Blackout and Obfuscator: An Exploration of the Design Space for Privacy-Preserving Interventions

Varun Chandrasekaran, Thomas Linden, Kassem Fawaz, Bilge Mutlu, Suman Banerjee
University of Wisconsin-Madison

ABSTRACT
The pervasive use of smart speakers has raised numerous privacy concerns. While work to date grants us an understanding of user perceptions of these threats, limited research focuses on how we can mitigate these concerns, either through redesigning the smart speaker or through dedicated privacy-preserving interventions. In this paper, we present the design and prototyping of two privacy-preserving interventions: ‘Obfuscator’ targeted at disabling recording at the microphones, and ‘Blackout’ targeted at disabling power to the smart speaker. We present our findings from a technology probe study involving 24 households that interacted with our prototypes aimed to gain a better understanding of the design space for technological interventions that might address these concerns. Our data reveals complex trade-offs among utility, privacy, and usability and stresses the importance of multi-functionality, aesthetics, ease-of-use, and form factor. We discuss the implications of our findings for the development of subsequent interventions and the future design of smart speakers.

INTRODUCTION
Smart speakers, representing network-connected speakers with integrated virtual assistants, are becoming increasingly pervasive in households. By the end of 2019, 200 million smart speakers will be present in the market worldwide, with 46% of the devices in US households [32]. Smart speakers offer their users a convenient way to access information, set alarms, play games, or set to-do lists. Smart speakers also integrate with other devices to realize smart home applications. However, this convenience comes at a potential privacy cost; these devices operate in always-on mode at earshot of nearby conversations.

Smart speakers already provision built-in privacy controls: they are supposed to process audio inputs locally until they detect a wake word, and they pack a button that mutes their internal microphone. Unfortunately, both provisions are not very effective at protecting the user’s privacy. Recent incidents raise concerns about perceived privacy threats [1, 21, 22, 17]. Smart speakers can mistakenly be triggered without the presence of a wake word [15, 20], causing it to record speech not intended as commands. Further, security researchers have documented actual vulnerabilities that indicate the potential for malicious exploitation of smart speakers [26, 14, 8, 13, 36]. The effectiveness of the mute button to address these problems is in doubt [21]. Recent studies, including the one in this work, indicate that users find this button inconvenient to utilize and is not trustworthy in some cases.

As a result, there is a need to investigate more convenient and trustworthy privacy controls for smart speakers. We believe that the design space for such interventions is underexplored and that design research into defining its elements and understanding user experience with these interventions is required. While the privacy issues surrounding smart speakers are of more immediate interest, our exploration can inform the design of privacy-preserving technologies in physical spaces.

In this paper, we aim to better understand the user perceptions around the potential technological solutions to the privacy issues involving smart speakers. In particular, we conceptualized and prototyped two technology probes [16]. The objective of our study is not to validate our particular design choices, but to better understand user perceptions of such interventions and extract design requirements for them. We utilize the smart speaker’s built-in mute button as a baseline, to understand user perceptions of how device manufacturers provide privacy control. Both our prototypes are bolt-on privacy-preserving interventions: (a) Blackout, a smart plug that allows the user to engage/disengage the power supply to a smart speaker remotely, and (b) Obfuscator (Figure 1), which uses ultrasound to deafen the smart speaker’s microphone, preventing the smart speaker from listening to nearby conversations. The probes intercept two key resources required for successful smart speaker functionality: power (for basic operation) and microphone inputs (for voice-based interaction).

To promote user reflection on our privacy-preserving interventions, we conducted in-home demonstrations of our technology probes through in-depth interviews at 24 households. Our interviews took place over two phases in the course of a year.
providing us with insight into how such perceptions and attitudes might change over time. Our interviews involved users with diverse demographics, including casual (or recreational) users and power users, enabling us to distinguish perceptions and design requirements for different user groups. Our findings highlight a complex trade-off between privacy, utility, and usability: the interventions (a) should be plug-and-playable i.e. require minimal setup and upkeep, (b) have a small physical footprint and fit within its environment, (c) offer additional features beyond privacy preservation, (d) do not affect the interaction model with the smart speaker, and (e) must survive the test of time i.e. it should be compatible with existing and future iterations of smart speakers. In the remainder of the paper, we present the design of our technology probes and our in-home study, and discuss our findings. We conclude with a discussion of their implications for the smart speakers as well as other privacy-sensitive technologies.

**BACKGROUND**

Our study considers two popular smart speakers: (a) Google Home Mini and (b) Amazon Echo Dot. A smart speaker has to be always on, continuously listening for a user to speak a wake word, such as “...Alexa” or “...Google.” Ideally, the device should only record, and communicate to its cloud, the commands that were triggered by a wake word; the detection of wake words happens on the device. In many circumstances, however, the device’s operation might not match its expected behavior giving rise to two privacy threats.

The first occurs due to compromise of the actual device or its operation. A malicious entity can compromise the software running on the smart speaker to turn it into a listening device. Such an entity can also change the operation of the device through developing applications that record the user’s conversations [37, 20, 26] or inject stealthy commands to wake up the device without the user’s awareness [28, 36, 5]. We refer to such threats as actual privacy threats.

The second may occur due to innocuous recording i.e. when the speaker misunderstands ongoing conversations to contain the wake word. Figure 2 shows the portal of a popular smart speaker referencing instances were recordings where originally misinterpreted as queries to the smart speaker. We refer to such threats as perceived privacy threats. It is unclear when and how smart speakers are spuriously activated, and what is done with the collected information. There have been several incidents where devices have exported user conversation, including those not preceded with a wake word. While one organization claims this is a one-off act [15], the other blame erroneous code [8, 12]. Further, there have been reported instances where several organizations hired human contractors to listen and tag different recordings from these devices, which include commands and non-commands [13].

**METHODOLOGY**

Two strategies exist to safeguard users’ privacy against both actual and perceived privacy threats: (a) redesigning the smart speaker to provide provable privacy guarantees, and (b) designing interventions that co-exist with the smart speaker. The former is a challenging proposition as most of the software and hardware required for successful smart speaker functioning is proprietary. To this end, we focus on the latter option and explore the design of bolt-on, hardware-based interventions through our technology probe approach [16]. Hardware-based interventions are less abstract than software-based ones; they allow the participants to physically and directly interact with the interventions. In contrast, software-based interventions involve no such interaction with complex and potentially untrustworthy software. For thoroughness, we compare and contrast our findings with usage of a built-in feature found in smart speakers—the mute button. Through the results of our research, we can inform better design of smart speakers, and privacy-preserving interventions in general in physical spaces.

In designing our technology probes, we followed an iterative design process. We first explore the broad space of solutions (presented in Table 1), their efficacy against an adaptive adversary, and discussed the advantages and disadvantages of each approach. It is clear that modifying device hardware and controlling network flow do not provide the desired properties. While one could change the wake word to reduce the frequency of spurious activation/renording, this phenomenon is not well understood for it to be a definitive fix.

![Figure 2: The portal of a smart speaker showing statements that were incorrectly interpreted as queries.](image)

We converged on a set of dimensions which we found relevant to the final design of our interventions. These dimensions include (a) the method of user interaction with the intervention i.e. hands-free vs. physical, (b) the ease of deployment, and (c) the ease of understanding the privacy properties the intervention provides. We stress that these dimensions are not exhaustive. We do not seek to evaluate the efficacy of each of these interventions in preserving privacy. We do not attempt to understand how people use these interventions as well. Doing so requires running a long-term study with the intervention deployed in users’ homes. We follow a technology probe [25] approach to understand how the users of smart speakers react

| Possible Solutions | Actual Threats | Perceived Threats |
|--------------------|----------------|------------------|
| Network interception | ✗ | ✗ |
| Hardware modifications | ✗ | ✗ |
| Change the wake word | ✗ | ✓ |
| Discard smart speaker | ✓ | ✓ |

Table 1: Broad space of possible solutions and their effectiveness against malicious programming (or actual privacy threats) and inadvertent recording (or perceived privacy threats).

We converged on a set of dimensions which we found relevant to the final design of our interventions. These dimensions include (a) the method of user interaction with the intervention i.e. hands-free vs. physical, (b) the ease of deployment, and (c) the ease of understanding the privacy properties the intervention provides. We stress that these dimensions are not exhaustive. We do not seek to evaluate the efficacy of each of these interventions in preserving privacy. We do not attempt to understand how people use these interventions as well. Doing so requires running a long-term study with the intervention deployed in users’ homes. We follow a technology probe [25] approach to understand how the users of smart speakers react
to different privacy-enhancing technologies using proof-of-concept prototypes.

We describe the interventions used in our study, including those we conceptualized, below.

**Mute**: The “mute” feature represents a built-in privacy control (Figure 3a). It is conveniently available as a push button on the top panel of the Amazon Echo Dot and as a sliding button on the side of the Google Home Mini. The device manufacturers state that the microphone is deactivated when the mute button is turned on. Naturally, activating the mute button stops the smart speaker from responding to the user’s voice commands. Upon activation, the Echo Dot’s ring color changes to red, and the four lights atop the Google Home Mini turn red. The mute feature, however, requires the user to physically interact with the device to engage/disengage the control, and to place trust in the manufacturer’s implementation of the muting feature.

**Blackout**: While the mute button focuses on disengaging the microphone inputs, we conceptualize another intervention to disengage the electricity supply, causing a “blackout.” A naive way of achieving our goal is to either disconnect the smart speaker’s cord from the outlet or disconnect the cord connected to the smart speaker. However, both options involve physical interaction with the device, which might be tedious if the devices are concealed. Thus, we use a remote-controlled outlet1 (Figure 3b). The user deploys Blackout by connecting the smart speaker to the outlet through the smart plug (as seen in Figure 3b). We use a commercial smart-plug because we believe that users will be familiar with such products, minimizing their time for acclimatization. Additionally, we believe that users will trust the functionality of such widely-used products. Blackout is conspicuous and rugged: we believe that its form factor makes it easier to understand and use. The user can engage/disengage Blackout through a remote control (with a range of operation of 100 feet) without the need to physically interact with the device. Additionally, the smart plug we chose provides a visual cue — an LED glows red when powered on to indicate that the smart speaker is active.

Clearly, Blackout offers immediate privacy guarantees. This comes at a cost; the users have to wait for a lengthy boot time whenever they wish to reuse the smart speaker. Additionally, the form factor of Blackout makes it difficult to use in some environments (with concealed/narrow outlets).

**Obfuscator**: This intervention targets the microphone of the smart speaker (Figure 3c). Obfuscator generates inaudible ultrasound to deafen the microphone of the smart speaker when the user needs privacy protection (Figure 4a). Using a remote control, users are able to engage/disengage the intervention without having to physically interact with it. When disengaging the jamming, the user can immediately interact with the smart speaker. Due to non-linearities in off-the-shelf microphones’ power and diaphragm [28, 27, 36, 10], Obfuscator creates high-power, human-inaudible noise at these microphones but does not affect its operation otherwise.

Figure 4b shows the captured signals from a commodity microphone before and after Obfuscator is engaged. Before jamming is invoked, the microphone records a conversation which is audible at playback. After engaging Obfuscator, the ultrasound jamming signal is recorded at the microphone, and completely overwhelms the conversation’s signal.

**Design Evolution**: Obfuscator’s circuitry includes a DC power supply that is a remote-controlled, an ultrasound generator (produces signals at 27 kHz), and a horn speaker that emits the ultrasound signal. We explored different design options for the prototype that houses the circuitry. A challenge in prototyping Obfuscator was the relatively large footprint of the circuitry as compared to the other interventions. Additionally, horn speakers are bulky, and reducing their size considerably inhibits their effectiveness.

---

1Beastron Remote Controlled Outlet

---

Figure 3: The three employed privacy interventions.

Figure 4: The system design of the Obfuscator intervention.

Figure 5: The design evolution of the Obfuscator intervention.
Our design process started with a search for a privacy metaphor, one that creates the perception of privacy control for the users. Our initial prototype was based on a “cage” metaphor. Here, the Obfuscator intervention is housed in a cage-like structure with a door, and the smart speaker is placed within the cage. When the user closes the cage door, Obfuscator generates the ultrasound obfuscation signal to prevent the smart speaker from listening. The user has to manually open the door to disable obfuscation and communicate with the smart speaker. Closing the door “locks” the device in a cage, providing a user with a perception that the device is not active and their space is private. Opening the door unlocks and opens up the smart speaker to the user’s space.

The first version of the Obfuscator intervention followed the cage metaphor as a 3D printed cylinder (Figure 5a). The cylinder has two compartments; the lower chamber containing the circuit and the ultrasound speaker. The upper chamber has space for the smart speaker as well as the door. The first version has a height of 15.5 cm and a diameter of 12 cm. We refined the cage-based design into a smaller, lighter and less conspicuous 3D-printed cylinder (Figure 5b) with a height of 13 cm and a diameter of 11 cm.

Based on pilot studies with 2 participants, we found both versions to be neither user-friendly nor fitting with home decor. Participants explicitly indicated that this design was not something they would want in their homes. Further, we observed that individuals did not associate with the privacy metaphor. First, they did not favor the idea of physically interacting with the prototype as it takes away the convenience of using a hands-free device. Second, covering the smart speaker inside the cylinder deprives the users of the ability to observe the visual cue. This is a short-coming of placing the smart speaker within the intervention. Finally, they thought that the actions of opening and closing the prototype door was conspicuous, and would label them as privacy-conscious in the eyes of others.

We factored these opinions into designing a third version of the prototype. We considered three aspects that the users were not fond of: physical interactions with the door, covering the smart speaker, and the aesthetics. The third version of the prototype (Figure 5c) features a platform-like solution which addresses those shortcomings. This version has a glass cylinder which houses the circuit and the ultrasound speaker. The upper chamber is 11 cm and diameter is 12.5 cm. The platform, where the smart speaker sits, is encased with synthetic leather. The user can engage/disengage the jamming signal via remote control, obviating the need for physical interaction. This version of the Obfuscator intervention follows a different privacy metaphor: “virtual veil.” By engaging the jamming signal, Obfuscator creates a virtual privacy dome around the smart speaker, preventing it from listening to the conversations. Our subsequent discussions and reflections about this version revealed that the open nature of the prototype might not enforce the privacy metaphor; users are less likely to perceive privacy control over the smart speaker. This version remains co-located with the smart speaker, increasing its form factor. This is not ideal in scenarios where the smart speaker is concealed.

The design search process led to our final prototype of the Obfuscator intervention, as shown in Figure 3c. We substantially reduced the form factor of the final version. The new prototype houses the same circuitry in a glass candle holder. The glass is filled with decorative sand and sealed with burgundy burlap. The user only needs to place the prototype next to the smart speaker. This prototype is built using commonly found household artifacts, enabling it to fit in with existing decor. This final prototype represents a technology probe that allows us to identify the design guidelines for privacy enhancing interventions in the smart speaker ecosystem. The probe packages the core functionality of the privacy intervention: a jamming device which enforces the privacy metaphor. We kept the prototype as simple and basic as possible to avoid making design decisions [4] that influence our findings. In our study, we use the prototype to elicit participants’ reflections about what design elements are missing and need to be introduced.

In-home User Study

We recruited 24 families (including single individuals) within a 15-mile radius of a university campus, utilizing the university mailing list, over two phases. Our first phase included 13 interviews, while the second phase (10 months later) included 11 interviews. We chose to perform shorter and focused interviews as opposed to longer studies (such as diary studies); the tech probe approach allowed us to capture our many goals related to capturing baseline privacy perceptions, introduce the privacy priming, and gain reflection upon interacting with the interventions. The results reported in the paper are based on interviews with 30 participants ($P_1 - P_{30}$) from these 24 interviews. Our data coding and analysis started immediately and took place simultaneously with data collection, enabling us to monitor the emergence of new codes and themes and determine saturation. We reached saturation by the 18th interview and collected data from 6 more households to assess how perceptions evolve with time. Our approach exhibits several limitations, the most important of which is the sampling of a relatively ethnically homogeneous population; the reported results are less likely to generalize to another population of users. We sought to recruit participants with different backgrounds in age, educational background, and technological proficiency. Our participant pool comprised of 15 males and 15 females. The youngest participant was 12 years old, while the oldest was 67 (with a mean age of 37.4 and standard deviation of 13.9). The occupations of the participants ranged from students to faculty. The wide spectrum in age and profession enables us to gain feedback from a pool with varied technical knowledge and awareness, and offers a breadth of experiences and backgrounds that are useful to analyze user interactions with the interventions.

We conducted all interviews in the participants’ homes at a time of their convenience. Each interview lasted for 90 minutes on average, and the participants were compensated for their time ($40 USD per study). The study protocol was approved by our Institutional Review Board (IRB). We conducted the interview in three stages, which we elaborate below.

\[^2\text{Some households had more than one participant.}\]
1. Environment Exploration: The interview began with the participants providing a brief tour of their home. Emphasis was placed on the rooms with smart speakers. Then, the interviewer and the participants convened in the room with the frequently used smart speaker, so as to simulate a common usage scenario. After obtaining informed consent, the interviewer provided each participant with an online questionnaire to fill. This pre-interview questionnaire contains a set of four questions on a Likert scale to capture the participant’s privacy baseline. We utilize the “Concern for Privacy” [24] scale which is modeled after the well-known “Information Privacy Concern scale” developed by Smith et al. [30], related to online services. The objective of the pre-interview questionnaire was to establish baseline privacy perceptions. After the questionnaire, the interviewer asked more detailed questions about the smart speaker’s role in the participant’s life. The questions focused on frequency, duration, and the purpose of usage. Also, the questions covered the conversations and activities participants have around their smart speakers. Then, the interviewer inquired about the participant’s degree of trust in these devices (in terms of the potential for their conversations to be recorded), and trust in their manufacturers and hypothetical third parties (with whom the recordings might be shared/leaked). The interviewer asked whether individuals have read the news or heard anecdotes about unexpected or undesirable behaviors by the smart speakers. These questions created the appropriate context to discuss privacy-preserving interventions; while our questionnaire and follow-up questions are capable of biasing the participants, we believe that they are essential in creating the right environment to discuss the ambiguous space of privacy issues surrounding smart speakers.

2. Interaction with Interventions: In a randomly generated order, the experimenter briefly introduced the capabilities of each intervention. The participants were given time to familiarize themselves with the intervention and set it up. By setting up the intervention themselves, we expected the participants to gain greater familiarity with its operation. The random ordering of intervention across participants helped to reduce ordering effects. In settings with families, the interviewer asked different family members to interact with the intervention individually. After setting up the intervention, the interviewer asked the participant to issue voice commands after engaging/disengaging the intervention. At each step, the interviewer probed the participant about their level of comfort with the intervention and how it impacts the usability of their smart speaker. The participants were encouraged to envision future use-cases for each intervention and stress-test the intervention’s functionality.

After the interaction with each intervention, the interviewer inquired about the participant’s level of trust in the intervention. Based on the nature of the response, the interviewer asked several follow up questions to determine reasons for high/low levels of trust. The interviewer proceeded to discuss perceived privacy control, trust level, convenience, and aesthetics of the interventions. These interview questions were designed to elicit critical reflections.

3. Concluding Discussions: After interacting with the three interventions, the interviewer engaged the participants in an open-ended discussion about the interventions and their impact on their privacy. The interviewer then administered another survey (to determine any changes in their privacy perceptions over the baseline measurements). This post-questionnaire asked the same privacy-related questions as the pre-interview survey, but contained questions to collect demographics information. Finally, the participants received compensation.

All interviews were audio-recorded, resulting in over 30 hours of recordings; photographs were taken of (a) the interventions in action and (b) the areas where the smart speaker is typically used. We then transcribed, coded and analyzed the interviews using a Grounded Theory approach [6, 11]. The coding was performed with two coders working independently. Our coders were in moderate agreement, with a Cohen’s Kappa (κ) of 0.57 [31]. We started the analysis with an open-coding stage to identify more than 200 informal codes that define critical phenomena in the interview transcripts. Using these informal codes, we extracted recurrent themes within the transcripts and converged on a set of 85 formal codes. We further refined the formal codes into 15 axial codes. Finally, we organized the codes into four major themes as summarized in Table 2.

FINDINGS

In this section, we present and discuss the four key themes that emerged from our analysis. In summary, we found that:

1. Participants were reluctant in sacrificing the convenience associated with smart speakers; hands-free interaction was most preferred, and physical interaction was seen as being not ideal.

2. Participants expected bolt-on interventions with existing household decor and to offer cues informing them of the state of both the intervention and the smart speaker.

3. Multifunctionality, fine-grained control (per-user and per-device), and cost of the intervention are important factors that might influence adoption.

4. While participants believed in both actual and perceived privacy violations, they were comfortable with their conversations being overheard because they believed that their conversations were not sensitive (in comparison to personally identifiable information available using their location/web footprint).

User Attitudes regarding the Smart Speakers

Types of Users: Through our study, we identified two types of users: (a) casual users who utilize their smart speakers for setting alarms, inquiring about the weather, asking questions etc., and (b) power users who have integrated the smart speakers with other devices in their homes (such as smart lights, house monitoring systems etc.). We also observed that while most participants in our first interview phase were casual users, a majority of the users in the second interview phase belonged to the latter category. This phenomena could be based on the pervasive availability and easy installation of various smart home devices. We observed that power users were also more familiar with various perceived privacy violations and with the
We observed that users in the second interview phase were aware of recent privacy violations. We expect that power users will be more willing to adapt privacy-preserving interventions as they have more to lose if their devices were compromised, i.e., as their households were more tightly integrated with the smart speaker, compromising the smart speaker could be the gateway to more exploits. We also observed that a majority of the participants did not change their conversations around the smart speakers (in comparison to conversations in rooms without smart speakers), but a small minority reported feeling conscious of having discussion around them.

Understanding of smart speaker operation: We observed that a minority of the participants were unaware of how smart speaker’s operate, i.e., they were unaware that their vocal commands were processed off-site, and were used to improve the machine learning algorithms used. Participant P5, for example, believed that the smart speakers did "some local learning but also some more... I think at some point people were involved in [the processing]... I think there’s an automated learning that occurs to adjust itself to the household right?" These perceptions were shared across participants with different educational backgrounds.

Trust in device manufacturers: Trust in the device manufacturers fragmented our participant population. This includes fractions (a) that believed that these organizations can be trusted; their belief comes from faith in the legal system which would penalize organizations if there is evidence indicating malpractice, (b) that believed that some manufacturers were not in the business of collecting personal information and can be trusted, (c) that trusted the manufacturers, but believed that any information collected could be leaked, or shared with other organizations they do not trust, and (d) that trusted the manufacturers as long as there is personal utility from their information being collected. A recurrent theme was participants’ comfort in being recorded because they believed they were part of a large pool of smart speaker users, and their vocal footprint provided corporations no additional insight into their lives. Participant P10 states, "I mean we’re not planning any nefarious capers... like we’re very boring people and therefore nothing that we’re talking about would be of interest to anyone on the other end of [the smart speaker]."

Some participants justified this notion by commenting on the nature of advertisements they received after introducing the smart speaker in their homes; P5 states "the way Google that Google ads operates ... you know if... I talk about something; it starts showing up ... if I’m scrolling through Facebook".

Vocal footprint vs. other sources of information: Some participants suggested that the vocal footprint shared with smart speakers is both limited and not as informative as their web footprint and location information. Participant P2 states, "my information is certainly more out there on social media than it is [with smart speakers]. I also don’t feel like I have anything to hide... I mean if they use my information it’s going to be for some monetary reason like to sell to me". These participants also believed that social engineering is a more potent form of harm than audio-based profiling. Participants’ perceptions did not conform to academic attack models. While we observed that participants were comfortable if their conversations were overheard, they were uncomfortable if the entity overhearing is a human i.e. participants were more comfortable with algorithms digesting their information. However, all participants agreed that recording and storing data was unacceptable.

User Attitudes regarding the Interventions

State of operation: Participants believed that the current designs of the interventions make it too inconvenient to use the smart speaker. They state that using privacy preserving interventions makes the interaction with a smart speaker a two-phase procedure: first check the state of the intervention (engaged vs. not) and disengage if necessary, and then interact with the smart speaker. They claim that the additional set of steps defeats the purpose of owning a smart speaker i.e. to have spontaneous interactions. Some participants stated that the interventions added a mental burden in terms of remembering the state of the intervention. Participant P3 stated: "when you were to power it off say how do you distinguish that state [when it has no power when using Blackout] from a wake word doing nothing, like I don’t know I unmutate this right now ... it looks the same." Participants believed that owning these interventions will serve as a contingency if there is documented evidence of foul play; P3 states "we lock our doors at night; it’s [the proactive step]... nothing bad might happen... it’s insurance pretty much."

Ergonomics: Participants were comfortable with the usability of the interventions. The interventions were easy to set up and use, and the time taken for the intervention to get engaged is acceptable (almost instantaneous in all cases). However, participants expressed dissatisfaction at the longer boot-up times induced by Blackout. For example, P3 stated, "I would find it especially irritating”. Participants suggested that technologies such as Obfuscator that, when disengaged, make the smart speaker immediately available were ideal; P3 explains, "I’d probably lean more towards something like [the Obfuscator] over even like just the outlet for the convenience factor of like you can turn that off with a button and not really have to worry about [the Dot] like warming up." Some partici-
pants were concerned about the generalizability of Obfuscator. They believed that the technology is specific to their smart speakers, and would not extend to future smart speakers or smart speakers made by other vendors. Participants were also comfortable with the interventions because they were not connected to the network (and thus believed that the Obfuscator intervention will not be a privacy violation). Their comfort levels with the interventions were tied to their belief that manufacturer heterogeneity introduces greater privacy protection, i.e., neither Blackout nor Obfuscator were manufactured by the smart speaker manufacturers. In fact, participant P₁₀, when asked if they had a preference over the intervention developer, replied: "I wouldn’t but I’m sure like older generations would feel much more comfortable ... if it came from McAfee."

We observed that participants unanimously found the mute-button the least convenient intervention; the act of walking to the smart speaker to engage/ imposed a significant usability barrier. Participants were more comfortable using a remote control, but felt that their homes have many remotes, and that the remotes could be easily misplaced. In fact, when proposing the addition of another remote, P₉ exclaimed, "they're all over the place, so many remotes! We can’t have another remote." Some participants suggested moving intervention control to a mobile phone app; unlike remote controls, participants believed that their mobile phones were less prone to being misplaced and alleviate other issues pertaining to remotes. While participants enjoyed the convenience of using the remote control, they were apprehensive in imagining a voice-controlled intervention (as they were informed of how smart speakers currently process voice commands off-site).

Trust in bolt-on interventions: Finally, participants trust bolt-on interventions more than the built-in mute button. Participants suggested that trust in the bolt-on intervention would be low if it came from the device manufacturer, or any organization that had a similar business model. Participant P₁₃ recommended "a competing company or just a general company that seems like they’re like honest" could develop the interventions. Participants suggested that bolt-on interventions were easier to debug, and were easier to understand. However, participants feel that purchasing one bolt-on intervention for every smart speaker is not economically feasible.

Aesthetics and Physical Footprint
With regards to the mute button, participants felt comfortable with its design and placement, while finding it inconvenient to use. A very small fraction of the participants were unaware of the existence of the mute button, and an even smaller fraction were unaware of its utility.

Physical Footprint: Participants were concerned with the physical footprint of our designed interventions. While smart speakers were electronic devices, participants often associate them with decorative items (Figure 6) and invest effort in determining where these devices should be placed. A common example of a description about the Obfuscator solution we received was P₁’s description: "a piling on of devices". Some participants found it difficult to reorganize other items around the smart speaker to facilitate the intervention. Additionally, some participants prefer to conceal their outlets, and Blackout-like interventions were inconvenient in such scenarios. Participants were uncomfortable with interventions that involve additional wires (as in the case of Obfuscator).

Cues: Another point of contention is the utility of visual cues in the interventions. Recall that Blackout has an LED indicator that glows red when engaged; participants found the color of the indicator a red herring — the red color led participants to believe that the device was malfunctioning. This situation is further exacerbated in the scenario where participants preferred to have their outlets hidden. Participants did not notice that the interventions had visual cues, and believed that this complicated understanding its state. While participants found the visual cues uninformative in some settings, they did state that having cues relieves burdens associated with ascertaining device/intervention state. They suggested that other cues, which should be more informative, would be preferred in such situations. For example, P₇ states that they would like to "see the video [of the Obfuscator signal] feedback to the [listening] device, but have [the Obfuscator haptic light] go green when it’s working."

Preference towards built-in solutions: Some participants suggested that they would prefer a trustworthy built-in intervention: this could be designed as software updates (or skills) that could be added to the smart speaker. They argue that built-in interventions were preferred as they do not add to the physical footprint of the smart speaker, and it does not add additional economic strain. Building upon what was discussed earlier, participants suggested that their ideal built-in intervention should also be voice activated. We argue that the previous statements (with regards to the trustworthy built-in interventions) were oxymorons i.e. an intervention that is built-in can not be trustworthy as it is produced by the organization that is allegedly violating privacy. How one can design such an intervention, potentially using techniques from cryptography and secure hardware design, is out of the scope of this paper.

Utility of the Interventions
Damage to environment: Participants were concerned that Obfuscator will cause harm to animals present in their homes; questions we received upon presenting the Obfuscator were often like P₂’s, "is [this] going to ... make my dog crazy?". While we did not observe any agitation/discomfort, the participants suggested that their pets could perceive the ultrasound
signals, and were not bothered by it. Additionally, participants were concerned about exposing their smart speakers to ultrasound for a prolonged period of time. Again, a detailed study is needed to understand the impact of ultrasound on electronic devices.

Cost and Multi-Functionality: Cost was repeatedly discussed; participants suggested that the cost of the interventions should not exceed the cost of the smart speaker. Some participants received their smart speakers as gifts, and were unaware of their market value. Consequently, they were unable to establish a value for the intervention; P8 states, "that’s a really interesting question in the sense that I didn’t pay for this in the first place. Maybe that’s also another reason that I don’t have much investment in using this in general". On the other end of the investment spectrum, we observed that participants who owned multiple smart devices were invested in safeguarding their privacy, and were willing to adopt the interventions independent of the cost. Participant P8, who had previously stopped using their smart speakers due to privacy concern, even stated that they would consider using their device once more given that the intervention were, “cheap... I think would have to rival that remote plug-in cost right because ... it has to be like a cheap utility ... or a cheap accessory like that.”

Participants were also concerned about the amount of electricity consumed by Obfuscator. Obfuscator could be used in a proactive way i.e. always-on, or in a reactive way i.e. use when needed. Participants felt that a reactive approach, though tedious, would be easier to understand. Participants also believed that a (potentially high) cost could be justified if the intervention provided multiple features. This could be achieved by integrating the design of Obfuscator with other home decor, such as lamps, lights, clocks, radios etc.

Fine-Grained Control: The final observation we make is an extension to multi-functionality; we observed that in some households, some participants preferred to utilize the intervention more than others. In such scenarios, they desired customized usage profiles based on their requirements i.e. fine-grained control per-user. Another observation we make is that some participants preferred to have one intervention (like Obfuscator) being used to preserve privacy against a wide range of smart speaker-like devices. In such scenarios, fine-grained control per-device was desired. Based on the current design of the Obfuscator prototype, meeting both these requirements is challenging, and requires further research.

DESIGN IMPLICATIONS
In our observations and analysis, several themes emerged which offer the following implications (Table 3) for the design of privacy-preserving interventions for smart speakers.

1. Aesthetics
The interventions should be offered in different forms, shapes, and colors, enabling easier integration within their home decor. As individual tastes vary widely, devising a one-fits-all design is challenging. One possible approach is to explore different design options for different types of users, including shapes, forms, colors, and material. This approach has been successful with smart speakers, where participants feel comfortable with the aesthetic of the smart speaker. For example, Amazon has four offerings of their Echo product featuring combinations of forms and fabric colors. With time, participants perceived the smart speaker’s design to become more polished, from an inexpensive plastic exterior, to more refined design (with fabric and different colors). Participants expressed similar concerns about Blackout, but stressed more upon its physical footprint, which we discuss next.

2. Physical Footprint
The footprint of the intervention should be small enough to not force a reorganization of the layout of owner’s house.

3. Multi-Functionality
The intervention is better when providing additional functionality (such as a clock) to reduce its footprint and integrate better with home decor.

4. Ease of Deployment and Understanding
Battery-powered interventions are easier to deploy. Also, proper understanding of the privacy metaphor improves the adoption of interventions.

5. Trust in Technology
Trustworthy interventions are: bolt-on, not network connected, designed by a different trustworthy organization, and pose no additional risk.

6. Mode of Interaction
Using the intervention should not change the interaction with the smart speaker. Hands-free interaction is most preferable.

7. Informative Cues
Interventions should offer cues that communicate their state. Visual, auditory, or text cues might be applicable depending on the deployment.

8. Cost
The intervention should cost less than the smart speaker.

9. Fine-grained Privacy Control
The intervention can offer per-user and per-smart speaker privacy controls.

10. Awareness
Awareness of privacy violations increases trust in intervention designers.

Table 3: Summary of the identified design guidelines.
of the horn speaker in our current prototype was chosen to ensure maximum ultrasound distribution and coverage. Extending such a design to smart speakers that are larger, or have a different orientation for the microphone inputs will require rethinking the design and form factor.

3. Multi-Functionality: Closely tied to the aesthetics, participants indicated preference toward an intervention (specifically Obfuscator) that offered features beyond privacy-preservation. They suggested that the Obfuscator intervention could be combined with other household artifacts, such as a lamp, radio, clock etc. Doing so reduces the footprint of the intervention. Multi-functionality provides an alternative avenue for customizing the product, making it easier to integrate with existing household decoration. Participants who are worried about the social stigma of being labeled as overly privacy-conscious would benefit from such designs, i.e., the intervention would be inconspicuous. Another interpretation of this point could be to envision interventions as artifacts that co-exist with the smart speaker, such as a stand to hold the smart speaker, or a sleeve for the smart speaker. There is a demand for such artifacts based on our analysis of reviews for such products, and we believe such designs would promote adoption.

4. Ease of Deployment and Understanding: Participants preferred to have a solution that was easy to deploy in their homes; the biggest impediment to any intervention similar to Blackout is its physical footprint. Many participants preferred to conceal the interventions’ wiring, and the nearby outlets can be hard to reach. Attaching Blackout to wall outlets, even once, requires considerable re-positioning of other devices and their wires. Attaching Obfuscator would require an additional outlet, which is not always readily available. One naïve solution would be to split the outlet among multiple devices. Participants suggested that an Obfuscator design capable of operating on batteries would be more preferred, even if this required periodic replacement. Participants also suggested that since the current version of an Obfuscator-style intervention will not operate in an always-on mode, the energy consumption will be limited. All participants were able to easily grasp the metaphor associated with Blackout, but the technology behind Obfuscator proved complicated for some. Thus, interventions whose operation is easy to explain may be preferred. While Obfuscator is easy to use once deployed, debugging it may pose problems for users who are lack proper understanding of its operation. We also believe that understanding the detriments (if any) of ultrasound towards humans, animals, and other electronics may put users at ease.

5. Trust in the Technology: Participants were more comfortable with technologies that they believe will survive the “test of time,” i.e., be useful for smart speaker models in the future. The privacy guarantees of Blackout can be thwarted by smart speakers that are battery operated. However, thwarting Obfuscator’s guarantees is more challenging and would potentially require much more expensive microphones. As discussed earlier, trust also stems from knowing that the interventions do not pose any additional risk. Specifically, we observed that (a) participants wanted to know about any detriments introduced by the interventions such as potential damage to the smart speaker by frequently disconnecting it from its power source or subjecting it to ultrasound; and (b) our current interventions are not network connected and do not present the same risks as the smart speakers. Finally, participants preferred our bolt-on interventions as opposed to the built-in interventions as they were designed by an organization they trusted (more than the smart speaker manufacturers).

6. Mode of Interaction: We observed that participants placed a high value on the convenience of using smart speakers from which they are not willing to compromise. Thus, interventions that, when disengaged, delay the smart speaker operation (as in the case of Blackout) are not preferred (even though Blackout provably preserves privacy, and its mode of operation is very easy to understand). Additionally, any form of physical interaction, be it using remotes or buttons, is far from ideal; some participants expressed preference toward using an app on their smartphones. We believe that future privacy-preserving solutions must be designed so as to disrupt the convenience of the use of these systems minimally. An ideal design would have a voice interface that allows the user to control it as they control their smart speakers. However, such an always-on and listening privacy-preserving solution can have the same pitfalls as smart speakers, and they must be designed in a manner that does not erode user trust. For example, the can lack a network interface to provide the users with hard privacy assurances. Another issue that may arise with voice-activated interventions is erroneous activations; understanding how this can be minimized requires additional research.

7. Informative Cues: As stated earlier, some participants concealed their smart speakers and would prefer concealing their interventions as well. Some participants take this notion to the extreme; they believe that any electronic device that does not provide extensive visual information should be concealed. Thus, visual cues are not ideal in all situations. Additionally, participants suggested that the red light on the Blackout intervention suggested that the intervention was broken, as opposed to indicating the state of the intervention. Interacting with the smart speaker when the intervention is enabled helps users determine the state of the smart speaker (operational vs. not), but such an approach is reactive. Participants indicated preference for a proactive approach. Combined with the observation that visual cues are not informative, we believe that auditory cues may be preferable. The Obfuscator-style intervention can announce using speech or text that the smart speaker is inactive when users try to activate it.

8. Cost: Another factor that impacts adoption is cost of the smart speaker. A large fraction of our participants own smart plugs similar to Blackout, leading us to believe that such an intervention is affordable. However, the cost of prototyping Obfuscator was $70, exceeding the cost of smart speakers (priced at approx. $30). This cost includes the price of the commodity parts needed to construct the prototype. Participants believe that the cost of the intervention should not exceed the cost of the smart speaker; this is especially true if the intervention can provide privacy-protection against a single
smart speaker. We believe that if such an intervention would be adopted widely, the production costs could be amortized. Additionally, understanding the engineering requirements to design an Obfuscator-like intervention that provides privacy against various smart speakers located at different parts of a home requires independent research.

9. Fine-grained Privacy Control: Several households owned more than a single smart speaker, and they had members with different (and potentially conflicting) privacy requirements. Thus, we believe that there is a requirement for (a) fine-grained control per user and (b) fine-grained control per smart speaker. For the latter, a naïve solution would be to deploy one intervention for every smart speaker in the household, but depending on the cost per intervention, such a solution may not scale. Thus, an ideal design would provide privacy protection for more than one smart speaker. This design could be conceptualized as smaller interventions co-located with the smart speakers but controlled centrally. Providing per-user control is a more challenging problem; it requires understanding how disparate the privacy requirements are, how frequently users are utilizing a smart speaker together, and how to mitigate conflicts should they arise. Providing a solution to this problem requires additional research [35].

10. Effect of Awareness: Based on our pre- and post-interview questionnaires, we observed the following trend amidst the participants of our interview phases. The participants of our second phase are more concerned about the potential privacy threats from the smart speakers (in comparison to the participants of the first phase, who are also concerned). This concern stems from increased awareness; recent smart speaker mishaps, erroneous code used in them, and immoral practices by device manufacturers have led to an increasing concern amongst the participants. Based on our discussion, we observed that participants believe that these issues are not being seriously audited by the device manufacturers. Discussing various loopholes that can be implemented in the built-in interventions in the status quo (i.e., local wake word processing, and the mute button) also increased participants’ awareness. Due to these factors, participants believe that interventions created by third parties (who do not share the same business motives as the device manufacturer) provide the desired privacy properties.

RELATED WORK
Privacy Perceptions: The methodology of our study is most similar to Zheng et al. [38], and Kaaz et al. [18]; however, their objective is different. They attempt to understand the privacy perceptions of users living in homes with various IoT devices. Similar to our work, surveys are carried out in [7, 23, 3], where the authors try to identify the various challenges associated with setting up and using these devices. Zeng et al. [34] and Lau et al. [21] attempt to understand smart speaker users’ reasons for adoption through a combination of a detailed diary study and in-home interviews. Similar to this work, we observe that smart speaker users are not privacy conscious because of the lack of value they associate with their conversational data. Along a similar vein, Abdi et al. [1] find that users have incomplete mental models of smart speakers. Similar to our work, they use this understanding to present design recommendations. Some of our findings are coherent with those of Malkin et al. [22], e.g., participants are unaware that their conversations are being recorded and stored.

We stress that the primary contribution of our work is not in ascertaining the privacy perceptions people have about smart speakers (as done in earlier studies). We wish to understand users’ perceptions towards privacy-enhancing technologies and to use this insight to guide future design of both smart speakers and such technologies.

Intervention Design: Prior research has investigated system-level solutions to these privacy threats. Feng et al. [9] propose continuous authentication as a mechanism to thwart privacy issues related to smart speakers. Gao et al. [10] propose using ultrasound jamming to address stealthy recording. In this work, we wish to validate the usability claims made by the above; consequently, we base our intervention design on the above proposals. Other solutions involve intercepting/monitoring traffic at the network gateway [2, 29]. However, such solutions fail when network traffic is encrypted. A maliciously compromised device can cache recorded conversations and leak them, using a valid skill, in a stealthy manner. A network-level solution would be ineffective in preventing these types of privacy leaks, especially when the attacker introduces code to react maliciously to voice inputs [20].

The Alias project [19] is designed to achieve similar goals to ours. This solution constantly plays noise through a small speaker placed atop the smart speaker and stops the noise upon hearing a custom wake word. Their solution differs from Obfuscator in two ways. First, the Alias intervention does not use ultrasound; the reduced form factor is achieved by not using horn speakers, which are crucial for transmitting ultrasound. The noise generated by the Alias prototype may be bothersome to pets and potentially to people. Second, the Alias intervention obscures the visual cue provided by the smart speaker; such a design is not preferred.

Design Studies: To safeguard privacy and security in the smart home, Zeng et al. [35] prototyped a smart home app and evaluated its effectiveness through a month-long and in-home user study with seven households; the users are assumed to be non-adversarial and cooperative. They used their findings to guide future designs for smart home applications. To achieve similar goals as ours, but for smart homes (as opposed to smart speakers), Yao et al. [33] adapted a co-design approach and designed solutions with non-expert users. We borrow our study methodology from the work of Odom et al. [25]; technology probe studies serve multiple purposes related to designing, prototyping, and field testing the interventions.

CONCLUSIONS
We presented the design and prototyping of two privacy-preserving interventions: ‘Obfuscator’ targeted at disabling recording at the microphones, and ‘Blackout’ targeted at disabling power to the smart speaker. We presented our findings from a technology probe study involving 24 households that interacted with our prototypes, aimed to gain a better understanding this design space. Our study revealed several design
dimensions for the design of privacy interventions for smart speakers.
REFERENCES

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In Symposium on Usable Privacy and Security (SOUPS).

[2] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. 2017. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. arXiv preprint arXiv:1708.05044 (2017).

[3] AJ 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. ACM, 2115–2124.

[4] Marion Buchenau and Jane Fulton Suri. 2000. Experience prototyping. In Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 424–433.

[5] Nicholas Carlini, Pratyush Mishra, Tavis Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. 2016. Hidden voice commands. In 25th {USENIX} Security Symposium ({USENIX} Security 16). 513–530.

[6] Kathy Charmaz and Liska Belgrave. 2012. Qualitative interviewing and grounded theory analysis. The SAGE handbook of interview research: The complexity of the craft 2 (2012), 347–365.

[7] 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. ACM, 41–44.

[8] CNN. Google admits its new smart speaker was eavesdropping on users. http://tiny.cc/dwyvcz. (????).

[9] Huan Feng, Kassem Fawaz, and Kang G Shin. 2017. Continuous authentication for voice assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking. ACM, 343–355.

[10] Chuhun Gao, Varun Chandrasekaran, Kassem Fawaz, and Suman Banerjee. 2018. Traversing the Quagmire that is Privacy in your Smart Home. (2018).

[11] Barney G Glaser and Anselm L Strauss. 2017. Discovery of grounded theory: Strategies for qualitative research. Routledge.

[12] Google Home Help. [Fixed issue] Google Home Mini touch controls behaving incorrectly. https://support.google.com/googlehome/answer/7559221?hl=en. (????).

[13] The Guardian. Apple contractors regularly listen to recordings. http://tiny.cc/tryvcz. (????).

[14] Kashmir Hill and Surya Mattu. 2018. The House That Spied on Me. https://gizmodo.com/the-house-that-spied-on-me-1822429852. (2018).

[15] Gary Horcher. Woman says her Amazon device recorded private conversation, sent it out to random contact. https://kiro.tv/235OLwp. (????).

[16] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B. Bederson, Allison Druin, Catherine Plaissant, Michel Beaudouin-Lafon, Stéphane Conversey, Helen Evans, Heiko Hansen, Nicolas Roussel, and Björn Eiderbäck. 2003. Technology Probes: Inspiring Design for and with Families. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’03). ACM, New York, NY, USA, 17–24. DOI: http://dx.doi.org/10.1145/642611.642616

[17] Haoqian Jin, Minyi Liu, Kevan Dodhia, Yuanchun Li, Gaurav Srivastava, Matthew Fredrikson, Yuvraj Agarwal, and Jason I Hong. 2018. Why Are They Collecting My Data?: Inferring the Purposes of Network Traffic in Mobile Apps. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 2, 4 (2018), 173.

[18] Kim J Kaaz, Alex Hoffer, Mahsa Saeidi, Anita Sarma, and Rakesh B Bobba. 2017. Understanding user perceptions of privacy, and configuration challenges in home automation. In Visual Languages and Human-Centric Computing (VL/HCC), 2017 IEEE Symposium on. IEEE, 297–301.

[19] Bjorn Karmann. Project Alias. http://bjoernkarmann.dk/project_alias. (????).

[20] Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey. 2018. Skill squatting attacks on amazon alexa. In 27th {USENIX} Security Symposium ({USENIX} Security 18). 33–47.

[21] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW) (2018).

[22] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. Proceedings on Privacy Enhancing Technologies 2019, 4 (2019), 250–271.

[23] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The contextual complexity of privacy in smart homes and smart buildings. In International Conference on HCI in Business, Government and Organizations. Springer, 67–78.

[24] George R. Milne and Mary J. Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices. Journal of Interactive Marketing 18, 3 (2004), 15 – 29. DOI: http://dx.doi.org/https://doi.org/10.1002/dir.20009
[25] William Odom, Richard Banks, David Kirk, Richard Harper, Siân Lindley, and Abigail Sellen. 2012. Technology Heirlooms?: Considerations for Passing Down and Inheriting Digital Materials. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’12). ACM, New York, NY, USA, 337–346. DOI: http://dx.doi.org/10.1145/2207676.2207723

[26] Danny Palmer. 2018. Amazon’s Alexa could be tricked into snooping on users, say security researchers. https://zd.net/2qXadSj. (2018).

[27] Nirupam Roy, Haitham Hassanieh, and Romit Roy Choudhury. 2018b. BackDoor: Sounds that a microphone can record, but that humans can’t hear. GetMobile: Mobile Computing and Communications 21, 4 (2018), 25–29.

[28] Nirupam Roy, Sheng Shen, Haitham Hassanieh, and Romit Roy Choudhury. 2018a. Inaudible Voice Commands: The Long-Range Attack and Defense. In 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18). USENIX Association, 547–560.

[29] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehan. 2015. Network-level security and privacy control for smart-home IoT devices. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on. IEEE, 163–167.

[30] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals’ Concerns about Organizational Practices. MIS Quarterly 20, 2 (1996), 167–196.

[31] Anthony J Viera, Joanne M Garrett, and others. 2005. Understanding interobserver agreement: the kappa statistic. Fam med 37, 5 (2005), 360–363.

[32] voicebot.ai. 2019. Smart Speaker Statistics. http://tiny.cc/4lxvcz. (2019).

[33] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. ACM, 198.

[34] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In Symposium on Usable Privacy and Security (SOUPS).

[35] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In 28th {USENIX} Security Symposium ({USENIX} Security 19). 159–176.

[36] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taemin Zhang, and Wenyuan Xu. 2017. DolphinAttack: Inaudible voice commands. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 103–117.

[37] Nan Zhang, Xianghang Mi, Xuan Feng, XiaoFeng Wang, Yuan Tian, and Feng Qian. 2019. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. IEEE, 0.

[38] Serena Zheng, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Privacy in Smart Homes. arXiv preprint arXiv:1802.08182 (2018).