Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers

JOSEPHINE LAU, University of Michigan, USA
BENJAMIN ZIMMERMAN, University of Michigan, USA
FLORIAN SCHAUB, University of Michigan, USA

Smart speakers with voice assistants, like Amazon Echo and Google Home, provide benefits and convenience but also raise privacy concerns due to their continuously listening microphones. We studied people's reasons for and against adopting smart speakers, their privacy perceptions and concerns, and their privacy-seeking behaviors around smart speakers. We conducted a diary study and interviews with seventeen smart speaker users and interviews with seventeen non-users. We found that many non-users did not see the utility of smart speakers or did not trust speaker companies. In contrast, users express few privacy concerns, but their rationalizations indicate an incomplete understanding of privacy risks, a complicated trust relationship with speaker companies, and a reliance on the socio-technical context in which smart speakers reside. Users trade privacy for convenience with different levels of deliberation and privacy resignation. Privacy tensions arise between primary, secondary, and incidental users of smart speakers. Finally, current smart speaker privacy controls are rarely used, as they are not well-aligned with users' needs. Our findings can inform future smart speaker designs; in particular we recommend better integrating privacy controls into smart speaker interaction.

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

Additional Key Words and Phrases: Privacy; smart speakers; voice assistants; technology adoption.

ACM Reference Format:
Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (November 2018), 31 pages. https://doi.org/10.1145/3274371

1 INTRODUCTION

The Amazon Echo smart speaker debuted in November 2014 [61]. Since then, Google [12, 18], Apple [6], and Microsoft [54] have introduced their own smart speakers, and audio companies have started integrating Alexa, Amazon's smart voice assistant, into their own speaker products [41, 55]. Millions of smart speakers have been sold [31] and worldwide spending on these devices is expected to reach $2 billion by 2020 [27].

Smart speakers offer users hands-free voice control, but to detect and respond to voice commands, the speakers' microphones have to continuously listen for their *wake word* (e.g., "Alexa") [3, 29]. The privacy implications of this technical capability – especially when placed in the intimacy of personal

Authors' addresses: Josephine Lau, jlauuom@umich.edu, Benjamin Zimmerman, benzim@umich.edu, Florian Schaub, fschaub@umich.edu, University of Michigan School of Information, Ann Arbor, MI 48109, USA.

2573-0142/2018/11-ART102 $15.00
https://doi.org/10.1145/3274371

homes – have been the focus of much public debate [10, 24], prompting consumers to question what is being recorded, how collected information will be used, how it will be protected [10], and whether it will be used for targeted advertising [11].

Prior research has explored consumers' privacy concerns with smart home technology [63], connected toys [36], smart meters [33], and robots [17]. Other research studied how people use smartphone-based voice assistants in public [38], showed how the device is embedded into everyday, conversational settings [43], and identified benefits that individuals with disabilities could gain from using smart speakers in their homes such as speech therapy and support for caregivers [46]. Meanwhile, security researchers have identified security vulnerabilities [7, 32] that would allow attackers to exploit smart speakers as wiretaps [30]. Despite the privacy-intrusive potential of smart speakers' ability to continuously record voices in intimate spaces such as the home, consumers' privacy concerns with smart speakers and how these concerns affect smart speaker adoption and use have not been studied in detail.

A better understanding of these aspects can inform future smart speaker designs and privacy controls. We thus asked the following research questions:

(1) What factors affect the (non-)adoption of smart speakers?
(2) What are individuals' privacy perceptions and concerns regarding smart speakers?
(3) How do those privacy concerns affect their behavior around and with smart speakers?

To address these research questions, we conducted a diary study followed by semi-structured interviews with 17 smart speaker users, as well as interviews with 17 non-users. We found that non-users refrain from adoption due to a perceived lack of utility, or because they have privacy concerns and distrust speaker companies. Smart speaker users, on the other hand, express few privacy concerns, but we find that their rationalizations exhibit an incomplete understanding of privacy risks, such as believing that they are 'not interesting' or that it would not be feasible for companies to comprehensively collect and store audio content. Users largely trust the speaker companies to protect their privacy, mainly because this trust was necessary in order to use smart speakers. They additionally hoped that protecting user privacy would be in the company's best interest. We find that users expressed varying levels of awareness, deliberation, and resignation with the required privacy-convenience tradeoff. Finally, we find that users rarely used speakers' privacy controls, such as the mute button and audio logs. These controls were perceived as cumbersome and did not align with users' actual privacy control needs. Based on our findings, we provide recommendations for designing more usable and better-integrated privacy controls for smart speakers.

2 BACKGROUND AND RELATED WORK

Internet of Things (IoT) devices are becoming increasingly common. We first provide context as to how smart speakers compare to other IoT devices, then review prior work on privacy in smart homes and voice interactions.

2.1 Smart Speakers

Smart speakers, like other Internet of Things (IoT) devices such as smart light bulbs and thermostats, are comprised of sensors that measure physical properties of the environment, controllers that process sensed information, and potentially actuators that perform actions [16]. To detect when a user makes a request, a smart speaker's multiple microphones continuously listen for the device's activation keyword (e.g., "Alexa" or "Hey Google"). The smart speaker responds to a request through virtual or physical actions and audio feedback [3, 29]. User requests are processed by the smart speaker company's voice assistant technology, such as Amazon's Alexa, Google Assistant and Apple's Siri. Through those voice assistants, smart speakers can stream music, answer basic

questions, tell the weather and news, order pizza, control light bulbs and other smart home devices, and complete many other functions. Smart speakers can be connected to a multitude of smart home devices, but processing of commands largely occurs in the device maker's cloud-based backend. Smart speakers can also run automation applications such as IFTTT (If This Then That) [60] that connect to other services on user's phones and in the cloud [3, 4, 29]. Typically, smart speakers integrate with their parent company's other services; for example, users can access their Google Calendar through Google Home while Amazon Echo users can make purchases from Amazon. Smart assistants' capabilities can be expanded through third party applications, also known as "skills" for Alexa and "actions" for Google. Some speakers further offer the ability to place calls and connect to multiple accounts in households with more than one user [3, 29].

Although the only direct sensors on smart speakers are their microphones, microphones are perceived as one of the most privacy-invasive sensors next to video cameras [16, 40]. This, in combination with smart speakers' elaborate range of capabilities, as well as their placement in users' homes, result in smart speakers posing particular privacy challenges.

Current smart speakers are equipped with some privacy features. While the device's microphones are always listening, speech recognition is performed locally by the device until the activation keyword has been detected, at which point the subsequent voice command is forwarded to the maker's servers for processing. In addition, most smart speakers are equipped with a physical button to mute the microphones. Companion mobile apps and websites enable users to review and delete prior voice interactions with the device should they feel uncomfortable or not want companies to keep particular voice recordings on their servers [5, 28].

2.2 Privacy in the Internet of Things

Internet of Things technologies pose complex privacy implications. The sensitivity of an activity [19], the physical location of sensed data, the type of data collected, and data retention period [39] will affect how comfortable people are with their data being collected. Naeini et al. found that participants did not want to share their data in IoT scenarios when there was a perceived risk of their data being misused or used in a way that would harm them [39]. And while playback recordings of collected audio/video data can be useful, they can also be damaging if taken out of context [20]. The home is one of the most privacy-sensitive locations for IoT data collection [39]. Detailed data collection from a single device in the home [33] and the aggregation of sensed data [16] can reveal intimate insights on residents' activities, e.g., when smart meter's power measurements can reveal when nobody is home [33].

With IoT devices in the home, power dynamics among household members and guests can add additional privacy tensions, e.g., due to unequal access to smart home capabilities [63]; Zeng et al. found that primary users would sometimes restrict control to IoT devices or checked how and when other family members used the devices [63]. Conflicting attitudes between household members and guests on sensing or recording devices in the home can create further tension [20]. IoT home devices further enable monitoring of children's activities, challenging parents to weigh respecting their children's privacy with wanting to know their children's activity [20, 36, 58]. Finally, the private companies that make home IoT devices often have data collection and data use interests that differ from the interests of their users, creating conflicts of interest. Consumers have to balance the tradeoff between maintaining their privacy and the convenience afforded by the technology [33].

When IoT devices are used for surveillance, an unintended consequence can be a loss of trust, such as when parents use IoT systems to monitor their teenagers' whereabouts [58]. Oulasvirta et al. found that participants subjected to long-term surveillance would engage in privacy-seeking behavior around sensors and felt deprived of the solitude and intimacy expected at home, but also grew accustomed to and began tolerating surveillance over time [40].

Prior work has further studied what factors can affect IoT adoption. Brush et al. identified high costs, lack of heterogeneous integration, and security concerns as barriers to broader adoption of smart home technology [15]. Lack of trust in the organization controlling a device's functionality and data can also hinder IoT adoption [62]. For the aging population, privacy is often weighed against autonomy in adoption decisions; older adults might accept an intrusive monitoring technology to age-in-place [57]. However, Portet et al. find that older adults would not use voice-activated technology for fear of being perceived as dependent and losing their autonomy [44]. In contrast, Pradhan et al. find that individuals with disabilities found smart speakers to increase their independence and improved their safety [46].

Privacy concerns have also been identified as a reason for why users abandon technology [21, 23]. Satchell and Dourish [50] also stress the importance of examining non-use [9], when people actively resist adopting technology due to disenchantment, displacement, or disenfranchisement; or because they conscientiously object [14].

2.3 Voice Assistants and Privacy

Few studies have looked at the privacy implications and perceptions of voice assistant use. Talking to a phone-based voice assistant, especially in public, can create discomfort [37]. Moorthy and Vu [38] found that users of smartphone-based voice assistants were cautious when sending private information, noting factors such as their location (public vs. private space) and modality choice (keyboard vs. voice). Lambertsson [34] tested 12 participants' interactions with voice-activated smart home and mobile app prototypes. The mobile app prototype required participants to press a button to start voice interaction, the smart home prototype did not. Even though the button increased privacy by limiting when the microphone was on, participants felt having to press a button first removed the convenience of voice interaction. Zeng et al. [63] studied security and privacy concerns in smart homes, including but not focused on smart speakers. They found that reasons for participants' lack of security and privacy concerns regarding smart homes included not feeling personally targeted, trusting potentially adversarial actors (like companies or governments), and believing their existing mitigation strategies to be sufficient [63].

To address privacy concerns with audio/video recording technologies, researchers have recommended recording indicators [36] and user interfaces that display privacy risks and provide settings to control use and dissemination of collected data [16]. Such indicators and interfaces have to be designed carefully in order to be effective [45, 51, 52]. Moorthy and Vu recommended the ability for a user to store sensitive information, such as a home address, and then retrieve it with generic voice commands (e.g., "take me home"); this could remove the need to speak aloud private information in public [38].

While prior work examined privacy perceptions and concerns with IoT devices and smart home environments, little research has focused specifically on smart speakers and associated privacy perceptions and concerns. The integration of 'always listening' voice assistants with smart speakers brings an additional privacy challenge due to their use in the home and domestic environment; we bridge this gap through examining the use and non-use of these devices.

3 STUDY DESIGN

We included both smart speaker users and non-users in our study to understand privacy's role in adoption decisions and use of smart speakers. To distinguish participants, we refer to them as "users" and "non-users" respectively. With smart speaker users, we conducted a diary study followed by semi-structured interviews in their homes to gain insights on day-to-day behaviors around the smart speaker, as well as their privacy perceptions and concerns regarding smart speakers.

With non-users, we conducted abbreviated semi-structured interviews on campus focused on their decision not to adopt and use a smart speaker. Our study was approved by our institution's IRB.

3.1 Diary Study and Semi-Structured Interviews with Smart Speaker Users

Following the diary-interview method [8, 64], we first conducted a one-week diary study with smart speaker users to learn how users engage with their smart speakers on a daily basis and mitigate recall bias often present in isolated interviews; we then followed the diary study with semi-structured interviews [64]. During the follow-up interviews, we wanted to understand participants' awareness of their voice interactions being recorded as well as their awareness of privacy controls, such as the audio logs. Since we were also interested in understanding the context of users' interactions with their smart speaker, we opted for a diary study to allow participants to reflect on their interaction with the speaker, including potentially unspoken thoughts and considerations, rather than introducing an additional recorder to capture audio before and after an interaction [43] or asking participants to give us their smart speakers' audio logs.

Prior to the beginning of the diary study, one of the authors video-called each user to explain the diary procedure and study. Users were asked to submit at least one diary entry per day for one week through an online survey (see Appendix A). We asked about instances in which they used the device, as well as times they had considered using the smart speaker but did not, as those situations might signify privacy-seeking behaviors. We also asked users to report accidental smart speaker activations, in case these instances triggered reflection on privacy. Users could submit entries for each instance or daily summaries; they could also indicate that they had no speaker interaction on a particular day. Once participants started the diary study, we tracked their progress throughout the week via the survey tool and sent email reminders if they had not submitted at least one entry by 9pm. Participants were compensated $15 for completing the diary study.

After completing the diary study, we interviewed each user in their homes. After initial warm-up questions, we asked users to show us where they had placed their smart speaker and describe how its placement was chosen. With the users' approval, we photographed the smart speaker within its surrounding environment. We then asked what factored into their decision to obtain a smart speaker, as well as how they thought smart speakers function. We modeled parts of our interview script (see Appendix B) after other qualitative smart home and IoT privacy studies [15, 36, 63]. We first asked questions about their general use and setup of their smart speakers, guests' awareness and use of their speakers, their use of the speakers when others are around, other household residents' access to the device, and if they thought the device could remember what they say to it. A user's diary entries next served as prompts, especially entries about non-interaction or accidental interaction. If privacy had not already been mentioned and discussed at this point, we then explicitly asked about their privacy perceptions and concerns regarding smart speakers and how they thought their data was handled by speaker companies and third parties. We ensured that our questions about privacy were balanced and used 'forgiving' language to minimize the desirability bias of participants over-reporting desirable behaviors, such as responsible privacy behaviors [47]. We probed to assess their awareness and use of current speakers' privacy controls: physical mute button and audio logs in the companion app. We further asked, whether users considered smart speakers' current privacy controls sufficient, and how they would want a 'dream speaker' to protect their privacy. Participants received another $15 for completing the interview.

3.2 Semi-structured Interviews with Non-users

Non-users were interviewed on our university campus, using an abbreviated version of the smart speaker user interview script (see Appendix C). We first asked about their decision to not obtain a smart speaker, followed by questions that had indirect privacy implications. If privacy had not

been raised at this point, we then directly asked if privacy was a concern in their decision. We additionally asked participants if they had concerns of how different parties handled the privacy of their data, if they considered smart speakers' privacy controls sufficient, and how they would want a 'dream speaker' to protect their privacy. Non-users were compensated $15 after the interview.

3.3 Recruitment and Demographics

We recruited user and non-user participants with separate recruitment flyers, which we posted in buildings, libraries, restaurants, and cafes around our university campus and across town. We also posted announcements on Facebook and the local subreddit, and emailed a university mailing list. Over fifty potential users and forty potential non-users completed our online screening survey.

To reduce self-selection bias, we did not mention privacy in our recruitment material and screening survey (see Appendix D). Based on screening survey responses, we only invited users who reported use of at least one smart speaker. We only invited non-users who had considered owning a smart speaker but decided not to, and who did not list price as the top or only reason for non-adoption, as we were not interested in purely economic considerations.

We invited all eligible individuals to participate, and were able to interview 17 users and 17 non-users for a total of 34 participants. The two groups had similar ratios of men to women (4 female users, 5 female non-users); similar number of participants in engineering jobs (5 users, 4 non-users). The non-user group included more students (8 vs. 3). Two users and one non-user declined to provide their age. Users were 18–45 years old (median 33); non-users 18–55 (median 26). See Appendix E for detailed demographics.

At the time of this study, Amazon's Echo, Dot, Tap, Show and Google Home were the dominant smart speaker devices sold in the U.S. market. Our users owned one or more of the aforementioned speakers, with 13 in Amazon's ecosystem and 4 in Google's. While the majority of users had purchased their smart speakers, U01, U07 and U09 had received theirs as a gift. Users who had owned their speaker for less than a month (3 users) were balanced out by those who had owned it for over a year (4 users); other users were evenly distributed in between.

Interviews with non-users were conducted July to August 2017. They lasted 19–60 minutes (median: 32 minutes). The diary study was conducted in July 2017 and users interviews were scheduled and conducted shortly after each participant had completed their one-week diary. Of the eighteen users scheduled for diary studies, seventeen completed this portion; one participant was excluded from the study due to inappropriate diary submissions. Interviews with users lasted 25–59 minutes (median: 44 minutes).

3.4 Qualitative Analysis Approach

All interviews were transcribed using a transcription service, with subsequent quality control by the authors. Two of the authors inductively derived a codebook for the data. The codes were a combination of structural, magnitude, and descriptive codes [49], adjusted based on the need of the research question. For example, to identify what factors influenced a participant's privacy perception, descriptive codes were used under the category 'privacy factors,' and included: concerns about third-parties, choice, always listening, intrusion to private space, nothing to hide. To answer the research question about awareness and use of privacy controls, structural codes were used; under the parent code 'mute button,' its subcodes included: aware, unaware, use, potential use, and non-use. Thus, excerpts were coded 'aware - mute button' when a participant talked about being aware of this control, and an excerpt would be coded 'unaware - mute button' and 'potential use - mute button' when a user who was unaware of the mute button was speculating how they would use it.

Throughout the process of interviewing and creating the codebook, the first author kept analytic memos to keep track of running themes and identify emergent categories [49]. Using the memos and an iterative approach, two of the authors iteratively coded subsets of interviews multiple times, resolving disagreements and refining the codebook between iterations. The final codebook consisted of 136 codes in 25 categories. One of the authors then coded all interviews, using qualitative analysis software NVivo, while another researcher coded the diary entries and pictures with the same codebook. Afterwards, we used NVivo to query and subset excerpts, such as comparing how users and nonusers held different opinions about having 'nothing to hide' or what 'trust in parent company' meant to them. We then continued to create and iterate on affinity diagrams to further group codes and responses, identifying themes and insights.

3.5 Limitations

Since our study involved conducting in-home and in-person interviews, our study was limited to the metropolitan area surrounding the university. Additionally, despite our efforts to mitigate recall bias through the diary-interview method, diary entries and interviews are self-reported and participants may have omitted or forgotten certain interactions. Our study included 34 participants, a small sample size, but we are confident that the qualitative insights from this study facilitate a deeper understanding of privacy perceptions, concerns and behavior regarding smart speakers.

4 FINDINGS

We first provide context on who our smart speaker users are and how they are using the devices. We then describe the primary factors in participants' adoption (convenience; early-adopter identity) or non-adoption (lack of utility; privacy and security concerns) of smart speakers. We next analyze in more detail participants' security and privacy concerns regarding smart speakers, as well as how levels of awareness, deliberation and resignation affected how participants made privacy-convenience trade-offs. Lastly, we discuss how and why most users do not engage in privacy-seeking behaviors around their device or use current privacy controls. We end with how users envision their dream speakers would handle privacy.

4.1 Smart Speaker Use and Context

Our user participants included mostly primary users — people who have set up their smart speaker themselves and connected it to their own accounts. Users mostly placed their smart speakers in central locations in their homes to maximize utility.

4.1.1 Who is setting up and using smart speakers. Fifteen of the users set up the smart speakers themselves. We consider them primary users since the smart speakers were connected to their personal accounts, giving them control over the device [52, 63]. The remaining two users (U06, U09) were secondary users – they had not set up their speaker, instead their spouses did. Eleven of the primary users had secondary users, such as roommates or family members, in their homes.

Many users further mentioned incidental users. Incidental users, such as guests or children, are bystanders who may not be aware of or understand how the smart speakers work. Seven users reported visitors using their smart speakers; for others this was not a scenario because the smart speaker was located in a more intimate parts of the home (e.g., bedroom). Some users taught their guests how to use the smart speaker to control other smart home devices, such as lights. Five users reported that their children enjoyed using their smart speakers frequently for games and simple knowledge queries. U17 commented about their child: *"He probably uses it more than I do."* The devices enabled users' very young children to ask questions that they would otherwise be unable to look up, given that they cannot yet read or type.

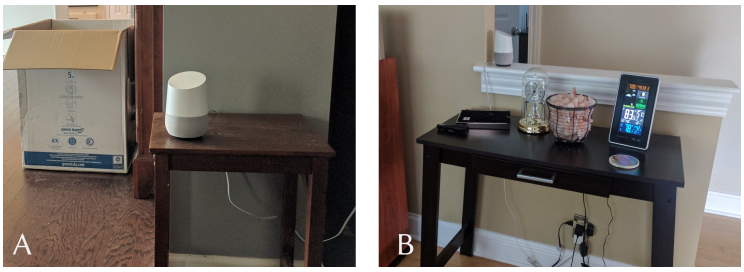

Fig. 1. Smart speakers were commonly placed in central locations in participants' homes, sometimes on dedicated tables situated at intersection points of multiple rooms, as demonstrated by U06's (A) and U04's (B) smart speaker placements.

4.1.2 Smart speaker placement. Since some rooms in people's homes are more private than others [2], we investigated if users considered this when placing their speakers. Main factors in the placement of speakers were centrality (15 users placed speakers in their home's most frequented areas), proximity to other electronics or entertainment systems (7), and frequency of use when not placed centrally (6). The seven users with multiple speakers placed one in a central location and another in a room they also tended to spend much time in, such as a bedroom or office. Some used these secondary speakers for specific tasks, like setting alarms.

All users put considerable thought into their smart speakers' placement. Generally, users chose speaker placements so their speakers would be able to pick up voice as much as possible; sometimes placing speakers in range of multiple frequently-used rooms, as shown in Figure 1. Privacy was not mentioned as a consideration in placement by any users. Twelve users moved their smart speakers around, trying to find the best place in terms of accessibility and sound. These users explained their actions as an iterative process where they continued to try new locations until they found where the speaker could be used most often. U04 stated: *"I started with it here, I've experimented with putting it here, also there. But I found that that is the best centralized location."*

4.1.3 Smart speaker usage. Participants reported various uses for their speakers, which were also reflected in their diary responses (frequencies based on diary responses): music playback (14), checking the weather (13), probing smart speaker capabilities (11), controlling other devices (8), asking knowledge questions (6), setting timers (6), checking the time (4), checking the news (3), setting alarms (3), setting reminders (3), checking their calendar (2), purchasing items online (2), playing games (1), and listening to the radio (1). Some utilized multiple different features of their smart speakers, but many stated they used their smart speakers almost exclusively to play music.

A major pattern in reported smart speaker use was users exploring boundaries of smart speakers' capabilities by testing queries for which they didn't know whether they were supported, with some treating it as a game to see how far they can push the speakers' abilities. Users tended to be more exploratory shortly after device setup. Fifteen users, who reported daily use of their smart speakers, stated they had initially used a wider range of features. As time went on, they got comfortable with the smart speaker's capabilities and their use cases simplified. U03 said: *"I definitely use it less now. I use it more for alarm setting, playing music. I guess when I first got it I was like trying all the new features."*

Seven users controlled other IoT devices in their home with the smart speaker, such as lights, thermostats, and home security systems. This required users to purchase other, potentially expensive, IoT devices that can be linked with smart speakers. These users reported high satisfaction with

how *"it makes life easier"* (U15). Many less tech-savvy users found the setup and linking of those IoT devices difficult, limiting access to this use case.

4.2 Factors Influencing Smart Speaker Adoption

Users adopted smart speakers for the convenience they would provide or because they liked to be early adopters. Non-users either did not find enough utility in the devices to warrant adoption or had privacy and security concerns regarding smart speaker use. Privacy-conscious non-users' concerns ranged from 'just enough' to deter them from adoption to high concern. The highly privacy-conscious non-users distrusted companies to adhere to their terms of service (ToS), believing that the company could change the ToS at any time. While a few privacy-conscious non-users said uneasiness about privacy and device security deterred them from adoption, they also expressed interest in possibly owning one in the future, if their concerns were better addressed. For example privacy-concerned NU15 said: *"If Google or Amazon or whatever came out with a really great ad campaign and said, "Actually this is what we do with your data." And they were actually honest about it, and it was very kind...then maybe I would feel a little more obliged."*

4.2.1 Primary motivators for smart speaker use. Users' primary motivating factors for purchasing a smart speaker were convenience and being early adopters, additional factors contributed to the decision for some.

Convenience. For users, the most prevalent motivating factor for purchasing a smart speaker was the convenience offered by smart speakers. Convenience is defined as the utility that they get from using the smart speaker frequently and effectively. Prior to adoption, many users sought the ability to easily ask for the weather, hear their schedule, or listen to music or the news, among other basic tasks. U02 describes their experience: *"I probably wouldn't have bought one if my girlfriend wouldn't have had one already...I use that a decent amount, I thought it was nice... and it was cheap so I decided to get one."* Participants with babies, such as U15, point out that additionally *"it's helpful being hands-free when you're holding a baby."* Finally, many users bought their speakers in order to easily control other IoT devices, such as light bulbs and entertainment systems, with their voices. Almost every non-user also considered the convenience of using the speakers for basic tasks. For them, however, other factors outweighed potential convenience.

Identity as an early adopter. Eleven of our users either explicitly said they liked to be an 'early adopter' or implicitly described themselves as such. They liked to stay current with technology and derived pleasure from being among the first users of new gadgets. As U09 described it, they wanted to be on the *"bleeding edge."* Indeed, two early adopters bought smart speakers impulsively without fully understanding what a smart speaker was or did; U18 said: *"I just jumped in. I didn't even really know what a smart speaker was, but, it sounded pretty neat. I just went for it."* Thus, these users' desire to be among the first people to own this technology propelled them to adopt smart speakers.

Contributing factors for smart speaker use. While convenience and early adoption emerged as primary factors driving smart speaker adoption, we identified a number of additional factors that contributed to participants' decisions: considerations of price (6), family and housemates (5), technology ecosystem and integrations (5), and device aesthetics (1). Six users stated they would not have bought a smart speaker at full price, but ended up buying them during an online sale. All five users who lived with their family or housemates thought about those potential secondary users when buying or setting up a smart speaker, consulted them, and took their use cases into consideration. Five users considered the specific ecosystem of products and services offered by a speaker company. They wanted their smart speakers to integrate and align with technology they already use.

4.2.2 Primary motivators for smart speaker non-use. Non-adoption of smart speakers was primarily motivated by either a perceived lack of utility or privacy and security concerns.

Perceived lack of utility. While many non-users discussed the potential convenience of smart speakers, they did not feel the devices' usefulness justified their cost, yet. We interpret this weighing of cost and functionality as an assessment of utility. Nine non-users fell into this category of 'utility-oriented non-users.' NU08 explained: *"It was expensive for as limited as what it could do... I probably would have only gotten for the lighting controls, but as they add apps to it, maybe one day, but not right now."* Related to perceived utility, non-users considered the potential abandonment of devices if they lacked utility, NU11 said: *"I'm going to hold off getting anything like [a smart speaker] until I actually know if it's something that I'm going to use, or if it's just going to sit in a box or sit on a counter."*

Privacy and security concerns. As expected, privacy emerged as a major deterring factor for smart speaker adoption. The other eight non-users fell into the category of 'privacy-conscious non-users.' They brought up privacy concerns on their own during interviews and were deeply uncomfortable with the idea of a *"microphone-based"* device that a speaker company or an *"other"* with malicious intent could ostensibly use to listen in on their homes. They believed in the sanctity of their home and expected their private home affairs to remain private. They expressed that they have a right to privacy, even if they have nothing to hide. Most non-users in this group did not trust the smart speaker company to abide by the ToS in perpetuity. NU09 explained: *"Many companies will list things that they collect and even describe what they use it for, but these agreements aren't necessarily accurate. They're subject to change unalterably at any time. You basically have to take the company at their word."* NU09 also believed that the speaker companies could be installing concealed backdoors and feared surveillance. While a few of these privacy-conscious non-users were certain that they would never have smart speakers in their homes, others mentioned that if these concerns were addressed, they might consider getting one in the future.

Non-users NU17 and NU07 trusted the companies to only record voice commands, but were still concerned for their privacy because someone might be able to listen in on them. They posited that since major companies like Yahoo and other IoT devices like baby monitors have been hacked, it is highly unlikely that smart speaker companies can guarantee safety from hackers. NU07 said: *"I think there's a capability there to listen in when you're not expecting it...Certainly I think Amazon would do everything they can to assuage your fears about protecting your privacy...I'm just saying a lot of things and websites and places that you thought were secure have been found to be not as secure as you'd hoped. I don't think that there's a way for them to 100% guarantee that they can't be hacked."*

While two users (U06 and U18) were also afraid of speakers being hacked, many users and some utility-oriented non-users, felt they could trust large companies to secure consumers' data because they have sufficient resources and scale. Users believed it would be in the companies' self-interest to protect user data or their customers will go somewhere else. NU15 said: "*I think it's probably important to know that Amazon, Apple and Google don't really seem to have a track record of being hacked, so there probably isn't really much use in worrying about their servers being attacked."*

Participants considered multiple factors, but their adoption decisions ultimately came down to convenience or them being early adopters. For utility-oriented non-users, when price was not a factor, the largest barrier to adoption was a perceived lack of utility of the device. Privacy-conscious non-users rejected smart speakers for privacy reasons and high distrust in speaker companies. Our privacy-conscious non-users are similar to what Satchell and Dourish describe as non-users engaged in "active resistance" while the utility-oriented non-users are part of the "lagging adoption" group, non-users who simply do not use the technology *yet* [50]. To better understand these two types of non-users, we continue to differentiate between them in subsequent sections.

4.3 Privacy Perceptions of and Concerns with Smart Speakers

In addition to the primary reasons behind participants' (non-)adoption of smart speakers, we explored how privacy perceptions and concerns figured into these decisions and users' interaction with smart speakers. Privacy-conscious non-users readily discussed smart speakers' privacy implications. However, privacy was rarely brought up by utility-oriented non-users and users. When probed about privacy concerns, the majority of these participants rationalized why they were unconcerned.

4.3.1 Value placed on personal data privacy. Privacy-conscious non-users were deeply uncomfortable with smart speakers' potential to give companies and malicious actors access to the intimacy of their homes. Despite having 'nothing to hide,' they strongly believed in their right to privacy and did not trust companies to respect that right.

Conversely, many users and utility-oriented non-users were not similarly concerned. While privacy-conscious non-users were not comfortable with 'anyone' having access to their data, users trusted the speaker company with their data. U01 additionally pointed out that *"the data that gets shared to the public is almost non-existent. For example, there's no way for you to view my Alexa skills history."* Users and utility-oriented non-users further justified their lack of privacy concern by labeling themselves as having "nothing to hide" or "not interesting," meaning that no one would care to know about them, go through their voice snippets, or spy on them through their speaker.

4.3.2 Participants' perceptions of how smart speakers work. Participants' perceptions of how smart speakers work help contextualize their privacy concerns or lack thereof. We found that privacy-conscious non-users did not trust companies to abide by their ToS and only record users' commands; others did not trust that the speakers were safe from malevolent actors. Utility-oriented non-users and users rationalized that it would require 'too much storage' and 'too much processing power' to collect, store, and analyze 'everything' from their smart speakers.

Smart speakers' potential to listen and record was invariably brought up by privacy-conscious non-users. This group of non-users highly distrusted a device specifically designed to be 'always listening.' NU05, NU15, and NU17's uncertainty with how speakers work and when they are recording made them uncomfortable having a smart speaker in their home. NU05 directly weighed smart speakers' benefits against privacy risks in a privacy calculus [22]: *"I guess for me it's in terms of the benefits to me using it versus the cost in terms of a perceived loss of privacy."* Users and utility-oriented non-users varied in their understanding of when the speakers are listening versus recording. Utility-oriented non-user NU13 perfectly encapsulated this confusion: *"I think it could definitely record what you're saying, but I don't think it's intelligent enough to remember. I don't know if that makes sense...I guess, theoretically, it could record anything that you happen to be talking about that you're in the room with. But I don't know what anyone would really do with that."* Many users and non-users also reasoned that the companies would not continuously record because *"the data that would be involved in storing all that information would be astronomical"* (NU07) and that it would require exorbitant computing resources to find the *"few things in there that might have some relevance"* (U08). However, these participants' assumptions miss the possibility that companies could feasibly collect everything about specific individuals when compelled to do so.

NU12 was uncertain about the potential value of the data smart speakers could collect: *"I think the unanticipated consequences are the main thing,...you don't realize how much information or how valuable it is...or how they can spin that into something else."* Although several privacy-conscious non-users acknowledged how much online companies already know about them, they did not want these companies to know any more about them than necessary. Others (NU11, U11, U17), however, considered the information they give to their smart speakers to be just small additions

to everything that the companies already know about them. When asked if they have concerns of how their speakers handle the privacy of their data, U17 said: *"No, because it's not the device handling the privacy. It's Amazon and their cloud. I already give them so much information. I don't think a little bit more matters."*

Two users said they would accept speaker companies potentially recording everything, not just their commands. U15 believed that it was only recording his commands, but *"if I am wrong, I don't care. I understand that not all of my information is gonna be private, and sometimes I will give up some of my privacy for convenience."* U16 assumed his speaker was already recording everything: *"I think they're just recording everything because they haven't found all the use cases yet. And it's better to have all these data points now and kind of figure it out in the future."*

In summary, while most users and non-users expressed uncertainty about whether smart speakers were always recording, they engaged with this uncertainty quite differently. Privacy-conscious non-users did not trust smart speakers to record only commands and to protect their data from malicious parties. Users and utility-oriented non-users believed that the smart speakers were only recording commands because recording everything continuously would require too many resources.

4.3.3 Speaker data used for targeting advertising. Most participants were aware that their online behavior is being analyzed to serve them targeted ads, but participants would feel uncomfortable if their smart speaker voice commands were used to target ads. U18 and U10 remarked that they have not yet seen targeted ads based on their smart speaker use. U18 said: *"If I'm shopping,...I haven't seen any evidence that there's some algorithm that's spying on me or making things happen that only the Echo can know."* While non-users and users alike generally found targeted ads "creepy," many also found them useful [59] and preferable to irrelevant ads. Privacy concerned non-users on the other hand were especially leery of their data being used and sold for ad targeting. NU15 said *"I guess any time your own data is sold to someone else, it sort of feels a little bit like something is being taken."* They were also uneasy about not knowing how their data could be used against them, or if they can challenge the accuracy of the profiles advertisers build about them. For these reasons, NU12 did not feel comfortable with smart speakers being another data source for advertisers.

Almost all participants expressed privacy concerns with third parties. Privacy-conscious non-users did not trust the parent companies to keep their data to themselves. NU12 said: *"let's say I do get a smart speaker. I expect that my relationship will be just with Amazon, but if Amazon is going behind my back and selling that information to Spotify, I didn't really want to make that relationship with Spotify...once you let go of that data,...you don't know what's going to happen to it."* Users on the other hand trusted that speaker companies would not share their data with third parties. U07 said: *"But Amazon having it, fine. When they start giving it to third party users, and I don't know exactly who they are or what they're doing, that's probably where I start to get concerned."* However, third parties developing 'skills' for smart speakers already receive a user's commands when the skill is activated [56].

In summary, while privacy-concerned non-users were uncomfortable with an 'always listening' device in their home and cite their right to privacy, users and utility-oriented non-users felt the opposite. Users felt safe relying on the socio-technical context within which smart speakers reside; they trust the companies because of their scale, resources, prior positive experiences with them, and additionally, because they felt companies would protect their privacy for their own economic self-interest and public image. Moreover, users make arguments from both sides of the problem: one, that speakers cannot record everything since it would require too much storage, and two, that if speakers were recording everything, the recordings would not be of interest to themselves or anyone else. Users' need to justify both sides speaks to the uncertainty with how comfortable they are with trading their privacy for convenience.

4.4 Awareness, Deliberation, and Resignation in Privacy-Convenience Tradeoffs

Throughout the process of conducting the interviews and analyzing the reasons why users and non-users perceive the privacy risks of smart speakers differently, we observed that participants expressed their reasons for privacy concern or unconcern with varying confidence and comfort. We find that their level of confidence was connected to how aware they were of the tradeoff they were or would be making – privacy for convenience – which was also affected by their attitude and level of resignation to the current state of technology (i.e., pervasive data collection and sharing, large companies already having their data). In this section, we describe how participants actively refused to trade off their privacy for convenience, consciously accepted the tradeoff, or were unaware of a tradeoff occuring.

4.4.1 Refusal to trade privacy for convenience. The eight privacy-concerned non-users all consciously refused to trade off their privacy for convenience, actively choosing to forgo smart speakers in their homes. They were deeply aware of the risks of having an 'always listening' device in their home, and did not think that utility of the devices would offset these risks. NU09 pointed out that *"some things I will trade for free service. Some things I won't trade for free service...I can take a smart speaker and have a network firewall [check if the speaker is doing what it says it is doing], but that's additional work and expense and it demands an increased level of vigilance from me. I just don't see that as being worth the trade offs."* For these non-users, smart speakers would constitute an overwhelming *inconvenience*, due to the perceived need to monitor its operation for malice.

These non-users, who were aware and conscious about the involved privacy-convenience tradeoffs, were also the least resigned to the present state of technology, taking action to control their personal data privacy. NU05 said: *"With my phone if they really wanted to listen, they could ...I don't really – no choice in the matter. But with smart speakers...I can avoid having it, so I'd really not, I don't want another thing that could possibly violate my privacy."* Finally, while some of them are resolute in their stance against having a smart speaker in their homes, others may become more accepting over time. For instance, despite how passionately NU07 talked about their privacy and security concerns with smart speakers, they said: *"I'm not going to buy one. If I would accept a free one, okay maybe. I don't know. Probably I shouldn't considering how passionately I feel about [privacy]."* There is thus a range in how strongly and confidently these non-users stand in their refusal of the technology due to privacy concerns.

4.4.2 Acceptance of privacy-convenience tradeoff. In contrast, the majority of users (11) acknowledged that they have actively traded, or were willing to trade, their privacy for convenience. We make this distinction between the tenses to draw attention to the spectrum of participants' deliberation regarding this tradeoff: two users had actively considered the privacy risks and determined it to be worth the convenience, meanwhile expressing the highest level of resignation. The remaining users in this group were comfortable with the tradeoffs they made, expressing resignation to a lesser extent. We further find that while the non-users made their decision to not trade privacy for convenience specifically with respect to smart speakers, participants in this group accepted privacy-convenience tradeoffs more generally. For these users, the privacy-convenience tradeoff did not factor specifically into their consideration of adopting smart speakers; rather, they had acted from a place of resignation, having to give up privacy for the adoption of new technologies.

Two users in this category were especially cognizant of the privacy-convenience tradeoff. U04 and U13 had previously taken great care to protect their privacy, but eventually succumbed to tech companies' free but privacy-invasive offerings. U04 explained: *"When I was younger, I used to hate it. I did the whole software freedom thing. Over time, I think I'm either getting more cynical or I just don't care...The slippery slope is past already."* U13 echoed this sentiment, *"It got to be so*

inconvenient that I just actually did a 180 and I bought a Google phone, I reinstalled everything. I said, just have all my shit. I don't care. Same thing with Amazon. I don't care." The main reason for this drastic shift was a sense that it became increasingly impossible to avoid cloud offerings and resist the convenience they promised: *"It [became] prohibitively time consuming to find other email systems, find other services that you could store stuff in the cloud on...with all the convenience of being able to share docs [...] it was just too much to fight, and I just gave up."* They have completely resigned themselves to the knowledge that convenience comes at the cost of privacy. These two users accepted the privacy risks of their smart speakers with clarity, having already surrendered control of their personal data to the big technology companies that now also make smart speakers. Thus, for them, this decision was part of a broader resignation that technology adoption requires giving up privacy, rather than specific to the smart speaker.

The other nine users in this category were comfortable with the privacy-convenience tradeoff they had made, but still exhibited different levels of resignation to the need for this tradeoff. When asked about their lack of privacy concern when using smart speakers, they expressed that convenience was worth giving up some privacy. Five explicitly mentioned being comfortable trading their privacy for convenience but also expressed resignation about how current technology has eroded privacy. For example, U16 commented, *"I think the battle of privacy and convenience has been won by convenience. And I'm okay with that because I live in a world where this convenience is what makes my life a little bit easier to navigate and things more enjoyable and I'm okay."* In regards to Amazon knowing what they say to their speaker, U07 said: *"I would like to think that we have privacy and things like that, but I know we don't. I wish we did, but I guess I've come to understand that it's just going to be a part of life."* And in response to having an 'always listening' device in his home, U11 said: *"Give and take. Google has access to all of my email, which means in principle it has access to everything that I do on the internet anyways. It's not that different. It's obvious it's a little bit more intrusive, but I don't think it's that much more intrusive relative to what I gain from using it...I think it's a trade off that's worth making."*

Based on their non-negative experiences with Amazon or Google, two users (U10, U11) trusted these speaker companies to protect the privacy and security of the data that they were giving them. U10 said: *"I've been using Google stuff for years and I can't find any instances of them breaking my trust."* Both U15 and U16 however say that they trust the company to protect their data only because it would be in the company's best interest; U16 said: *"They sign a contract that is legally binding that if they don't do this they can lose their business, so it's in their best interest to try to protect people."* Interestingly, three users also rationalized and supported the companies' need to use their collected voice data to advance their speakers' capabilities. U04 explained: *"I have no misconceptions about what they're doing with my data. But I also understand that in order for it to achieve that Star Trek-like thing that we want, that you need to have a huge cloud. You need Google to collect voice data for decades in order to get that to happen."*

Lastly, while U03 and U11 both were willing to pay the cost, they mentioned wanting companies to be more transparent about data use, collection, and deletion for others who are more skeptical of smart speakers. U11 said: *"I can appreciate why someone certainly wouldn't want them and I think if there's some more transparency in that whole process of what exactly Google's doing with that data, they could address some criticisms of that particular use of it...just saying exactly what they record, how long they store it for, some verification that they're actually deleting it when they say deleted. Just a basic oversight of that process."*

4.4.3 Unawareness or avoidance of privacy-convenience tradeoff. The remaining six users were either not aware of the privacy-convenience tradeoff associated with smart speaker adoption (U08) or deliberately avoided thinking about it (U01, U02, U06, U07, U17). These users explicitly said they

'try not to think about it,' with 'it' being the privacy implications of technology. U06 explained her discomfort, *"It's kind of the whole, I'm afraid to dig too much into it because I'm afraid of how much the world knows about me. I kind of wish that wasn't a fear of mine. I kind of wish I didn't have to be afraid of how much Google or Facebook or whatever knows about me."* Indeed, this fear can cause these users to be less than fully aware of the privacy risks of technologies they are adopting. When asked how they felt about how the smart speakers handle their privacy, U08 responded, *"Until we started having this conversation I never really thought of a smart speaker as having anything to do with privacy."*

Smart speakers' 'always listening' microphones come with an inherent risk when placed and used in intimate spaces such as homes. However, this inherent risk was not apparent to all participants. While some of the non-users actively decided against speakers in their homes, users' resignation and growing acceptance of the privacy-convenience tradeoff may be discouraging them from deliberately weighing the specific privacy tradeoffs associated with new technologies, such as smart speakers, on a case-by-case basis.

4.5 Privacy-Seeking Behaviors and Privacy Control Needs

Since prior research had found that microphones were perceived as one of the most intrusive sensors in home contexts [16, 40], we studied if and how users were engaging in privacy-seeking behaviors around smart speakers, similar to those reported by Oulasvirta et al. regarding ubiquitous home surveillance [40]. Additionally, Pradhan et al's recent study on the use of smart speakers by people with disabilities found that two of their participants turned off the microphone during sensitive conversations and another unplugged it [46]. However, none of our users reported any privacy-seeking behaviors in their diaries. In interviews, we probed deeper to see whether they might switch to another device (e.g., their phone) for more sensitive interactions or whether accidental smart speaker activations might cause concern of being listened to. We found no evidence of specific privacy-seeking behaviors around the device. The one user who reported switching to their phone from the speaker did so because their phone allowed them to more quickly look at and retain weather information. Six users reported accidental activations but found them humorous not privacy concerning.

We also found that most of our users did not use any of the privacy controls provided by their smart speakers. Yet, some users still expressed privacy control needs that are presently unmet, indicating a mismatch between user needs and current privacy controls. Lastly, we found that those users who actively avoided thinking about privacy implications of their smart speaker tended to be unaware of the available privacy controls.

4.5.1 Use of smart speaker privacy controls. Many users were aware of the ability to review audio logs and the mute button on their smart speaker, but did not use those controls for privacy regulation for multiple reasons.

Smart speaker mute button. If a user wanted to stop their smart speaker from listening to them and responding, they can press the mute button atop the speaker. Eleven users were aware of their smart speaker's physical button to mute the microphone, but only U15 and U16 actually used them. U15 used the mute button the most but not for privacy reasons; they used it to prevent their child from playing with the speaker too much. Interestingly, neither U15 or U16 expressed that they did not fully trust that the mute button would switch off the microphone. U16 stated: *"I don't really trust it to stop recording. There's no real evidence that it stopped besides it just stopped responding to you."*

When we prompted participants to explain how they would stop their smart speaker from listening, U15 stated *"If I really wanted to, I'd unplug it. You can hit the mute button on top. I don't*

know if it's actually doing anything or not." Nine users' first instincts were similar: they speculated they would unplug the device before thinking to press the mute button. Even though they were aware of the mute button, two users assumed that if there was a situation where they would want the speaker to stop listening, they would unplug it because it would be *"safer...because I understand how electricity works and I don't know what that button is doing behind the scenes"* (U09). Three privacy-concerned non-users felt similarly about the way mute buttons worked, not trusting it to actually work the way it's intended. NU09 said: "*this phone can be listening and recording right now. I don't know. The screen is off. I've set it to mute, but just because I've done that, how do I know it's not actively doing this right now? I don't. Same thing with the mute button on an Amazon Echo.*"

Four users expressed that using the mute button would negate the device's primary functionality – hands-free operation. U07 said: *"But I'm torn... if you have to go over and press the button every time, that kind of defeats the purpose of having a [smart] speaker."*

Three users (U06, U09, U14), two of them secondary users, were completely unaware of the mute button, and another three (U07, U13, U17) were aware of the existence of a button but did not know how they worked. During our interviews, while guessing how they could deactivate the speaker from listening, two users discovered the mute button but assumed it would silence the speaker rather than prevent it from listening. U17 explained: *"I always think that's turn the speaker off, not turn the listening off."* This incomplete mental model lines up with how mute buttons typically work on other devices, such as TV remotes. Lastly, while they were aware of the mute button, a few participants erroneously believed they could also silence their speaker through a voice command, saying commands such as *"Alexa, mute yourself"* (U13) or *"Hey Google, stop recording"* (U11) during the course of the interviews.

Smart speaker audio logs. Users can also access the audio recordings of their commands through their smart speakers' mobile or web companion app; through those apps, they can also delete selected or all of their recordings if they do not want them kept on the speaker company's servers. Both Amazon and Google mention these voice history or activity logs as part of their privacy and security protection measures for their voice assistants [5, 28].

All users were aware of these audio logs, except for U06, a secondary user, and U08, who had impulsively bought a smart speaker to be an early adopter. For three users (U10, U11, and U12) the audio logs demonstrated that only their commands are recorded by the speaker. U11 explained: "*I know with the speaker, at least I can go online and see whenever it's triggered from the keywords what exactly it records.*" Privacy-concerned non-user NU05, however, was not convinced by the audio logs in the same way: "*Uh, I don't know if it's just recording voice commands though, or if it's recording extra conversations, whatever. I mean it'd be nice to see, but it still wouldn't change my mind.*"

Only U11 had deleted audio logs, because they *"just didn't want that stored on their servers. Just on the off chance that someone thought it was inappropriate, I deleted it."* Otherwise, only U04 recognized audio logs as a form of privacy control, comparing it to how "*on my browser sometimes, I'll go and delete something;*" however, they said they don't do this with the speaker's audio logs because *"generally speaking, if there's anything inappropriate, I'm searching on the computer, not on the speaker. Kind of have that separation."*

Many (11) users used the audio logs simply to see what they had said and if any funny interactions happened with their smart speaker. For example, U07 described checking their audio logs when, *"I'm bored, and I'm like, 'Hey, I might as well see what I've done'."* It is important to note that while most users were aware of the ability to look back on their voice interactions in the companion apps, only U04 and U11 made the connection that this capability can also serve as a privacy control. Indeed, a few users said it was not common practice for them to look at the app because it "*isn't*

very useful" (U07) or that "*normally, I don't really have any reason to actually go through and look at [the audio logs]"* (U11).

Rather than using it as a privacy control, two users actually used their audio logs to surveil or monitor secondary and incidental users. U15 checked how house sitters are using the device: *"It's a little voyeuristic but I like [to check the audio logs] when somebody is staying here. They're watching the house for us. Just to see how badly they do or the thing that they search for when I'm not here. I find it entertaining."* U10 saw audio logs as artifacts of their children's childhood, akin to baby pictures: *"I like to go back and hear my kids asking. I think it's kind of neat, because eventually they're not going to talk like that anymore... To hear them interact with something like that, it's kind of cute."* While some privacy-concerned non-users expressed concern about how long the smart speakers would store their audio logs, this user wanted the logs stored forever so they can listen to their young children's voices indefinitely. Yet, McReynolds found in the context of voice-activated toys that children are often not aware of voice commands being recorded and find it scary when they learn about it [36].

4.5.2 Unmet privacy control needs. While the non-use of smart speakers' privacy controls could suggest that users might not feel the need to regulate privacy around those devices, that is not the case. Multiple users expressed privacy control needs that were just not met by existing controls.

Incognito mode. Many users mentioned privacy strategies they used on other devices, like their phones or laptops. Several users mentioned using private browsing modes while searching or browsing the Internet. U06 and U09 alluded to how there is no similar functionality on smart speakers. When asked what privacy controls they would like to see, U06 said she would want something like *"Google [Chrome]'s incognito mode, something like that...And having control over what it gets and what it doesn't get."* U04 also explicitly stated that he would switch to the incognito mode on his computer for searching 'anything inappropriate.' U03 suggested that such an incognito mode could be time-limited: *"I guess that also brings in more sense of comfort and privacy if I ask something maybe I don't want Amazon knowing, I can kind of restrict that. Or maybe tell Amazon, ..."Hey Alexa. Don't collect my information for the next blank hours."* This shows that users desired a more proactive way, such as an incognito mode, to prevent their recordings from being saved: they would feel more comfortable having the option to control what data gets collected, and were already familiar with incognito modes from other technology contexts. In contrast, deleting an audio log is more retroactive and requires users to look for them.

Improved account management for secondary users and multi-user contexts. Users, in particular secondary users U06 and U09, also talked about issues they had with using their smart speaker with multiple users. U06 perceived herself as having less control of the device because she was not the primary user, she explained: *"I guess my assumption is that [my husband] has slightly better access just because his devices work more naturally with it...I'm not sure but it feels like the Google Home prefers his phone over mine. So like if we tell it to play something, it always thinks of his phone first instead of mine."* Meanwhile, U09 described how she has to share an account with her housemate, another secondary user, while her partner, the one who had set up the device, has his own account; she said: *"Well, that's the funny thing about having three adults in the household, is that, um, I don't think we can set up three adults. So two of us log in on the same account to the Alexa. Like [my partner] has his, and then [my housemate] and I share, like, I log in under her username."* This sharing of account credentials may lead to privacy issues. This user's household had also disabled the ability to shop with their smart speaker; they did not *"want it to be too easy to shop...and I think for privacy reasons too. Cause as much as we have shared lives..I don't necessarily wanna know what [my partner] is ordering."* U18 set up a pin number for purchases so their daughter *"couldn't accidentally order*

anything." He would have liked more options to restrict smart speaker skills: *"As she got older I would probably be more into possibly locking some other features down although I haven't thought of or encountered any capabilities that would make me worry about her using it other than spending my money."*

U09 was more concerned with the smart speaker leaking sensitive information. She would like the smart speaker to give her updates or notifications of a more private nature, such as banking information; however, she didn't "*see a good way right now to mitigate the aspects of not wanting to share that with other household members or with guests.*"

5 DISCUSSION

While smart speakers can offer users convenience and more efficient lifestyles, their use comes with privacy risks and implications. For non-users, perceived lack of utility or privacy concerns were main reasons for their non-use. Privacy-conscious non-users made an active choice to not own smart speakers. Our findings regarding smart speaker users reveal that privacy was not a primary consideration in their adoption decision; rather, convenience and identifying as an early adopter were dominating motivators in acquiring smart speakers. However, their rationalizations for their lack of privacy concerns convey resignation regarding privacy incursions by smart speakers and companies more generally. We found that although users shared similar rationalizations, their awareness and deliberation of privacy tradeoffs associated with a smart speaker and their resignation to technology's progressive intrusiveness varied. Their level of awareness and resignation affected how comfortable and confident they felt and how willing they were to trade privacy for convenience. We additionally found that primary users and non-primary users do not share an equal awareness of smart speakers' privacy controls and understanding of their privacy implications. Users did not use current privacy controls as they were cumbersome, misunderstood, or did not meet participants' control needs. These findings form the main contribution of this paper. We next reflect upon their potential implications for researchers and designers. We describe these suggestions conceptually to spur discussion on how we might design more privacy-friendly smart speakers.

5.1 Trust's Crucial Role in Smart Speaker Adoption and Use

We find that smart speaker users trust speaker companies, like Amazon and Google, due to their established, mostly positive relationships with these companies in other contexts. Non-users distrust these same companies for the opposite reason – they often have adverse relationships with these companies. They believe the companies do not have consumers' best interests in mind, that they will change their terms of service as it suits them, and that they could be infiltrated by bad actors. While these companies have yet to experience the massive data breaches that other companies have sustained, the possibility of future privacy calamities causes concern. Furthermore, as a few non-users noted, it is difficult to assess if companies are behaving honestly. The difficulty in monitoring companies' behavior coupled with a general distrust of smart speaker makers led non-users to abstain from smart speakers. This dichotomy in perspectives illustrates the crucial role trust plays in how individuals reason about technology and its implications.

Notably, those participants who trusted their speaker's companies, did so because of prior experiences in other contexts, rather than the company's specific security and privacy measures for smart speakers; they often exhibited an incomplete understanding of how smart speakers work. Given the challenges for consumers in researching and understanding an individual product's privacy implications or protections, we argue that both IoT device makers and society at large have a responsibility to ensure that the trust placed in technology is not blind but actually warranted. Policy makers, regulators, as well as industry need to create **strong standards for IoT security and privacy protections** that IoT devices need to implement in order to establish a reasonable

baseline consumers can rely on. Security certifications of devices could further ensure that certain standards are met by a device and communicate that information to consumers, similar to safety seals for electronics products.

Companies need to truly provide **transparency about smart speakers' data practices** to consumers, including what data is collected, how long it is stored for, who has access to it, and how it is protected. This information needs to be provided in an easily accessible and understandable fashion. Rather than hiding privacy information in lengthy and ambiguous privacy policies or terms of service [48, 51], smart speaker companies should leverage the main interaction capabilities of their products – voice – to integrate **conversational privacy dialogs** into the smart speaker user experience. During setup, the speaker could inform users how the speaker works and even obtain consent for certain practices. Rather than reading out policy statements at length, over time the speaker could progressively introduce data practices, explain the need for certain data collection or use practices, and through conversation with the user jointly establish which practices the user agrees with or rejects. For example, rather than immediately storing all voice interactions, which might require immediate notice and consent, the speaker could inform the user after a few days of use about the benefits and risks of storing voice interactions, ask for consent, and then also introduce how to access and delete prior voice recordings. Users should also be able to ask their speakers about its data practices and modify their privacy settings through voice commands.

5.2 Privacy Resignation is Common and Nuanced

Our findings underline that technological development and its requisite pervasive data collection are slowly chipping away at people's agency regarding their privacy. We found that there is a spectrum of how engaged and confident people are when choosing between privacy and convenience. Some users who previously cared about personal data ownership have given it up as cloud services and IoT devices continually improve and offer evermore convenience. And while people may attempt to resist the onslaught of privacy-corroding agents, the current choice architectures of technology in general [1] and smart speakers in particular, which are often tipped in favor of more information disclosure, make it difficult to effectively manage one's privacy. Our findings further show that users adopting new technologies, especially those that may be privacy-invasive, should not be misconstrued as a sign of people accepting and endorsing privacy-invasive data practices; rather, it might be evidence of their struggle to balance the benefits of using new technologies and being forced to give up their privacy bit by bit.

Of particular concern are individuals for whom privacy resignation leads to actively avoiding the topic, potentially because they are afraid of what they might find. As a result, individuals may be unaware of privacy risks, would not go out of their way to educate themselves about data practices or privacy controls, and may not make informed decisions regarding privacy. We therefore challenge speaker designers to **design privacy notices for the most resigned users**, and prompt them to make privacy decisions that they might otherwise avoid. Smart speaker's voice interaction seems uniquely suited for this, as such prompts could be integrated into conversational interaction; for instance, after the user gives a voice command that does not suggest urgency. Such privacy decision prompts could further provide concise information about a data practice's privacy implications to users in order to nudge users to reflect on the decision's implications and take informed actions regarding their data privacy. Such interactions do not just benefit the user, the company can leverage these opportunities to highlight and explain potentially unexpected practices [51], thus limiting user surprise and helping users form accurate mental models of the smart speaker's functionality. Furthermore, smart speakers and other IoT devices should implement **privacy-friendly defaults**. Regulation may be required to create respective incentives for companies. Europe's General Data Protection Regulation (GDPR) [25] mandates stricter transparency and consent requirements, as

well as privacy-friendly defaults and data portability. Regulation and standards like this may help tip choice architectures at least slightly in favor of enhanced consumer privacy.

5.3 Privacy Tensions in Multi-User Settings

The current design of smart speakers is oriented towards control by a single user – only one user can set up the device – but usage scenarios for smart home IoT devices frequently involve multiple users. Indeed, many of our participants placed smart speakers in central locations where secondary users (other family members, roommates) and incidental users (guests and children) could access the devices. We find that users desired ways to keep certain data private from other users and manage what speaker functionality could be accessed by guests. We additionally find a similar power imbalance between primary users and non-primary users as Zeng et al. [63]. Secondary users and some of the more resigned users in our study were more likely to be unaware of privacy controls and also in more danger of being unknowingly surveilled through smart speakers. Although users may like being able to check on the audio logs and recordings of their guests and children, the latter groups may not approve. Furthermore, IoT devices and other technology have also been used as surveillance and suppression tools in cases of domestic violence and abuse [13, 26]. Those who are setting up the devices can turn the technology against others and use IoT devices to monitor, harass, and control their victims [13, 35]. Finally, connecting other smart home devices to smart speakers can make it mandatory for guests and other users to use the smart speaker to control even basic amenities, such as lighting.

Smart speaker companies and IoT device makers should adopt **multi-user-oriented user experience design** to yield more productive, comfortable and inclusive IoT environments for users of all types. This could be achieved by giving multiple user accounts equal configuration power over the device, making it easier to use the device privately without leaving traces, and limiting the amount of information that is revealed through audio logs and the smart assistant's responses.

For instance, since both Amazon's and Google's smart speakers can now also differentiate between voices [5, 42], they could adjust responses to the privacy settings of the individual who made a request. In the course of processing a request, the speaker could also detect if there were other known or unknown voices in the background and adjust its response accordingly. Following the concept of **context-adaptive privacy** [53], such contextual information together with the privacy-sensitivity of the smart speaker's response could be used to dynamically adapt the level of detail or modality of the response (e.g., display on phone instead of voice output).

Smart speakers could further reassure users that others cannot access their private data through their speaker. Additional account and privacy management options could allow users to choose what can or absolutely cannot be accessed through the speaker, and what can be accessed only after additional verification. More private information, such as addresses and banking information, could be set to always require verification.

To reduce friction between user types and prevent data from being collected without consent, speakers could automatically switch to a **guest mode** when a request is made by a voice who has not been previously registered with the speaker. In guest mode, the speaker might still perform basic functions but would not record or maintain a log of requests. This would reduce the possibility of someone using the speaker's audio logs to monitor unassuming users, such as guests. This would also protect speaker companies from collecting voice data of individuals who have not yet consented to their privacy policy or terms of service. Additionally, requests that require access to account information (e.g., playing music from another user's account, purchasing something on Amazon) could be blocked or require further authentication.

Users should also have the option to create and control **separate accounts for children**, and be able to cede control of these accounts to their children when they are older; this way, children could

gain control of their own data when appropriate. Designers should ensure that smart home devices connected to a smart speaker, such as smart lights, can still be accessed through other controls. This would allow guests or other uncomfortable users to access smart home devices without being forced to use their voice.

5.4 Current Privacy Controls Misaligned with User Needs

Although the users in our study may not consider their current voice interactions with their speaker as sensitive and did not make use of privacy controls, they did consider their phone conversations and financial information private. And while they may not currently feel safe to converse or conduct banking through their speaker, we can assume that future iterations of these products are likely to make it easier to perform more privacy-sensitive tasks. Just as how people have grown accustomed to shopping online with their credit card, it is possible that consumers will become more comfortable using smart speakers for more privacy-sensitive tasks as the functionality of the devices increase. The design of suitable and usable privacy controls for smart speakers therefore needs to advance with the smart speakers' capabilities.

Although the mute button has been recommended as a form of privacy control for other IoT devices, such as smart toys [36], this solution proved too cumbersome for our smart speaker users, who mostly did not use the mute button. Users in our study expected to be able to disable their speakers' microphones via voice commands (e.g., *"Alexa, stop listening"*), which is currently not possible. Allowing users to **mute smart speakers with voice commands** seems straightforward and would align this privacy control with how users interact with smart speakers. Such mute commands could be extended with a time duration, as some users had suggested (e.g., *"Hey Google, stop listening for the next hour"*), after which the speaker should audibly announce that it is listening again. This would address users' concern that they may forget to unmute the speaker otherwise.

Audio logs were not commonly perceived as a privacy control and are often buried in speakers' companion apps. This suggests that smart speaker companies need to **more clearly communicate audio logs as a privacy feature** to users; for instance, by making it more apparent that entries can be deleted from the interaction history, as well as helping users make the connection that reviewing audio logs is similar to looking through and deleting items from a browser history.

Users had also asked for something similar to a web browser's **incognito mode for smart speakers**, revealing that users might prefer proactive privacy controls, which allow users to take active measures to prevent data from being collected, over retroactive controls, where users have to remember to access the log to delete data after it has already been collected. Allowing users the option to activate an incognito mode manually, either through a voice command or from the companion app, could help them feel more comfortable asking more private requests if they know that the request will not be saved as an audio log/command. Ideally, smart speakers would **provide both usable proactive and retroactive privacy controls** discussed here.

6 CONCLUSION

Smart speakers are finding their way into more and more homes. While they offer hands-free convenience supported by smart voice assistants and can control other smart home devices, their 'always listening' microphones pose privacy and security risks. Although studies have examined the privacy implications of other smart home devices, there has been little research on the privacy perceptions, concerns, and privacy-seeking behaviors regarding smart speakers specifically.

Through our diary study and interviews with seventeen smart speaker users and interviews with seventeen non-users, we found privacy was not a primary consideration in users' adoption decisions but did serve as a deterrent for some non-users. Many users justify their lack of privacy concern based on an incomplete understanding of the privacy risks. However, both users and

non-users exhibit resignation to privacy loss, but at varying degrees. Smart speakers' current privacy controls are largely not used and audio logs are often not perceived as a privacy control, indicating that those controls do not meet users' needs. Instead, users have to trust that smart speaker companies will protect their privacy. We provide a number of recommendations that could provide more agency to smart speaker users regarding their privacy. Strong security and privacy standards, conversational privacy dialogs, designing privacy information with resigned users in mind, and privacy-friendly defaults could provide a better foundation for people's trust in smart speakers, as well as soften the feeling of resignation. Designing for multi-user scenarios, integrating context awareness, introducing an incognito mode, and introducing voice commands to mute microphones could further better align smart speakers' privacy controls with users' privacy needs.

ACKNOWLEDGMENTS

This research was partially funded by the University of Michigan School of Information and the Institute of Museum and Library Services (RE-01-15-0086-15). We are grateful to all of our participants and pilot participants. We also thank David Connell, Justin Petelka, Louis Spinelli, Libby Hemphill, Silvia Lindtner, and the anonymous reviewers for their helpful feedback on earlier versions of this article.

REFERENCES

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages. https://doi.org/10.1145/3054926

[2] Christopher Alexander. 1977. *A pattern language: towns, buildings, construction.* Oxford university press.

[3] Amazon. [n. d.]. Amazon Echo (2nd Generation) — Always Ready, Connected, and Fast. Just Ask. https://www.amazon.com/Generation-improved-sound-powered-design/dp/B06XCM9LJ4?

[4] Amazon. [n. d.]. Amazon Echo Dot. https://www.amazon.com/dp/B01DFKC2SO

[5] Amazon. [n. d.]. Amazon.Com Help: Alexa and Alexa Device FAQs. https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230

[6] Apple. 2017. HomePod Reinvents Music in the Home. https://www.apple.com/newsroom/2017/06/homepod-reinvents-music-in-the-home/

[7] Mike Barnes. 2017. Alexa, Are You Listening? https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening

[8] Ruth Bartlett and Christine Milligan. 2015. *What Is Diary Method?* Bloomsbury Publishing.

[9] Eric P. S. Baumer, Jenna Burrell, Morgan G. Ames, Jed R. Brubaker, and Paul Dourish. 2015. On the Importance and Implications of Studying Technology Non-Use. *interactions* 22, 2 (Feb. 2015), 52–56. https://doi.org/10.1145/2723667

[10] BBC. 2017. Amazon Hands over Echo 'murder' Data. *BBC News* (March 2017). http://www.bbc.com/news/technology-39191056

[11] BBC. 2018. Amazon Patents 'voice-Sniffing' Algorithms. *BBC News* (April 2018). http://www.bbc.com/news/technology-43725708

[12] Dieter Bohn. 2016. Google Home: A Speaker to Finally Take on the Amazon Echo. *The Verge* (May 2016). https://www.theverge.com/2016/5/18/11688376/google-home-speaker-announced-virtual-assistant-io-2016

[13] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse - The New York Times. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[14] Danah Boyd. 2007. Why youth (heart) social network sites: The role of networked publics in teenage social life. *MacArthur foundation series on digital learning–Youth, identity, and digital media volume* (2007), 119–142.

[15] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home Automation in the Wild: Challenges and Opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2115–2124. https://doi.org/10.1145/1978942.1979249

[16] J. Bugeja, A. Jacobsson, and P. Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. 172–175. https://doi.org/10.1109/EISIC.2016.044

[17] Daniel J. Butler, Justin Huang, Franziska Roesner, and Maya Cakmak. 2015. The Privacy-Utility Tradeoff for Remotely Teleoperated Robots. In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction (HRI '15)*. ACM, New York, NY, USA, 27–34. https://doi.org/10.1145/2696454.2696484

[18] Rishi Chandra. 2017. Welcoming Mini and Max to the Google Home Family. https://www.blog.google/products/home/welcoming-mini-and-max-google-home-family/

[19] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a Glass House: A Survey of Private Moments in the Home. In *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp '11)*. ACM, New York, NY, USA, 41–44. https://doi.org/10.1145/2030112.2030118

[20] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 61–70. https://doi.org/10.1145/2370216.2370226

[21] James Clawson, Jessica A. Pater, Andrew D. Miller, Elizabeth D. Mynatt, and Lena Mamykina. 2015. No Longer Wearing: Investigating the Abandonment of Personal Health-Tracking Technologies on Craigslist. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 647–658. https://doi.org/10.1145/2750858.2807554

[22] Tamara Dinev and Paul Hart. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Info. Sys. Research* 17, 1 (March 2006), 61–80. https://doi.org/10.1287/isre.1060.0080

[23] Daniel A. Epstein, Monica Caraway, Chuck Johnston, An Ping, James Fogarty, and Sean A. Munson. 2016. Beyond Abandonment to Next Steps: Understanding and Designing for Life After Personal Informatics Tool Use. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 1109–1113. https://doi.org/10.1145/2858036.2858045

[24] Adam Clark Estes. 2017. Don't Buy Anyone an Echo. https://gizmodo.com/dont-buy-anyone-an-echo-1820981732

[25] European Parliament and Council. 2016. Regulation EU 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation). *Official Journal of the European Union* (2016), 88. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[26] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 667, 13 pages. https://doi.org/10.1145/3173574.3174241

[27] Gartner. 2016. Gartner Says Worldwide Spending on VPA-Enabled Wireless Speakers Will Top $2 Billion by 2020. http://www.gartner.com/newsroom/id/3464317

[28] Google. [n. d.]. Data Security & Privacy on Google Home - Google Home Help. https://support.google.com/googlehome/answer/7072285?hl=en

[29] Google. [n. d.]. Google Home. https://store.google.com/product/google_home

[30] Greenberg, Andy. 2017. A Hacker Turned an Amazon Echo Into a 'Wiretap'. https://www.wired.com/story/amazon-echo-wiretap-hack/

[31] Jacob Kastrenakes. 2018. Google Sold over 6 Million Home Speakers since Mid-October. https://www.theverge.com/2018/1/5/16855982/google-home-sales-figures-holidays-2017

[32] Swati Khandelwal. 2017. Bluetooth Hack Affects 20 Million Amazon Echo and Google Home Devices. *The Hacker News* (Nov. 2017). http://thehackernews.com/2017/11/amazon-alexa-hacking-bluetooth.html

[33] Andreas Kirmse. 2012. *Privacy in Smart Homes*. Technical Report. http://kirmandi.rumeln.net/data/paper-Privacy.in.Smart.Homes.pdf

[34] Christoffer Lambertsson. 2017. *Expectations of Privacy in Voice Interaction–A Look at Voice Controlled Bank Transactions*. Ph.D. Dissertation. KTH Royal Institute of Technology.

[35] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875

[36] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

[37] Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them. In *Pervasive Computing*. Springer, Berlin, Heidelberg, 143–160. https://doi.org/10.1007/978-3-642-31205-2_10

[38] Aarthi Easwara Moorthy and Kim-Phuong L. Vu. 2013. *Voice Activated Personal Assistant: Privacy Concerns in the Public Space*. M.S. California State University, Long Beach, United States – California. https://search.proquest.com/docview/1513579796/abstract/DFF130DF16554E2FPQ/1

[39] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA. https://www.usenix.org/system/files/conference/soups2017/soups2017-naeini.pdf

[40] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-Term Effects of Ubiquitous Surveillance in the Home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 41–50. https://doi.org/10.1145/2370216.2370224

[41] Ty Pendleburg. 2016. Denon HEOS and Amazon Alexa Voice Control Combine Forces. https://www.cnet.com/news/denon-heos-and-amazon-alexa-voice-control-combine-forces/

[42] Yury Pinsky. 2017. Tomato, Tomahto. Google Home Now Supports Multiple Users. https://www.blog.google/products/assistant/tomato-tomahto-google-home-now-supports-multiple-users/

[43] Martin Porcheron, Joel E. Fischer, Stuart Reeves, and Sarah Sharples. 2018. Voice Interfaces in Everyday Life. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 640, 12 pages. https://doi.org/10.1145/3173574.3174214

[44] François Portet, Michel Vacher, Caroline Golanski, Camille Roux, and Brigitte Meillon. 2013. Design and Evaluation of a Smart Home Voice Interface for the Elderly: Acceptability and Objection Aspects. *Personal and Ubiquitous Computing* 17, 1 (Jan. 2013), 127–144. https://doi.org/10.1007/s00779-011-0470-5

[45] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1649–1658. https://doi.org/10.1145/2702123.2702164

[46] Alisha Pradhan, Kanika Mehta, and Leah Findlater. 2018. "Accessibility Came by Accident": Use of Voice-Controlled Intelligent Personal Assistants by People with Disabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 459, 13 pages. https://doi.org/10.1145/3173574.3174033

[47] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. (May 2017). https://doi.org/10.13016/M22K2W

[48] Joel R Reidenberg, Jaspreet Bhatia, Travis D Breaux, and Thomas B Norton. 2016. Ambiguity in privacy policies and the impact of regulation. *The Journal of Legal Studies* 45, S2 (2016), S163–S190.

[49] Johnny Saldaña. 2015. *The Coding Manual for Qualitative Researchers*. SAGE.

[50] Christine Satchell and Paul Dourish. 2009. Beyond the User: Use and Non-Use in HCI. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7 (OZCHI '09)*. ACM, New York, NY, USA, 9–16. https://doi.org/10.1145/1738826.1738829

[51] F. Schaub, R. Balebako, and L. F. Cranor. 2017. Designing Effective Privacy Notices and Controls. *IEEE Internet Computing* 21, 3 (May 2017), 70–77. https://doi.org/10.1109/MIC.2017.75

[52] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security*. Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[53] F. Schaub, B. Könings, and M. Weber. 2015. Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making. *IEEE Pervasive Computing* 14, 1 (Jan. 2015), 34–43. https://doi.org/10.1109/MPRV.2015.5

[54] Andrew Shuman. 2017. Hey Cortana, Set a Reminder: Harman Kardon Invoke Voice-Activated Speaker Available October 22. https://blogs.windows.com/windowsexperience/2017/10/20/harman-kardon-invoke-voice-activated-speaker-available-october-22/

[55] Patrick Spence. 2017. Welcome to the Sonic Internet. http://blog.sonos.com/en/welcome-sonic-internet/

[56] The Verge. 2017. Amazon may give app developers access to Alexa audio recordings. https://www.theverge.com/2017/7/12/15960596/amazon-alexa-echo-speaker-audio-recordings-developers-data

[57] Daphne Townsend, Frank Knoefel, and Rafik Goubran. 2011. Privacy versus Autonomy: A Tradeoff Model for Smart Home Monitoring Technologies. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 4749–4752. https://doi.org/10.1109/IEMBS.2011.6091176

[58] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107

[59] 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 '12)*. ACM, New York, NY, USA, 4:1–4:15. https://doi.org/10.1145/2335356.2335362

[60] Blase Ur, Melwyn Pak Yong Ho, Stephen Brawner, Jiyun Lee, Sarah Mennicken, Noah Picard, Diane Schulze, and Michael L. Littman. 2016. Trigger-Action Programming in the Wild: An Analysis of 200,000 IFTTT Recipes. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA,

3227–3231. https://doi.org/10.1145/2858036.2858556
[61] Chris Welch. 2014. Amazon Just Surprised Everyone with a Crazy Speaker That Talks to You. https://www.theverge.com/2014/11/6/7167793/amazon-echo-speaker-announced
[62] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*. ACM, New York, NY, USA, 427–434. https://doi.org/10.1145/2901790.2901890
[63] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017*. Santa Clara, CA.
[64] Don H. Zimmerman and D. Lawrence Wieder. 1977. The Diary: "Diary-Interview Method". *Urban Life; Newbury Park, Calif.* 5, 4 (Jan. 1977), 479–498. http://search.proquest.com/docview/1292940175/citation/A16505C65BA645C4PQ/1

A DIARY PROMPT – USERS

Tell us about a recent experience with your smart speaker. This could be when you have actively used it, when you considered using it but did not, or if you had accidentally used the speaker.

B INTERVIEW SCRIPT – USERS

Reasons for Adoption/Non-Adoption

- To get started, can you show use where you have your speaker? Who set it up? How did you decide to put it there? Is it alright if we take a picture? Were there any other places you considered? What did other people in the house think about putting it where it is now?
- As you know, we're interested in understanding people's perceptions of smart speakers. Can you tell us how you first heard about them? What did you think about them?
- When did you start considering getting one for yourself? What factors did you consider?
- Did you look at any other speakers? Why did you decide to get [device they entered in the screener survery]?
- Did other people factor into your decision making process (For example: children, roommates, significant other)?
- Have you used or interacted with a smart speaker before you made your decision to get one?
- When deciding to get a smart speaker, did you have any hesitations about having it in your home?
- If you received it as a gift, prior to that, did you look into buying a speaker for yourself? What factors did you consider? Was there anything that made you hesitate in using the smart speaker?

Mental Model of Smart Speakers

- How would you explain how smart speakers work to another person?
- (if technical) how would you explain this to someone who's unfamiliar with the technical terms?
- What do you think a device does with what you say?

Current Use of Smart Speakers

- How has your experience with the smart speaker been so far?
- From you diary entries, it look like you mainly use your speaker to [primary use from diary study], can you think of anything else you use it for?
- Is there anything that you could (or like) to use it for, but don't? Why?
- Do you use your smart speaker to control any other smart home devices?
- What 'apps' (Google Home) or 'skills' (Amazon) do you have installed?
- Have you set up any automations with your smart speaker?

Multi-User Scenarios

- How many people live in your home? Who can use the smart speaker and does everyone have equal access?
- When others are around, does your use of the smart speaker change? Does it change depending on who that person is (e.g. having a colleague over vs. spouse/child/sibling)?
- Do guests use it when they come over? What has that been like? What do they think of it? Do you talk to them about it (or tell guests there is a smart speaker in the home)?
- How does your current use of the smart speaker compare to when you first started using it?
- How do you forsee your use of the speakers 1, or even 2, years from now?

Specific Use and Interaction

- Are there things that you prefer to use your phone or computer/laptop for, over the smart speaker?
- Are there things that you prefer to use the smart speaker for, over your phone or computer/laptop?
- (Select a few diary entries) Can you tell us more about this specific interaction you had with your speaker?
- (If they mention any feelings) Can you tell us why you felt [feeling they mentioned] asking it that?
- Other than the uses you have included in your diary entries, has there been a time that you wanted to use your smart speaker, but didn't? Why?
- How comfortable are you asking your smart speaker to perform these tasks?
- Going back to having others around when using the smart speaker, has there ever been a situation where something went wrong? Has anyone ever voiced an opinion or concern about your smart speaker?
- Do you have any concerns when using your smart speaker?
- Have there been any instances when you forgot that the device was on? Tell us about a recent time that this has happened
- Have there been any instances where you felt uncomfortable around the device? Tell us about a recent time that this happened.
- Did you do anything to address your discomfort? What did you do? How satisfied are you with [workaround] in addressing your discomfort?

Privacy Concerns - Smart Speakers

- You mentioned privacy as a concern when first using your smart speaker, can you tell me more about that?
- (If privacy was not mentioned earlier) Some people have privacy concerns when using smart speakers, do you have a similar concern? You may not have such a concern - that's fine, and we'd like to hear about that too.
- (Pull up their history of commands) Looking at how you have used your smart speaker in the past week, are there any situations that you would like to talk about where you had a privacy concern?
- Do you have any concerns with how your smart speaker handles the privacy of your data?
  - How do you think it protects, or does not protect your privacy?
  - Do you have any particular concerns with specific people, parties, or entities?
- Do you have any concerns with how [Google/Amazon] handles the privacy of your data?
  - How do you think it protects, or does not protect your privacy
- Do you have any concerns with how the third party applications handle the privacy of your data?
  - How do you think they protect, or do not protect your privacy

Privacy Controls

- How do you feel about how your privacy is handled right now?
- Are there any ways/measures you take to protect your privacy from your speaker?
- (To see if they are aware of the mute button) How would you prevent your smart speaker from listening?
  - If they point to the mute button...
    - How often do you use this feature?
    - Can you tell me about the last time you used this feature?
  - If they do not point to the mute button...
    - (Point to the mute button) Are you aware that you can mute the speaker so that it stops listening?
    - (If yes) Can you tell me or show me how? Have you used this feature? When and how do you use it?
    - How satisfied are you with this feature?
    - (If no) Now that I told you, how do you think you can mute the device?
- (To see if they are aware of where their history is stored) Do you ever look at the audio logs of your smart speaker? Can you show us how you would to that?
  - (If yes) How do you use this feature?
  - (If no, show them how) Would you use this feature?
  - When would you/do you use this feature?

Perceptions and attitudes around 'always listening' and sharing of data

- Could you explain to me how the smart speaker would know when to respond to a command or question?
- Have you heard of the concept of the smart speaker's 'always listening'?
- How do you feel about the smart speaker 'always listening'?
- How would you describe who can see (or access) your information?
- (in relation to their mental model) Are there certain entities, people, companies, organizations, etc., you would feel uncomfortable with having your information? (Google/Amazon, family members, third parties, advertisers, government, etc.)
- What do you not feel comfortable with how your data is used?

Privacy Concerns

- (If privacy is still not mentioned) Some people are concerned for their privacy in using smart speakers in their home, was privacy a concern for you when you were considering getting one?
- (If privacy was already mentioned)You mentioned privacy as a concern when considering buying a smart speaker. Can you tell me more about that?
  - What specifically are you concerned about?
  - Do you have privacy concerns in general when it comes to technology, or is it specific to smart speakers? (below as well)

Privacy Concerns

- What does privacy mean to you?
- How does privacy fit into your life?
- Can you tell me about specific instances or concerns about privacy that you've experienced with any technologies?
- Do you have privacy concerns in general when it comes to technology, or is it specific to smart speakers?

- Can you tell me what led you to being concerned for your privacy?
- How do these concerns affect how you use technology, if at all?
- Did you have any concerns with how the [the smart speaker/ Google or Amazon / third party applications] would handle your privacy?

Privacy Controls on Smart Speakers

- When you were doing research on smart speakers, did the device's security and privacy controls factor into your decision?
- Would you consider these security and privacy controls sufficient?

Redesign

- As you might have noticed, we've been asking you a lot of questions on your privacy concerns and perceptions of your smart speaker. The reason for this is we are interested in how people think about these devices and how they would want it to fit into their lives. In a world with no limits, what would the smart speaker of your dreams look like so that you would want to use one?
  - How would it fit into your life? What kind of features would it have?
  - How would you want the smart speaker to address your concerns?
  - How do you think the device should protect your privacy?
  - What kind of privacy controls do you think the device should have?
  - Where would you put this speaker?

C INTERVIEW SCRIPT – NON-USERS

Reasons for Adoption/Non-Adoption

- As you know, we're interested in understanding people's perceptions of smart speakers. To get started, can you tell us how you first heard about them? What did you think about them?
- When did you start considering getting one for yourself? What factors did you consider?
- From the screener survey, you indicated that you do not currently own a smart speaker, can you tell us more about why you decided to not buy one?
- You mentioned [insert reasons from their survey], are there any other factors that you considered?
- Was there anything that made you hesitate in getting a smart speaker?
- When you thought about getting a smart speaker, did other people factor into your decision-making process (For example: children, roommates, significant other)?
- Have you used or interacted with a smart speaker before you made your decision not to get one?
- Had you gotten one, can you tell me how you would have used it?

Mental Model of Smart Speakers

- How would you explain how smart speakers work to another person?
- (if technical) how would you explain this to someone who's unfamiliar with the technical terms?
- What do you think a device does with what you say?

Privacy Concerns - Smart Speakers (If privacy was not mentioned)

- If cost [deciding factor] had not been a deciding factor, can you tell me where you would have placed your smart speaker?
  - Why?
  - Are there places you would not be comfortable with having a smart speaker?

Perceptions and attitudes around "always listening" and sharing of data

- Could you explain to me how the smart speaker would know when to respond to a command or question?
- Have you heard of the concept of the smart speaker's always listening?
- How do you feel about the smart speaker "always listening"?
- How would you describe who can see (or access) your information?
- (in relation to their mental model) Are there certain entities, people, companies, organizations, etc., you would feel uncomfortable with having your information? (Google/Amazon, family members, third parties, advertisers, government, etc.)
- What do you not feel comfortable with how your data is used?

Privacy Concerns

- (If privacy is still not mentioned) Some people are concerned for their privacy in using smart speakers in their home, was privacy a concern for you when you were considering getting one?
- (If privacy was already mentioned)You mentioned privacy as a concern when considering buying a smart speaker. Can you tell me more about that?
  - What specifically are you concerned about?
  - Do you have privacy concerns in general when it comes to technology, or is it specific to smart speakers? (below as well)

Privacy Concerns

- What does privacy mean to you?
- How does privacy fit into your life?
- Can you tell me about specific instances or concerns about privacy that you've experienced with any technologies?
- Do you have privacy concerns in general when it comes to technology, or is it specific to smart speakers?
- Can you tell me what led you to being concerned for your privacy?
- How do these concerns affect how you use technology, if at all?
- Did you have any concerns with how the [the smart speaker/ Google or Amazon / third party applications] would handle your privacy?

Privacy Controls on Smart Speakers

- When you were doing research on smart speakers, did the device's security and privacy controls factor into your decision?
- Would you consider these security and privacy controls sufficient?

Redesign

- As you might have noticed, we've been asking you a lot of questions on your privacy concerns and perceptions of your smart speaker. The reason for this is we are interested in how people think about these devices and how they would want it to fit into their lives. In a world with no limits, what would the smart speaker of your dreams look like so that you would want to use one?
  - How would it fit into your life? What kind of features would it have?
  - How would you want the smart speaker to address your concerns?
  - How do you think the device should protect your privacy?
  - What kind of privacy controls do you think the device should have?
  - Where would you put this speaker?

D PARTICIPANT SCREENING SURVEY

- Are you currently over the age of 18? (Yes or No)
- Do you currently own a smart speaker, such as Amazon Echo or Google Home? (Yes or No)

If the respondant answered yes to this question:

- Which smart speaker(s) do you have? (Amazon Echo, Amazon Tap, Amazon Dot, Google Home, Other - fill in the blank)
- How did you obtain your smart speaker(s)? (I purchased it, I received it as a gift, I won it as a prize, Other - fill in the blank)
- How long have you been using your smart speaker? (<1 month, 1-3 months, 3-6 months, 6 months to a year, for more than a year)
- How often do you use your smart speaker(s)? (Every day, a few times per week, once a week, a few times per month, once a month, a few times per year, almost never)
- How many smart speakers do you own? (1, 2, 3 or more)

If the respondant answered no to this questions:

- Have you considered buy a smart speaker for use in your home? (Yes or no)

If the respondant answered yes to the previous question:

- Can you tell us more about why you decided not to buy a smart speaker for your home? (Open ended text response)

Demographics

- Age (Open ended text response)
- Gender(Female, Male, Prefer not to say, Other - fill in the blank)
- Highest level of education completed (High School, Vocational/Technical School (2 years), Some college, Bachelor's Degree, Master's Degree, Doctoral Degree, Professional Degree (MD, JD, etc.))
- Which of the following best describes your primary occupation? (Administrative Support (e.g., secretary assistant), Art, Writing, or Journalism (e.g., author, reporter, sculptor), Business, Management, or Financial (e.g., manager, accountant, banker), Education or Science (e.g., teacher, professor, scientist), Engineering or IT Professional (e.g., programmer, IT consultant), Homemaker, Legal (e.g., lawyer, law consultant, or law professor), Medical (e.g., doctor, nurse, dentist), Service (e.g., retail clerk, server), Skilled Labor (e.g. electrician, plumber, carpenter), Unemployed, Retired, Student (Undergraduate), Student (Graduate, Doctoral), Other - fill in the blank)
- Name (Open ended text response)
- Email (Open ended text response)

E PARTICIPANT DEMOGRAPHICS

Participant demographics for smart speaker users are provided in Table 1, and for non-users in Table 2.

Table 1. Users Demographics and Smart Speaker Data

ID	Smart Speaker Type	Use Span	Age	Gender	Primary Occupation
U01	Amazon Tap	6mo–1yr	18-25	Male	Engineering or IT Professional
U02	Amazon Dot	<1mo	18-25	Male	Student (Undergraduate)
U03	Amazon Dot	1–3mo	18-25	Male	Engineering or IT Professional
U04	Google Home	6mo–1yr	36-45	Male	Engineering or IT Professional
U06	Google Home	<1mo	26-35	Female	Engineering or IT Professional
U07	Amazon Echo	6mo–1yr	18-25	Male	Student (Graduate, Doctoral)
U08	Amazon Echo, Dot	>1yr	65+	Male	Retired
U09	Amazon Echo, Dot (x2)	6mo–1yr	36-45	Female	Education or Science
U10	Google Home	1–3mo	36-45	Male	Business, Management, or Financial
U11	Google Home	3-6mo	26-35	Male	Student (Graduate, Doctoral)
U12	Amazon Dot	1–3mo	18-25	Male	Engineering or IT Professional
U13	Amazon Dot (x2)	3-6mo	36-45	Male	Education or Science
U14	Amazon Echo, Dot	>1yr	26-35	Female	Art, Writing, or Journalism
U15	Amazon Echo, Dot	>1yr	26-35	Male	Business, Management, or Financial
U16	Amazon Dot	<1mo	26-35	Male	Education or Science
U17	Amazon Dot	6mo–1yr	N/A	Female	Homemaker
U18	Amazon Echo, Dot	>1yr	N/A	Male	Skilled Labor

Table 2. Non-users Demographics

ID	Age	Gender	Primary Occupation
NU01	18-25	Female	Student (Undergraduate)
NU02	18-25	Male	Service
NU03	18-25	Male	Student (Graduate, Doctoral)
NU04	18-25	Male	Engineering or IT Professional
NU05	18-25	Male	Student (Undergraduate)
NU06	46-55	Male	Student (Graduate, Doctoral)
NU07	N/A	Female	Service
NU08	18-25	Male	Education or Science
NU09	46-55	Male	Engineering or IT Professional
NU10	18-25	Male	Student (Undergraduate)
NU11	36-45	Male	Engineering or IT Professional
NU12	26-35	Male	Student (Graduate, Doctoral)
NU13	26-35	Female	Student (Graduate, Doctoral)
NU14	36-45	Female	Engineering or IT Professional
NU15	26-35	Male	Student (Graduate, Doctoral)
NU16	26-35	Male	Business, Management, or Financial
NU17	26-35	Female	Education or Science

Received April 2018; revised July 2018; accepted September 2018