what data they are collecting*" to allow people to make an informed decision of whether to use their service. RO10 expressed being uncomfortable finding out about their phone's IPA request history: "*I am not too certain about how google uses our information and [..] I didn't know that it actually has all your voice recordings. I remember going online and it actually had an entire section with all the times I've asked it questions. And I was like, at what point did I agree to my voice recordings being kept, stored online. Once I discovered that, I remember deleting all the clips and not using it again*". They explained that their reaction would have been different had they known about it, but "*I do not know that [the provider is] doing this and [they] did not make this absolutely clear*". Not only in the context of smart speakers, but service providers in general, all groups felt like they have not consented to certain uses of their data, in V12 words "*everything is being used for more than the reason it should be used for*".

Many of these participants agreed that learning more about data handling and "*educat[ing] ourselves*" (AO9) will allow them to protect themselves better. Most mentioned reading privacy policies and terms of service as a source of information "*because then [they] would know what the protection were and were not*" (RO11). AO9 said "*I need to be an informed citizen and read [privacy policies] to know where my data is going and how it's being used*". However, most also reported simply scrolling to the bottom and accepting privacy policies for any kind of service as it "*too long*" (RO11) or not understandable. As a lawyer, RO10 explained that terms and conditions are legal documents and difficult to understand for lay people. Only AO3 claimed to have read these documents before using their speaker and notes that this kind of behaviour is expected from companies: "*In many times it's not that they didn't tell you. They did tell you, but they didn't expect you to read. I'm pretty sure I can tell from the language they used*" (AO3). Thus, our participants mentioned similar difficulties with understanding policies as smart speaker owners in Huang et al. and Abdi et al. [1, 30]. We can clearly see a tension between understanding available information and giving consent. Generally users expressed being kept in the dark about what is happening to their data by the provider, not given an option to agree or disagree. RO10 said they "*would be fine with all of this, had [they] accepted this*".

5.6.3 Limiting Usage or Avoidance. When asked about how people can protect themselves from smart speaker risks, most participants straight away mentioned turning off the device or limiting their usage. Avoidance has been found as a tactic for both IPAs and smart homes [1, 19, 20, 30, 59]. V7 stated that"*turn[ing] off the device [...] help[s] to give some privacy*". RO2 as a flatmate felt that they have the control "*I have a choice not to interact with it. I have the choice to turn my phone off and leave it somewhere. It's the same with Alexa. I don't need her in my life*". In contrast to account owners and resident owners, who mainly expressed how any risk mitigation strategy defeats the purpose of having a smart speaker, visitors mentioned the general difficulty to opt out of any web services with whose data policy they disagree with. They saw a tension between protection and the convenience of these services. V12 expressed that "*they made a system in which you have to agree for them to use the information*", so choosing protection blocks access to this service.

5.6.4 Trust in External Protections. We found that half of the participants in each group relied on external protection by the government, the service provider, or financial institutions. In contrast to existing work done in the US [7, 37], we not only see account owners, but also resident owners and some visitors expressing their trust in external groups. The higher confidence shown by our participants in the UK may have also been influenced by people's higher awareness of data protection laws due to thorough media coverage of GDPR going into effect in 2018. Unsurprisingly, the first, most often mentioned external protection were data protection laws which "*force companies to have more disclosure*" (RO10) and "*be more careful and responsible with data*" (V4). However, four participants also criticised that these laws are not imposed strictly enough and companies have good legal teams and are not transparent on their data use. Many agree with V14 who explained that "*if you are willing to give that much data to a large company, then they have to protect you*". They found that the responsibility of user protection lies with the provider to have enough protections in place such as authentication and anonymisation to keep their data safe. Two visitors hoped their data is anonymised, if shared, as they described it as the most effective protection strategy. Primarily in-house users believed that the providers do their best to protect them and have enough motivation to try and keep data from misuse as any untrustworthy action would come out and cause a loss of consumers or high fines. However, some also expected that the provider's protection may not be absolute and if a party wanted access to their data "*they will find a way*" (AO17). Another participant also mentioned to rely on their bank "*to pick up anything wrong*" with their finances (RO2).

5.6.5 Accepting a Lack of Options. Among all protections, acceptance emerged as a main coping mechanisms for all groups in regards to smart speakers, but also other web-based services.

Powerlessness. The strongest theme emerging from all mentioned protections strategies is that most participants acknowledged the lack of control over their data when using smart speakers or web services in general. They described feeling powerless and helpless as did participants in Huang et al.'s study [30]. "*It's very disempowering, not having the power over your information*", said RO10. V12 explained "*I do feel like we have no longer control over our data*". Many participants, especially in-house users, did not see opting out as an option if they wanted to use the service. V13 expressed with resignation that one "*need[s] to give away at least a bit of control to them*" to be able to have the convenience. RO1 said that "*you have an option, but it's not really an option*". One needs "*to be willing to make the trade off*" (RO10), confirming prior work on the acceptance of risks as a trade-off [37, 59]. The concept of our participants' helplessness and acceptance has been more generally discussed for digital entities under the term 'digital resignation' [16].

Control Imbalance. We can see that some visitors acknowledged the lack of options, but felt rather uncomfortable with it. Referring to their position as visitors or resident owners, participants had to

accept the IPA and all risks as they had no other option. For example, RO10 explains "*I don't [have the control], because I didn't put it there. It's not something I chose to put in my life and it's something that is potentially taking my data without my consent as I actually did not agree to the terms of service as I am not the one who set it up, which I think is a very interesting conundrum. I mean, implicitly I agreed to this because I have not removed it, but that's the situation in shared living arrangement. I think some of these nuances are lost in the law*". RO10 described an imbalance of control towards the owner because they are bound by the decision their partner made. In connection with the theme of informed consent for visitors, we find the need to include visitors and cohabitants in the user base of smart speakers.

Acceptance. Similar to prior work [30, 37, 59], we saw many participants accepting the situation by not worrying about their data or taking no precautions. V16 viewed their life as "*incredibly mundane*" and were "*very relaxed about it, maybe because [they] don't know the extent of how much our data is being shared*" whereas AO17 said "*I've got nothing to hide, so I've got nothing to worry about*". Four in-house users stated that they "*don't do anything*" (AO19) about it and that no matter what they do, it would not influence the situation. Some accepted the conditions as "*people still buy Alexas*" (RO2) so "*it can't be that bad*" (RO11).

6 DISCUSSION

6.1 System Understanding, Concerns, and Protections

Prior work has heavily explored concepts around system understanding, concerns, and available protections, our work confirms and expands on many of these findings.

Ownership, gifting, and system understanding. Prior research has shown that users have incomplete or incorrect knowledge of how smart home devices work [1, 30, 37, 59, 67, 69, 70]. Particularly with regards to third-party interactions [1]. Likewise, our work shows that visitors have similar misconceptions to other users groups, as do people who regularly interact with these devices.

In our study, several device owners used the device only because someone else had given it to them as a gift, meaning that they had not proactively sought out the device and decided to include it in their home. Prior work has primarily compared home residents to smart home "drivers" who actively want the devices, drive their adoption, and are also often in charge of managing other home technology [21, 37]. Typically these drivers might be considered similar to technology early-adopters in that they are enthusiastic about the technology and are willing to spend more time on setup and maintenance of it resulting in a more detailed mental model than other home residents [21, 37]. By comparison, our owners who received the device as a gift and setup the device seemed to have about the same level of understanding as visitors and people who regularly use the device, but were not part of the setup process. Our results compared with related work suggest that device setup is not sufficient to gain an understanding of its functions and that driver-style users are likely gaining much of their understanding from interactions outwith of the normal setup and usage processes.

We observed that participants recognised the need for third party involvement in situations where they themselves would have to involve a third party to complete the action, such as playing a song on Spotify or searching for the weather. But thought that no third party would be involved in an entirely in-home action like turning on a light switch. They were also cognisant that these third party interactions might result in their data being used for purposes like targeted advertising and marketing, though they strongly disagreed with that usage. This result ties in with concerns about data collection, use, and storage as also found for smart home users by Tabassum et al. [59]. The awareness of these third parties is a positive observation especially given that prior work has

found low awareness of their involvement [1]. However, as we discuss in the following paragraphs, that awareness may be unhelpful due to the lack of ability to act on concerns or use protections.

Concerns, trust, and uncertainty. Participants were concerned and uncertain about how their data was being recorded and for what purposes it was being used. Their concerns echo those of prior work [30, 46, 59, 67, 70] and mainly involve external parties. Risks from visitors or flatmates were rarely proactively mentioned, as found before [37, 67], contrasting the findings of Huang et al. [30]. We also observed that participants felt powerless to protect themselves, mentioning issues of a lack of control and transparency [30, 59].

Participants talked about informed consent as a way to manage their concerns and lower uncertainty, though many had not read the privacy policy or terms of service associated with devices they owned or used regularly. When asked why, they discussed concerns about not being able to understand the legal writing properly because it was designed by the companies to be confusing and not favour consumers. The results are similar to other works on how privacy policies are not providing details in an understandable format [51, 53] and give no options to opt out of specific aspects of data usage. The attitude that reading official documentation from IPA providers would not help inform concerns or reduce uncertainty is of particular concern. It suggests a lack of perceived ability to read and understand a document whose primary purpose is to provide informed consent. It also suggests a lack of trust in providers to tell consumers the truth about their actions. Considering that our study was conducted in the UK after GDPR went into effect, it also suggests that the regulation is not helping consumers gain proper informed consent for the usage of their data, even if they are direct owners of the device. The situation for visitors is even worse as they have less access to information sources and often do not even realise that a device is present. In none of the situations mentioned by our participants were visitors informed about an IPA in the room much less given any control options. Owners' unawareness of guests' need to be informed limits informed consent options.

Protections. The providers of IPAs do indeed provide a number of protections, which address concerns and risks around monitoring, data handling, and access control. All smart speakers come with a mute options that can be activated through voice request or by pressing a dedicated button, resulting in the device not reacting to any requests until the mute mode is turned off via button press. Also, IPAs offer the option of creating voice profiles and adding multiple accounts [3, 26]. When voice profiles are set up, private information like notifications and calendars can only be accessed by the authorised person. Users are given the option to view and delete voice recordings from the device history. During the set up of both Google Home and Amazon Echo this feature is mentioned multiple times, which is likely the reason that it is more known by owners than co-users.

Many of our participants were not aware of these existing protections, and thus, mainly mentioned avoidance or acceptance, protection strategies also found in prior work [30, 67]. Their lack of knowledge on how to protect themselves seems to be interconnected with their limited understanding of how the system works, but also how devices are being shared [30, 45]. An example is RO2's surprise on realising whose Spotify account their music requests are played from. Knowing about this encouraged them to look for a solution. Even regular interactions or a feeling of ownership do not lead to a better understanding of the system, potential risks, or use of available protections.

6.2 Perceived Ownership and Social Dynamics

The concept of device ownership is unsurprisingly complex. While ownership of a specific device like a smartphone or computer might be tied to a particular individual through social norms and classic access control (passwords), an IPA is designed to interact with anyone in vocal range by default, including flatmates, partners, or guests. This seamless interaction makes the device part of

the space itself similar to lighting or chairs and invites for regular interaction. The blending in of IPAs into their surroundings was discussed in prior work under the term 'democratization' [52]. This observation may be one of the reasons many of our participants identified as owning the devices located in their living spaces despite not being the person who legally owned the device and not having access to the accounts linked to the device. Additionally, social relationships vary from one smart home to another. Garg and Moreno mention the concept of "Family devices" [19]. However, we see that these are not exclusively found in family homes, but also in flat shares of younger users, showing a family-like relationship to flatmates and mutual trust in sharing these devices. However, these 'owners' do not have the same amount of control over the device as the account holder. Some of our participants expressed being irritated when an IPA was adopted without their consultation and not having a choice in the matter of adoption. But they still seem to feel that they will be offered the same user experience and level of protections. While we have not investigated this phenomenon in detail, we suggest future work on the effect of frequent exposure to IPAs and other factors, e.g. personification [40], on feelings of ownership.

6.3 Smart Speaker Interaction Etiquette as Access Control

Prior work showed that sharing devices in multi-user smart homes is based on social relationships and sharing rules [19, 21, 34, 65]. We show that not only rules for sharing, but also for guest interaction exist. When asked about being a visitor and using another person's IPA, some participants were hesitant for two reasons: 1) fear of being intrusive and 2) their own protection. The first reason was mentioned mainly by account and resident owners who perceived interacting with another person's device without permission as disrespecting their property and intruding on their privacy. Visitors mainly expressed reluctance due to wanting to keep their requests private or not share their voice data. We suggest that this behaviour is influenced by their privacy perceptions, which in turn seem to be influenced by two factors identified by Yao et al.: 1) perceived norms, namely their social relationship to the owner and their perceived trust towards the IPA provider, and 2) their privacy-seeking behaviour of protecting themselves by avoiding the device [65]. Most participants declared they would be comfortable using an IPA for basic entertainment purposes only and owners would find this an acceptable behaviour. Although we had reports of tensions with unexpected behaviour, similar to Geeng and Roesner [21], we see an interesting balance of socially acceptable behaviour and expectations by all groups, careful not to overstep any boundaries and staying polite. Kraemer et al. found that owners balance politeness and security when it comes to sharing with visitors and are mostly happy to accommodate guests' wishes [34]. Mazurek et al. found social rules to function as access control for sharing personal devices such as computers or phones [45]. Building on their research and our findings, we believe that generally, basic entertainment such as playing music or asking for facts is the border for owners and works as such an access control mechanism since these requests do not reveal many personal details, but allow guests enough convenience. The aspect of mutually, unwritten social interaction rules to protect both parties privacy is interesting and exploring which aspects impact the development of such an etiquette is worth looking at in future work.

6.4 Recommendations

Based on our analysis and our discussion, we make the following recommendations to improve how IPAs are shared with guests and co-users in a safe, respectful manner.

6.4.1 Add skills about privacy concern awareness. Our participants were worried about numerous data usage issues. They were also poorly informed about potential protection mechanisms that already exist. IPAs are designed to help users answer questions like "what time is it in London,

UK?", but do not currently have good support for answering questions about the privacy and data usage practices of the device itself. They also lack the ability to make recommendations about how to handle common concerns. These could be built into the setup procedure better as suggested by [37], but doing so would only assist the account owner. Adding these skills to the main device would allow all users easy access as well as a revisit of the information. So, instead of walking the user through the privacy policy in a dialogue format during set up, the IPA offers to answer privacy questions at any time. The device could then truthfully, using lay language, reply to questions like "what data do you share with Spotify?" or "what do you use my voice recordings for?". Such a skill would promote transparency as also suggested by other work [37, 59, 66] and provide accessible information to all users.

6.4.2 Make protecting visitors' privacy easy. Visitors using IPAs was a source of concern for the visitor as well as the account and resident owners as normal IPA functionality includes actions like online purchasing or adjusting settings in the home. Similarly to prior work, we suggest incorporating a way to better support multi-user households and visitors with different modes and privileges [19, 21, 37, 42, 66]. IPAs could come with an adaptable guest mode where the IPA limits its own functionality to ensure that guests cannot make unwanted changes and less data is being collected. Having such a mode is helpful to owners who then do not need to worry about privacy breaches, but it may also help guests feel more confident interacting with the device knowing that socially unacceptable actions have been blocked. Privacy could also be further improved by incorporating additional privacy features like not retaining recordings, flagging any recordings as being recorded in guest mode and therefore possibly without full consent, or setting the device to auto mute or turn off during set time periods.

A guest mode might allow the IPA to provide better transparency while acting in a more fun role. For example, supporting being introduced to a guest. So the host can introduce the IPA and have it respond socially properly, such as host saying "let me introduce you to our Alexa." and Alexa responding by saying hello and providing information about how to interact with it, such as "I'm happy to answer any questions you preface with my name, or you can also ask me to mute". By allowing customisation, the owner will be able to communicate their acceptable behaviour and establish social boundaries. For example, by adjusting the above message to say "I'm happy to play music requests you preface with my name, or you can also ask me to mute" the visitor is informed about which interactions are accepted.

Such a mode can also be extended to include various relationships in the home to give co-users more control over their data and existing protection strategies, as was also suggested by Geeng and Roesner [21] for smart home users and Lau et al. [37] for smart speaker owners. Our suggestion is to encourage the set up of different modes during set up and streamline the process as many of our users were not aware of the existing strategies.

6.4.3 Encourage communication about adoption. We see the need of communication even before the device is set up and in use. Installing IPAs in shared spaces may cause tensions with other people who are using the space such as partners, flatmates or family members. In the beginning of set up, owners should be encouraged to consult with their cohabitants in regards to adoption. The device may, for example, require all co-users to read or listen to a non-expert friendly introduction of the IPA's basic functionalities and protections and collect their consent during set up. Here, the set up process would be paused until all potential other users consented or a solution for any tension was found. At this point, all cohabitants should be aware of the owner's intention to install it and have either agreed or lead a conversation about IPA adoption. Giving co-users the option to voice their concerns, preferences, and expectations towards an IPA in a shared space will allow for informed consent and better control. As part of the co-user introduction, the device may suggest

enabling existing protection mechanisms such as adding multiple accounts and discussing social expectations of sharing these devices.

The activity during set up would entirely be based on trust with the goal to support the kind of consultation with co-users which brings transparency and avoids tensions. However, to follow up and ensure that all cohabitants were informed, the device could listen out for regular voices who have not consented earlier and encourage this user to consent to the device then. Encouraging consultation will help to create a comfortable and respectful environment.

7 LIMITATIONS

The study was conducted and advertised in an academic environment, resulting in participants with an above average level of education and a young average age of ~26. Participants were also predominately students, likely with lower incomes, which may have impacted their device purchasing and adoption choices as well as how they obtained devices. However, our sample of mature students and young professionals is still relevant in the context of shared spaces due to often living in shared households. We see that our participants' opinion may have been impacted by the assistants on their phone, who work very similar. Some even referred to or compared the IPA to the voice assistant on their phone. Since we focus on smart speakers and all of our participants have either interacted with or closely observed another person use a smart smart speaker, we consider the impact onto our results minimal.

The majority of our self-identified owners did not select the device they used. Instead they were gifted it or a flatmate introduced it into a living space. However, the group clearly represents IPA users in shared spaces as the younger age means that many of them were in shared living environments with non-family and use private spaces like bedrooms to host guests. Obtaining the device as a gift also removed financial limitations around attainment. Our study was run with participants resident in the UK. While the impact may be limited, their opinions on data protection may be different compared to participants from other countries. We chose to present the scenarios in a set order for all participants with the weather scenario first and the light last. This decision may have resulted in a learning effect where participants begin the study with a poorly defined mental model of how their device functions and then solidify that model over the course of the study through thinking and discussion with the interviewer. We feel that the impact was minimal and mostly caused participants to more clearly express their understanding of the device's functions.

8 CONCLUSION

With IPAs being increasingly adopted in multi-user homes, not only the person buying and setting up the device, but also any person sharing the space automatically becomes a user. We interviewed 19 participants who encountered, lived with, or owned IPAs and asked them to state whether they own a device or not. Our findings show that the concept of ownership of shared devices is highly complex and someone with regular IPA interaction may feel like an owner, although not having the same rights or controls. Confirming prior work, IPA users have a very limited understanding of an IPA system and third party involvement. Similar for all groups, participants have concerns about how their data is handled and a lack of control and transparency over the data processes. In our study, participants were unaware of a number of available protection mechanisms which could in fact mitigate their worries. The main protection strategies we found were avoiding IPAs or accepting the lack of control. However, a strong desire for informed consent emerged, for both secondary users when visiting or sharing a space and for owners to make an informed purchasing decision. Interviewing participants who encountered IPAs in various settings, we found that a smart speaker interaction etiquette exists, guiding acceptable interaction behaviour with other people's IPA, and providing an unspoken, trust-based access control mechanism. All participants deemed

basic entertainment functions as acceptable behaviour with minor differences. We found tensions caused by non-consultation on adoption and mismatched expectations when sharing devices. Thus, we see the need to establish a framework to integrate the various relationships in a shared smart home and provide a clearer way to match social expectations.

ACKNOWLEDGMENTS

We thank Bettina Nissen and everyone associated with the TULiPS lab for insightful discussions of the results and the study design. We also thank Adam Lopez for his encouragement. This work was supported in part by the UKRI Centre for Doctoral Training in Natural Language Processing (grant EP/S022481/1), an EPSRC DTA award, the University of Edinburgh, and a Google Faculty Research Award.

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 *Fifteenth Symposium on Usable Privacy and Security SOUPS 2019*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/abdi

[2] Abdulaziz Alhadlaq, Jun Tang, Aleksandra Korolova, and Marwan Almaymoni. 2015. Privacy in the Amazon Alexa Skills Ecosystem. (2015). https://www.petsymposium.org/2017/papers/hotpets/amazon-alexa-skills-ecosystem-privacy.pdf

[3] Amazon. [n.d.]. What Are Alexa Voice Profiles? ([n. d.]). https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GYCXKY2AB2QWZT2X

[4] Amazon. 2019. Amazon Alexa. https://developer.amazon.com/alexa

[5] Amazon. 2019. Amazon Alexa - Custom Skills. (2019). https://developer.amazon.com/en-GB/docs/alexa/custom-skills

[6] Amazon.com. 2019. Alexa and Alexa Device Terms. (06 2019). https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201566380

[7] Tawfiq Ammari, Jofish Kaye, Janice Y. Tsai, and Frank Bentley. 2019. Music, Search, and IoT: How people (really) use voice assistants. *ACM Transactions on Computer-Human Interaction* 26, 3 (2019). https://doi.org/10.1145/3311956

[8] Devon D. Brewer. 2002. Techniques to Maximize Output in Free Listing Tasks. *Field Methods* 14, 1 (2 2002), 108–118. https://doi.org/10.1177/1525822X02014001007

[9] Eugene Cho. 2019. Hey Google, Can I Ask You Something in Private? The Effects of Modality and Device in Sensitive Health Information Acquisition from Voice Assistants. In *CHI '19 Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–9. https://doi.org/10.1145/3290605.3300488

[10] Eugene Cho, S Shyam Sundar, Saeed Abdullah, and Nasim Motalebi. 2020. Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers. In *CHI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu, HI, USA, 1–13. https://doi.org/10.1145/3313831.3376551

[11] Soumyadeb Chowdhury, Md Sadek Ferdous, and Joemon M Jose. 2016. Bystander Privacy in Lifelogging. In *British HCI*. BCS Learning and Development Ltd., Bournemouth. https://doi.org/10.14236/EWIC/HCI2016.62

[12] Anthony Cuthbertson. 2019. Google admits workers listen to private audio recordings from Google Home smart speakers. https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-home-smart-speaker-audio-recordings-privacy-voice-spy-a9000616.html

[13] Matt Day, Giles Turner, and Natalia Drozdiak. 2019. Amazon Workers Are Listening to What You Tell Alexa. (04 2019). https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio?srnd=premium

[14] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery, 2377–2386. https://doi.org/10.1145/2556288.2557352

[15] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. 2019. Security - Visible, Yet Unseen?. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, New York, New York, USA, 1–13. https://doi.org/10.1145/3290605.3300835

[16] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New media & society* 21, 8 (2019), 1824–1839.

[17] Jide S Edu, Jose M Such, and Guillermo Suarez-Tangil. 2019. *Smart Home Personal Assistans: A Security and Privacy Review- A Preprint*. Technical Report.

[18] Hayden Field. 2018. Google Home and Amazon Echo Can Store Your Voice Recordings. Here's When They Could Be Used Against You. (Nov. 2018). https://www.entrepreneur.com/article/322896

[19] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interactive Mobible Wearable Ubiquitous Technol* 3, 2 (2019), 1–21. https://doi.org/10.1145/3328915

[20] Radhika Garg and Subhasree Sengupta. 2020. "He Is Just Like Me": A Study of the Long-Term Use of Smart Speakers by Parents and Children. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 1 (3 2020). https://doi.org/10.1145/3381002

[21] Christine Geeng and Franziska Roesner. 2019. Who's in control?: Interactions in multi-user smart homes. In *Conference on Human Factors in Computing Systems - Proceedings*. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300498

[22] Dedre Gentner and Albert L. Stevens. 1983. *Mental Models*. Lawrence Erlbaum Associates Inc. 1–6 pages.

[23] Google. [n.d.]. Google Home. ([n. d.]). https://store.google.com/product/google_home

[24] Google. 2019. Actions on Google. https://developers.google.com/actions/

[25] Google. 2019. Data Security & Privacy on Google Home. (2019). https://support.google.com/googlenest/answer/7072285?hl=en-GB

[26] Google. 2020. Link your voice to your Google Assistant device with Voice Match. (2020). https://support.google.com/assistant/answer/9071681?co=GENIE.Platform%3DAndroid&hl=en-GB

[27] 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

[28] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. (2015). https://doi.org/10.1145/2702123.2702183

[29] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers using Wearable Cameras. (2014). https://doi.org/10.1145/2632048.2632079

[30] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. (2020). https://doi.org/10.1145/3313831.3376529

[31] Andreas Jacobsson and Paul Davidsson. 2015. Towards a model of privacy and security for smart homes. 727–732. https://doi.org/10.1109/WF-IoT.2015.7389144

[32] Dan Jurafsky and James H. Martin. 2009. *Speech and language processing : an introduction to natural language processing, computational linguistics, and speech recognition*. Pearson Prentice Hall. 988 pages. https://dl.acm.org/citation.cfm?id=1214993

[33] Marziah Karch. 2019. Is Your Smart Device Spying on You? (06 2019). https://www.lifewire.com/is-your-smart-device-spying-on-you-4141166

[34] Martin J Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further Exploring Communal Technology Use in Smart Homes: Social Expectations. In *CHI '20 Extended Abstracts*. Honululu, HI, USA. https://doi.org/10.1145/3334480.3382972

[35] Sathish Kumar, Tyler Vealey, and Harshit Srivastava. 2016. *Security in Internet of Things: Challenges, Solutions and Future Directions*. 5772–5781 pages. https://doi.org/10.1109/HICSS.2016.714

[36] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies*. Technical Report. https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

[37] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31. https://doi.org/10.1145/3274371

[38] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2019. Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In *iConference 2019: Information in Contemporary Society*. 102–113. https://pearl.umd.edu/wp-content/uploads/2019/01/Liao_etal-2019-iconference.pdf

[39] 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

[40] Irene Lopatovska and Harriet Williams. 2018. Personification of the Amazon Alexa. *Proceedings of the 2018 Conference on Human Information Interaction&Retrieval - CHIIR '18* (2018), 265–268. https://doi.org/10.1145/3176349.3176868

[41] Ewa Luger and Abigail Sellen. 2016. "Like Having a Really Bad PA". In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. ACM Press, New York, New York, USA, 5286–5297. https://doi.org/10.1145/2858036.2858288

[42] 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. In *Proceedings of Conference on Human Factors in Computing Systems*. Honululu, HI, USA. https://doi.org/10.1145/3313831.3376311

[43] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 4 (2019), 250–271. https://doi.org/10.2478/popets-2019-0068

[44] Lydia Manikonda, Aditya Deotale, and Subbarao Kambhampati. 2018. What's up with Privacy?: User Preferences and Privacy Concerns in Intelligent Personal Assistants. In *AIES 2018 - Proceedings of the 2018 AAAI/ACM Conference on AI,*

Ethics, and Society. Association for Computing Machinery, Inc, 229–235. https://doi.org/10.1145/3278721.3278773

[45] Michelle L Mazurek, J P Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R Ganger, and Michael K Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *CHI'10: Proceedings of the 28th international conference on Human Factors in Computing systems*. https://doi.org/10.1145/1753326.1753421

[46] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, Norman Sadeh, Pardis Emami-Naeini, and Lorrie Faith Cranor. 2017. Privacy Expectations and Preferences in an IoT World. In *Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[47] Helen Fay. Nissenbaum. 2010. *Privacy in context : technology, policy, and the integrity of social life*. Stanford Law Books. 288 pages.

[48] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (6 2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[49] Donald A. Norman. 1983. Some Observations on Mental Models. In *Mental Models*. Lawrence Erlbaum Associates Inc, Chapter 1, 7–14. https://ar264sweeney.files.wordpress.com/2015/11/norman_mentalmodels.pdf

[50] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2016. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *SSRN Electronic Journal* (6 2016). https://doi.org/10.2139/ssrn.2757465

[51] James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, New York, New York, USA, 1–14. https://doi.org/10.1145/3290605.3300275

[52] Martin Porcheron, Joel E. Fischer, and Sarah Sharples. 2017. "Do animals have accents?": Talking with agents in multi-party conversation. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. Association for Computing Machinery, 207–219. https://doi.org/10.1145/2998181.2998298

[53] Joel R Reidenberg, Travis Breaux, Lorrie Faith Carnor, Brian French, Lorrie Faith Cranor, Amanda Grannis, James T Graves, Fei Liu, Aleecia Mcdonald, Thomas B Norton, Rohan Ramanath, N Cameron Russell, Norman Sadeh, and Florian Schaub. 2014. Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal* 30, 1 (2014), 39–88. https://doi.org/10.15779/Z384K33

[54] Jon Rogers, Peter Bihr, Anab Jain, Jon Arden, Max von Grafenstein, Loraine Clarke, Martin Skelly, Nick Taylor, Pete Thomas, Michelle Thorne, Solana Larsen, Katarzyna Odrozek, and Julia Kloiber. 2019. Our Friends Electric. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, New York, New York, USA, 1–13. https://doi.org/10.1145/3290605.3300344

[55] Richard M. Ryan and Edward L. Deci. 2000. Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology* 25, 1 (1 2000), 54–67. https://doi.org/10.1006/CEPS.1999.1020

[56] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. 2016. You are being watched: Bystanders' perspective on the use of camera devices in public spaces. In *Conference on Human Factors in Computing Systems - Proceedings*, Vol. 07-12-May-2016. Association for Computing Machinery, 3197–3203. https://doi.org/10.1145/2851581.2892522

[57] Daniel J. Solove. 2007. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review* 44, 4 (2007), 745–772. https://ssrn.com/abstract=998565

[58] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, Productivity and Pleasure in the Smart Home. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, New York, New York, USA, 1–13. https://doi.org/10.1145/3290605.3300875

[59] Madiha Tabassum, Tomasz Kosinski Kosinski, 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 Symposium on Usable Privacy and Security (SOUPS)*. Santa Clara, CA, USA. https://www.usenix.org/conference/soups2019/presentation/tabassum

[60] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart Home Beyond the Home: A Case for Community-Based Access Control. In *CHI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honululu, HI, USA, 1–12. https://doi.org/10.1145/3313831.3376255

[61] 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/

[62] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the eighth symposium on usable privacy and security (SOUPS)*. 1–15. https://doi.org/10.1145/2335356.2335362

[63] Jinping Wang, Hyun Yang, Ruosi Shao, Saeed Abdullah, and S. Shyam Sundar. 2020. Alexa as Coach: Leveraging Smart Speakers to Build Social Agents that Reduce Public Speaking Anxiety. In *CHI '20: Proceedings of the 2020 CHI Conference*

on Human Factors in Computing Systems. Honolulu, HI, USA, 1–13. https://doi.org/10.1145/3313831.3376561

[64] Allison Woodruff, Vasyl Pihur, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. 2014. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *USENIX Association Tenth Symposium On Usable Privacy and Security (SOUPS)*, Vol. 1. Menlo Park, CA, US. https://dl.acm.org/doi/10.5555/3235838.3235840

[65] 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*. Association for Computing Machinery, Glasgow, Scotland, UK, 1–12. https://doi.org/10.1145/3290605.3300428

[66] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3 (2019), 1–24. https://doi.org/10.1145/3359161

[67] Eric Zeng, Shrirang Mare, Franziska Roesner, and Paul G Allen. 2017. End User Security and Privacy Concerns with Smart Homes. In *Symposium on UsablePrivacy and Security (SOUPS)*. Santa Clara, CA. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[68] 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 Security Symposium*. Santa Clara, Ca, USA. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[69] Serena Zheng, Noah Apthorpe, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact* 2 (2018), 20. https://doi.org/10.1145/3274469

[70] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, Smart Home' – Exploring End Users' Mental Models of Smart Homes. In *Mensch und Computer 2018 - Workshopband*. https://doi.org/10.18420/muc2018-ws08-0539

[71] Verena Zimmermann, Ernestine Dickhaut, Paul Gerber, and Joachim Vogt. 2019. Vision : Shining Light on Smart Homes – Supporting Informed Decision-Making of End Users. (2019). https://ieeexplore.ieee.org/document/8802394

A INTERVIEW QUESTIONS

The following are the primary questions used in the semi-structured interview. These are the pre-planned questions, follow-on questions based on user responses are not included.

A.1 Questions for Owners

A.1.1 Basic Questions.

(1) What device is it?
(2) Did you buy and set it up?
(3) How long did you have it?
(4) What are the reasons for buying it?
(5) Please draw your house and the location of all smart speakers and smart devices.
(6) Is there a particular reason for choosing this location?
(7) What do you use it for typically?
(8) To what extent did you change your daily routines or processes since you are using the smart speaker?
(9) Some people use smart home devices like light bulbs, do you have any? Why?
(10) What object in your home do you most wish would work with your smart voice assistant? Why?

A.1.2 Drawing - Same For Both Groups. Please draw the process of what is happening in the background when the smart speaker fulfils your request. What would be the different steps?

- Scenario 1: Ask your device what the weather will be tomorrow.
- Scenario 2: Ask your device to play a specific song from Spotify.
- Scenario 3: Imagine the light in your kitchen is a smart light and can be turned on via your smart device. What happens when you ask your smart speaker to turn it on?

A.1.3 Free Listing - Same For Both Groups. List everyone, all parties and people who are involved in the interaction and could potentially record that such an interaction has happened.

A.1.4 Questions on Third Parties, Potential Threats and Protections Strategies. For each scenario:

(1) Why do you think that these parties have access to your interaction?
(2) Which of these do you think are necessary?
(3) What benefits are in for them?
(4) What kind of benefits are in for you?
(5) What do you think do they know about you after you've used the device for a while?
(6) And how do you think can this access be misused?

Then:

(1) What kind of protection exists to protect you as a consumer?
(2) What do you do to protect yourself?
(3) If you could wish for one thing to protect yourself better, what would it be?
(4) Have you thought about this before?
(5) In what ways has this interview changed how you think about your smart speaker?

A.1.5 Questions on Social Norms. In some cases, smart speakers are also used in shared spaces or by visitors.

(1) Who else has interacted with your smart speaker?
(2) How often do you have visitors?
(3) Do all of them know that you have a smart speaker?

(4) How do they react when they find out?
(5) How do they interact with it how comfortable are you with them interacting with your smart speaker?
(6) What might go wrong if a visitor freely used your smart speaker?
(7) In which space would you feel uncomfortable encountering such as device? Why?
(8) What can you learn about your visitor from your interaction and what can they learn about you from interacting with your device?

A.2 Questions for Visitors

A.2.1 Basic Questions.

(1) Please tell me about your experience interacting with a smart speaker.
(2) As a warm-up for the next activity, please draw the room you were in and explain who was in the room.
(3) What kind of device was it?
(4) How often have you interacted with it before?
(5) What kind of feature did you use on it?
(6) Why do you think they own the device and what do they use it for normally?
(7) How did you become aware that the device was in the room/space?
(8) How did you react?
(9) Have you ever interacted with smart home devices such as smart light bulbs or kettles before?
(10) If someone gave you a smart speaker would you use it? Why?

A.2.2 Drawing and Listing. Same as in Sections A.1.2 and A.1.3.

A.2.3 Questions on Third Parties, Potential Threats and Protections Strategies. Questions the same as for visitors in A.1.4, however these were asked additionally.

(1) What do you think do they know about you as a visitor after you've used the device for a while?
(2) What can you learn about someone by talking to their smart speaker?

A.2.4 Questions on Social Norms. In some cases, smart speakers are also used in shared spaces or by visitors.

(1) Keeping in mind the scenarios and the experience you told me about earlier, how okay are you with interacting with other people's smart speakers in other spaces?
(2) What actions are acceptable and which are not?
(3) Where would you feel comfortable? (living room, bedroom, enabled doorbell, guest room, public office, park, hotel lobby, hotel room)
(4) In which space would you feel uncomfortable encountering such as device? Why?

B CODEBOOK

The following nodes were used to identify points made at various points during the interview. As described in the data analysis, we then did an affinity diagram for concerns and protections as well as social norms to determine the finer-grained themes which might have gotten lost in a usual open code.

The questions under each node defined the code and worked as a guide for the two coders.

B.1 Set Up, Usage and Relationship

- What do people use their Smart speaker for?
- How did they change their routines? Dependence?

- How do visitors interact with the Smart Speaker? (Including both what visitors say about their interaction and what owner say about visitors to their smart speaker)
- Device Location
- Benefits?
- Would they buy one? Why?

B.2 Ownership

- How do people think about their relationship to the device?
- Do they feel like an owner or a visitor?
- Did they buy it, were they gifted? Are they living with it or not?

B.3 Mental Model

B.3.1 **In-home only** - No information is shared outside of the home

B.3.2 **Provider (and Spotify - for the Spotify scenario) only** - Information leaves house only to go to Provider's Servers (and Spotify)

B.3.3 **Third parties** - The information is shared with more parties than the Provider (and Spotify for music listening scenario)

B.4 Concerns and Threats, Protection Strategies, Discomfort

- What kind of concerns do they have around smart speakers?
- What threats are posed to visitors or from visitors?
- What risks are they aware of?
- Tradeoff: What do they trade and how do they explain the deal?
- What things they don't have the control over?
- What do they do to protect themselves?
- What do they need to protect themselves?
- What do they do to protect themselves from and what not? (Only brief as details would go into concerns and threats)
- What do they have the control over?
- What are they not concerned about?

B.5 Social Norms

- What is okay for a visitor?
- What are they okay to do with someone else's device?
- Is there anything they would be uncomfortable with?
- What would they be comfortable doing?

B.6 Other

There is an important part that is related to our work in the interview and the coder is not sure which node to use. Coders will discuss these together and decide which node they belong to.