Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes

Haojian Jin
haojian@cs.cmu.edu
Carnegie Mellon University
Pittsburgh, Pennsylvania

Boyuan Guo
boyuang@andrew.cmu.edu
Carnegie Mellon University
Pittsburgh, Pennsylvania

Rituparna Roychoudhury
ritu.19roy@gmail.com
Carnegie Mellon University
Pittsburgh, Pennsylvania

Yaxing Yao
yaxingyao@umbc.edu
Univ. of Maryland, Baltimore County
Baltimore, Maryland

Swarun Kumar
swarun@cmu.edu
Carnegie Mellon University
Pittsburgh, Pennsylvania

Yuvraj Agarwal
yuvraj@cs.cmu.edu
Carnegie Mellon University
Pittsburgh, Pennsylvania

Jason I. Hong
jasonh@cs.cmu.edu
Carnegie Mellon University
Pittsburgh, Pennsylvania

Abstract

In this paper, we studied people's smart home privacy-protective behaviors (SH-PPBs), to gain a better understanding of their privacy management do's and don'ts in this context. We first surveyed 159 participants and elicited 33 unique SH-PPB practices, revealing that users heavily rely on ad hoc approaches at the physical layer (e.g., physical blocking, manual powering off). We also characterized the types of privacy concerns users wanted to address through SH-PPBs, the reasons preventing users from doing SH-PPBs, and privacy features they wished they had to support SH-PPBs. We then storyboarded 11 privacy protection concepts to explore opportunities to better support users' needs, and asked another 227 participants to criticize and rank these design concepts. Among the 11 concepts, *Privacy Diagnostics*, which is similar to security diagnostics in anti-virus software, was far preferred over the rest. We also witnessed rich evidence of four important factors in designing SH-PPB tools, as users prefer (1) simple, (2) proactive, (3) preventative solutions that can (4) offer more control.

CCS Concepts

• **Human-centered computing** → **Human computer interaction (HCI)**.

Keywords

Smart Home; privacy protective behaviors

ACM Reference Format:
Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3491102.3517602

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3517602

1 Introduction

In recent years, there has been growing interest in supporting users' privacy-protective behaviors (PPBs) on the web, allowing users to actively manage and protect their privacy [3]. Some examples include using tracking prevention tools (e.g., ad blockers or Do Not Track functions in a browser), periodically deleting web browser history and cookies, and entering fake information in web forms [17]. Previous studies have investigated how and why users adopt or reject PPBs in various contexts, such as identity theft [52], privacy lies [38], and web privacy tools [39].

However, an emerging yet less studied PPB context is how people manage privacy in smart home environments, which we refer to as smart home privacy-protective behaviors (SH-PPBs). Supporting SH-PPBs has many differences from the online context. For instance, users need to manage multiple smart devices running continuously in the background, each with different sensing capabilities that can collect private data, and each located in potentially sensitive locations within the home. These devices might also collect the data of people besides the primary user, such as roommates, guests, passersby, and neighbors. While there is limited support for empowering SH-PPBs compared to online PPBs, smart home early adopters are improvising tricks to protect their privacy. For example, on reddit, there have been online discussions on how to program smart plugs to power off cameras at certain hours [35], how to purchase devices that are still functional without cloud access [33], and how to place smart cameras inside the home to minimize privacy concerns [34].

We conducted two online surveys to understand existing SH-PPBs and explore potential opportunities to better support users' SH-PPB needs. Our first survey (N=159) used open-ended questions to investigate the practices, contexts, and desired improvements of users' SH-PPBs, as well as the barriers preventing users from taking

[Character, Context]
John installed numerous smart home devices around multiple rooms in his house for security, sleep monitoring, video calling, watching entertainment, etc.

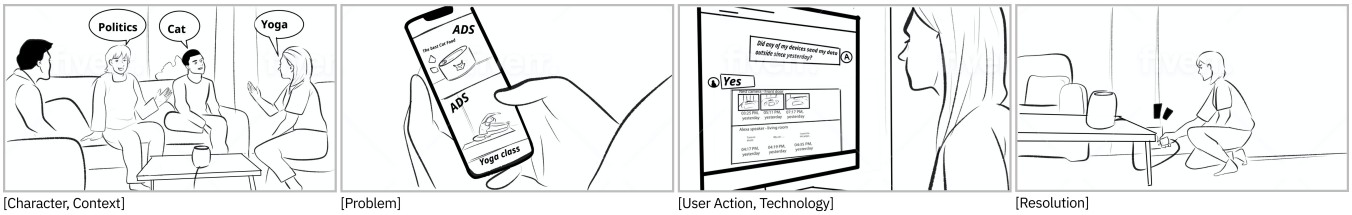
[Problem]
When setting up these devices, John tried to review and customize privacy settings. However, the descriptions of privacy setting options are confusing. Tired of looking through the app, John decided to continue with the default settings.

[Problem]
Lately, John read a report about hackers conduct privacy violations on the same type of voice assistants that he is using. The report criticized flaws in the voice assistant's default privacy settings.

[User Action, Technology]
John installs a privacy diagnostic app that can analyze and rate the privacy settings across all his devices. After the initial run, the app gives him a 72/100. It also pointed out where he lost points and gave step-by-step instructions on how he might improve the score.

[Resolution]
By following the app suggested instructions, John earned a 100/100. Now, he feels safer and more comfortable with all the devices.

Figure 1: Out of 11 different storyboards we created based on participants' wishlist features, *Privacy Diagnostics* was ranked as the most favored feature in 63% of the comparisons, when participants ranked three randomly selected storyboards. *Privacy Diagnostics* is a mobile app that can assess the smart home configurations across all the smart home devices and offer step-by-step instructions on how to improve the score. Participants praised it for "being simple," "offering privacy control," and "requiring little management efforts."



[Character, Context]
Annie installed multiple smart home devices in her living room. One day, she had some random conversations with her friends in the living room.

[Problem]
The next day, Annie noticed many Ads related to last night's discussion. She suspects that her smart home devices must have leaked her data.

[User Action, Technology]
Annie installs a tool that enables her to manage devices through a chatbot. She asks the chatbot, "Did my devices send my data out yesterday?" The chatbot reports all data that got sent out last night.

[Resolution]
Annie realizes that her conversations accidentally triggered the smart speaker, and part of her discussion was shared with Ads companies. She now decides to unplug the device whenever she has visitors over.

Figure 2: One of the less preferred SH-PPB storyboards was *Privacy Chatbot*, which was ranked as the least favored feature in 52% of the comparisons with other features. *Privacy Chatbot* monitors all the network data from smart home devices and allows users to ask privacy questions in plain English. However, participants criticized this feature since it "requires extra mental burden," "cannot prevent data leaks," "offers limited control options."

part in SH-PPBs. This survey offers insights into users' current SH-PPB practices (§4.1) and their specific needs for supporting SH-PPBs (§4.2). Our second survey (N=227) then asked participants to critique and compare privacy protection concepts that we created based on the needs observed in the first survey, similar to the process of UX speed dating [8]. In doing so, we addressed two limitations of the first open-ended survey. First, participants often have a limited understanding of how devices work and what potential privacy threats a smart home may introduce, making it difficult for them to speculate about concepts beyond their own experiences. Second, commercial products only offer limited privacy support, and most users have a relatively low baseline when evaluating a new privacy feature. This makes it hard to prioritize the privacy features to implement and identify important factors in designing SH-PPBs. Specifically, we created 11 storyboards, each depicting a privacy protection concept and how the concept might be used to address a privacy concern (see Figs. 1, 2, 9-17). We then asked each participant to critique three randomly selected storyboards in open-ended questions (i.e., what do people like/dislike about these scenarios?), and rank in order of their preference among the three concepts. We used the Plackett-Luce method [26] to merge these partial rankings into a global ranking across 11 concepts, similar to how the Elo rating system ranks chess players. We also analyzed the qualitative critiques and ranking rationale to identify the factors that most strongly influence the preference of a concept.

These methods allowed us to answer the following three research questions:

RQ1. What kinds of SH-PPBs are people already conducting, how often, and why? Our findings suggest that more than half of our participants (52%) actively do some kind of SH-PPB, despite the limited support and tedious effort required. The majority of reported SH-PPBs rely on ad hoc physical protection (57/80), such as powering off or physical blocking, while only two participants (1%) mentioned using third-party tools (e.g., Pi-Hole [13]). Among the 33 unique SH-PPBs we identified, the most common is participants manually unplugging a device based on different contexts.

RQ2. What types of support do users wish to have? Conversely, for people that have few or no SH-PPBs, what are the barriers that prevent them from doing so? Participants reported 18 types of wishlist features to enhance their SH-PPB experiences. The most popular one is a way to turn off (e.g., unplug) smart devices "really easily". Participants also wished to have more control of data collection (e.g., turning a camera's microphone off) and better privacy awareness (e.g., visual reminders for data collection). Indeed, most reported privacy features are reasonably easy to implement but do not exist in today's ecosystem. On the other hand, the most important SH-PPB barriers are "unaware of smart home privacy threats," followed by "lacking knowledge and tools" and "requiring too much effort."

RQ3. What are potential opportunities for building tools to support future SH-PPBs? Of the 11 storyboards, a simple technique we called *Privacy Diagnostics* (Fig. 1), which is similar to security diagnostics in many kinds of anti-virus software, was preferred the most and far ahead of the rest. We note that only one participant in the first survey expressed desire for this feature, suggesting the usefulness of our online speed dating approach. We then used the quantitative rankings of storyboards to guide the analysis of the qualitative responses. We also witnessed rich evidence of

four important factors in designing SH-PPB tools, as users prefer (1) **simple**, (2) **proactive**, (3) **preventative** solutions that can (4) **offer more control**.

Contributions: This paper makes the following contributions.

- We present the first study that systematically studies what users do and don't do in managing their privacy in smart home today. This study identifies 33 unique types of smart home privacy-protective behaviors, and finds that users heavily rely on protections at the physical layer and on ad hoc approaches.
- We present the results of online speed dating on 11 different privacy protection concepts based on needs observed from our first study. We found that a relatively simple technology, *Privacy Diagnostics*, was preferred far ahead of the rest in our study. We also identify four important factors in designing SH-PPB tools: simple, proactive, preventative solutions, and more control.

2 Related work

We have organized related studies into two categories: understanding privacy concerns in smart homes and privacy-protective behaviors.

2.1 Understanding Privacy Concerns in Smart Homes

Many studies have investigated users' privacy perceptions of smart home technologies [1, 2, 20, 23, 25, 37, 45, 48, 50, 51]. For example, Malkin et al. found that people were unsure of how smart TVs handled personal data, such as what data was collected, and how that data was used, re-purposed, and shared with third-parties [25]. Parents who bought smart toys for their children were concerned about whether their children's data would be collected and shared [27]. Children were concerned about whether their parents would be able to monitor them and hear their conversations through their toys [27]. Past research also found that users' privacy concerns vary across different data collection contexts [2], such as consent procedures, brands, data types. For example, Worthy et al. found that people's trust towards those entities that collected their data was associated with whether they would desire control of their information [45]. They argued that if users had less trust, they would seek a greater level of control [45]. Zheng et al. found that some people believed that entities collecting their information protect their data carefully [50].

In contrast, our study focuses on how users **mitigate** their privacy concerns (RQ1 & RQ2). Past privacy concern studies have identified a few SH-PPBs through semi-structured interviews when participants cited them as anecdotal evidence to illustrate their privacy concerns. For example, Zeng et al. [48] reported two security and privacy mitigation strategies through interviewing 15 participants: isolating smart home devices in a separate network and only using indoor cameras when users are away. However, these serendipitous findings can hardly scale and generalize. Indeed, Zeng et al. suspected that users might change their behaviors to mitigate privacy risks but did not find such SH-PPBs. In contrast, we specifically examined SH-PPBs through surveys, offering a more comprehensive and systematic views of common SH-PPBs. For example, our results show that a few users modify their behaviors to mitigate privacy risks, such as dodging cameras and speakers.

2.2 Online and Smart Home Privacy-Protective Behaviors

There also has been much work on understanding the adoption of online PPBs, such as changing privacy settings based on the platform and audience [11], deleting online content completely [5], hiding true identity through lying to a partner [42], and adopting ambiguous language [5] and privacy lies [38]. Recent studies find that conducting online PPBs remains challenging for many users despite broad support. For example, when users mistakenly believed that web browsers provide online behavioral advertisement, they would clear the browsing history more often and deemed it an effective way to protect their privacy [47]. In contrast, we focus on the less studied context of a smart home, aiming to improve the understanding of existing SH-PPBs and explore opportunities to better support users' SH-PPB needs.

Past research has shed light on users' SH-PPB needs. For example, Yao et al. found that users want data localization, a private mode, and a network intrusion detector to have more control of their data [46]. In addition, Tabassum et al. found that users expect to give consent before smart devices share their data explicitly (e.g., conversation) [40]. However, these studies often only offer a few high-level principles, since they involve few participants, and users can hardly speculate beyond their own experiences. In contrast, the scale of our study allows us to build an understanding of users' SH-PPB needs in a bottom-up approach, grounded in users' actual SH-PPB experiences (RQ2). These insights further guided us to generate attractive privacy protection concepts.

Meanwhile, researchers and practitioners are actively developing privacy-enhancing technologies to support users' SH-PPB needs. For example, a user now can either unplug the smart speaker to protect sensitive conversations being recorded [29] or use a mute button to stop it from recording temporarily [21]. Users can also delete the conversation log in the app associated with smart speakers [21], set up access controls based on either the tasks that users are trying to accomplish [12] or the specific user who is trying to use the devices [12, 41, 49], and use third-party tools (e.g., IoT Inspector [14]) to increase their awareness of the data collected by smart home devices. However, most of these proposals are studied independently and evaluated with a relatively low baseline, making it hard to prioritize the features to implement for future products and identify the critical design factors. To fill this gap, in this study, we derive a large number of privacy protection concepts, compare them head to head, and offer a list of the pros and cons for each concept (RQ3).

3 Method

In this section, we describe our study protocol, recruitment process, and analysis methods.

3.1 Study procedure

We organized our SH-PPB exploration into two separate online surveys. The first survey posed open-ended questions to participants (N=159), asking them to share their SH-PPB experiences. This

broad exploration helped us understand existing SH-PPBs while also learning users' needs to improve their existing SH-PPBs and search for new ones. Based on the findings from the first survey, we derived 11 privacy protection concepts (Table 7) and created structured storyboards to communicate the usage contexts of these concepts. We used a modified *speed dating* [8] method to evaluate these storyboards with a different set of participants through the second online survey (N=227).

3.1.1 SH-PPB Inquiry surveys: (Fig. 3) Participants were first asked about their perceptions of the severity of online privacy threats (e.g., "Having companies collect my online behavior is a problem for me?") and their online PPB experiences based on a set of questions adapted from a previous study [3]. We then asked about the types and the number of devices they have deployed in their homes. We used an initial list of 15 device types, supported by a popular home automation platform Home Assistant, and allowed participants to report any additional devices as freeform text.

We then presented participants with a short tutorial on SH-PPBs. We walked participants through a broad definition of SH-PPBs adapted from the online PPB context [3]: "*any strategies and actions you take to mitigate the collection, usage, and sharing of your personal information from these smart home devices to protect your privacy.*" To continue filling out the survey, participants had to correctly answer a 3-item quiz to distinguish SH-PPBs from other interactions. Participants received feedback on incorrect answers, which they must then correct to proceed. In doing so, we made sure that users have a correct understanding of SH-PPBs.

After passing the quiz, participants were asked whether they have any SH-PPBs to share and were reminded that we offer a $1 bonus for each valid SH-PPB. Those who had SH-PPBs to share were then asked to describe the SH-PPB, relevant devices, associated privacy concerns, frequency of use, perceived effectiveness, and what features they wish were available to improve their SH-PPB experiences. Participants who reported online PPBs in the earlier questions but had no SH-PPBs to share were asked to elaborate on any differences between SH-PPBs and online PPB experiences.

3.1.2 Generating storyboards: We first summarized users' specific needs for supporting SH-PPB by analyzing the wishlist features and the barriers that prevent users from conducting SH-PPBs. We then sought privacy protection ideas described in research papers (e.g., [9, 10, 18, 19, 28]) and online forums (e.g., [30, 32, 35]) that can potentially address the discovered needs. We discuss the storyboard selection criteria and process in §6.3. A typical challenge in soliciting users' feedback on a technology they have never experienced before is that users can hardly speculate on the imagined future and how technology could modify their behaviors. So, instead, we use a *speed dating* [8] like approach, presenting situated applications in a storyboard and asking participants to critique the storyboard. All storyboards (Figs. 1, 2, 9-17) contain 4-5 frames, covering the context, problem, privacy protection concept, and users' reactions, which are derived from the first survey's responses. To ensure that storyboards have similar fidelity, the authors first created textual scripts and then hired a freelance illustrator to make all the storyboards.

3.1.3 Speed dating surveys (Fig. 4): We adapted the *speed dating* method, initially designed for semi-structured interviews, to online surveys. The key idea is to force users to critique and compare a few reasonable promising privacy protection concepts, which can help us understand the factors that most strongly influence the preference of a privacy protection concept. A major challenge in adapting *speed dating* to surveys is the participant engagement required in terms of time to compare 11 storyboards. To address this, we asked each participant to critique three randomly selected storyboards around two questions. The first question, "Could you relate to the concern?" was used to validate whether the observed users' needs are aligned with the actual needs perceived by users (i.e., concept validation). The other question, "Does this tech address the concern?", was to assess how well the proposed concept could address those needs (i.e., need validation). We asked participants to offer a 5-point Likert assessment for both questions and elaborate their reasoning in one open-ended question (>80 characters).

After the individual assessments, we posed an attention check question requiring them to select the three storyboards they viewed among all eleven storyboards. To help participants pass the attention check, we primed participants on the question at the beginning of the survey. After passing attention check questions, we asked participants to rank the three viewed storyboards and explain the rationale (>140 characters).

3.1.4 Survey development and pilot tests: Before officially launching the surveys, we ran three rounds of pilots (N=10) for each study and then iterated on the survey design based on the quality of the responses. For the first survey, the main challenge was to incentivize users to reflect on their PPB experiences, so we introduced the bonus compensation design. We iterated on the second survey to determine the number of storyboards each participant needs to review. We also added attention check questions to help us filter out inadequate responses.

3.2 Recruitment and Demographics

We surveyed smart home users through TurkPrime [24], a participant-sourcing platform for online research and surveys. To avoid priming, we advertised the survey as a "smart home technology survey" rather than one specifically about privacy. We restricted the survey to participants located in the United States, and mentioned that "participants need to have some experience in interacting with smart home technologies". We distributed the surveys in batches of ten across multiple days to solicit diverse participants. For the first survey, we stopped data collection when we did not find any new SH-PPBs in the last three separate batches, as that suggested saturation in results. For the second survey, we stopped data collection once each privacy feature had been compared and critiqued at least 60 times.

159 participants completed the first survey. Among them, 67 participants contributed 86 SH-PPB practices, and 10 contributed more than one practice. The median task completion time was 5.4 minutes (mean = 6.7, std = 5.25) for crowd workers that did not report any SH-PPBs, and 9.5 minutes (mean = 10.8, std = 5.7) for workers that contributed at least one SH-PPB. The average hourly pay for participants was $12.50. 251 participants completed the second survey. We removed 24 who failed the attention check question in the later data analysis. To ensure our payments were fair to crowd

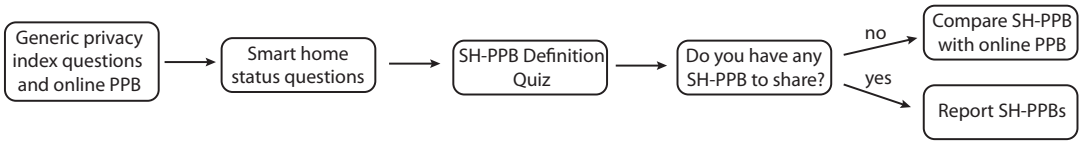


Figure 3: The first survey aims to collect qualitative descriptions about users' smart home privacy-protective behaviors. The base payment for the survey was $0.50, and we offered a $1 bonus for each reported SH-PPB. For those who had no SH-PPBs to share, we asked them to elaborate on any differences between SH-PPBs and online PPB experiences.

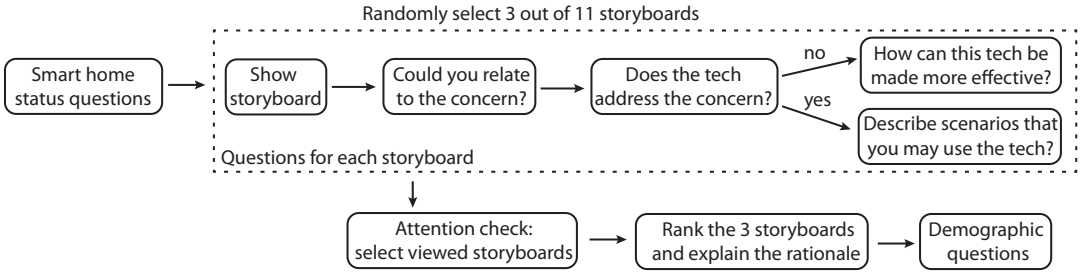


Figure 4: The second survey asks participants to critique three randomly selected storyboards using open-ended questions and rank their preferences. Each storyboard depicts an imagined situation with context, problem, proposed privacy protection concept, and users' reaction. To ensure data quality, we introduced an attention check question, where participants need to select the three storyboards they have viewed among 11 storyboards correctly. Participants were compensated with $4 for filling the survey, and the average time completion was 14 minutes.

workers, we only rejected assignments if a participant misidentified each of the three storyboards they were shown (N=11). The payment for the survey was $4, and the average time completion was 14 minutes.

Participants across two surveys reported various levels of experience with smart home technologies. Most participants reported deploying 5-10 devices (187) and 0-5 devices[1] (161), followed by 10-20 devices (31), 20-40 devices (5), 40-80 devices (2), The types of devices reported by the participants covered all 15 categories we had. Smart speakers (e.g., Amazon Echo, Google Home) were the most common device type (316), followed by Smart Lighting (194), Smart Thermostats (167), Robot Vacuums (164), Smart Cameras (127), and Smart Plugs (116). With respect to demographics, we had 154 females, 230 males, and 2 participants who preferred not to disclose their gender. Participants ranged in age from 18 to 74 (7% from 18-24, 42% from 25-34, 30% from 35-44, 13% from 45-54, 6% from 55-64, 2% from 65-74). Most reported having some college education (87%). The popularity orders of these distributions in the two surveys are identical, so we reported them in aggregate.

3.3 Analysis Methods and Metrics

For the first survey, we used an iterative, open coding process to analyze the open-ended questions. Two researchers first independently open coded all the responses. These openly generated codes were then collaboratively synthesized into a set of high-level codes, and the two researchers used the scheme to code the responses independently again. Upon completion, the coding team discussed potential extensions to the coding scheme. Once changes to the scheme were made, we re-coded all the responses with the new scheme. We conducted two coding iterations to reach a consensus. The overall inter-coder agreement was 0.86.

[1]Note that users may not deploy devices themselves and may sometimes interact with devices deployed by others.

For the second survey, we used the Plackett-Luce method [26] to merge the partial rankings into a global ranking, and used thematic analysis [4] to identify the factors that most strongly influence the preference of a concept. To conduct our thematic analysis, we (1) first coded the ranking rationale to create initial pro and con codes for each concept; (2) collated these codes with the corresponding open-ended critiques; (3) grouped codes into high-level themes and cross-checked with the global ranking.

3.4 Research Ethics

Our project was approved by the IRB at our institute. Participants need to read and sign an informed consent document before beginning the surveys. We reminded participants to focus on their own experiences and opinions and not reveal private or sensitive information throughout the surveys. Collected data is stored in a secure location accessed only by the research team. We only collected participants' contact emails for compensating them for their time. We deleted them afterwards and did not connect these emails to the rest of the study data.

4 Results

This section is structured along our research questions. We first present our findings concerning users' existing SH-PPBs, including how and why participants conducted SH-PPBs. Secondly, we summarized users' needs in improving their existing SH-PPBs and searching for new ones, and derived 11 privacy protection concepts. Finally, we present the speed dating results of comparing and critiquing the 11 concepts.

4.1 RQ1: What kinds of SH-PPBs are people already conducting, how often, and why?

To understand the current state of SH-PPBs, we first coded the reported SH-PPBs and clustered them based on devices, approaches, and privacy concerns. Many reported SH-PPBs were relevant but

only differed in few key aspects, so we coded them to multiple applicable primitives. For example, one participant only powers on the camera when she is out of town, while another participant removes a cloth covering her camera when she leaves home. We coded the first as "on-demand turn-on" and "powering off," and the second as "on-demand turn-on" and "physical blocking."

4.1.1 High-level statistics: Out of all 159 participants, 67 reported at least one SH-PPB. Of these 67 participants, we excluded 4 who, combined, reported 6 SH-PPB practices that are not exclusive to smart homes (e.g., "using VPNs for online browsing," "taping the camera on a laptop"). For the other 92 participants, we found that 20 participants described implicit SH-PPB practices, such as "not placing smart cameras inside the house," or "only purchasing safe sensors like door sensors." Overall, more than half of our participants (83/159=52%) reported valid SH-PPBs. We note that this number is a lower bound, for two reasons. First, participants were asked to do a recall task (i.e. listing what kinds of SH-PPBs they do), which may be incomplete. Second, there may be subtle SH-PPBs that people engage in but did not think of including (e.g. choosing not to place devices in specific places in a house).

4.1.2 Cameras vs. Microphones vs. Other devices: Our coding process identified 14 unique SH-PPB primitives for smart cameras (Table 1), 13 for smart speakers (Table 2), and 9 for the other devices (Table 3). Participants were most likely to develop an SH-PPB towards cameras, followed by smart speakers and other devices. We found that 68% of participants who own smart cameras reported a camera SH-PPB, but the numbers drop to 29% for smart speakers and 7% for other devices. One potential explanation is that most participants understood the risks of audio and video recording and knew how to stop the devices from recording (e.g., physical blocking, powering off), so they can improvise corresponding SH-PPBs accordingly.

In contrast, relatively few participants (6/159) had accurate mental models about potential inference threats regarding devices like lightbulbs and thermostats. For example, P16 understood the privacy threats of a thermostat correctly, "*we have turned off the learning mode for our Nest that tries to predict when you are home.*" P16 was concerned because "*it essentially tracks when we are home during the day and which days the thermostat is in use. Our schedule could be read if the information were ever hacked.*" But P43 misunderstood the privacy threats, leading to ineffective SH-PPBs: "*I changed the names of the settings on the smart thermostat so they aren't labeled 'home,' 'sleep,' etc.*" to prevent someone who can access this information from revealing his family's habits. Indeed, P43 spent significant effort on these less effective SH-PPBs: "*I changed the schedules on the smart lighting every three or four days, so they don't show such a consistent schedule of when there is someone home.*"

4.1.3 Built-in features, ad hoc physical features, and third-party solutions: In the online browsing context, most PPBs are due to either built-in privacy features provided by each website (e.g., opting-out of personalized ads) or third-party privacy features offered by the platform and privacy advocates (e.g., browser private mode, ad blockers). In contrast, there is relatively limited support for built-in privacy or third-party features for smart homes. For example, only 20 out of 80 SH-PPBs are enabled by built-in privacy features, including a built-in shutter (1) and mute buttons (8), time-based scheduling features (3), configuring exclusion areas for cameras (2), history management (3), guest access (2) and remote control (4). Only three SH-PPBs are empowered by third-party privacy features. P12 used an app called "Ropr" to set up a geo-bubble around his home so that when his or his wife's cellphone enters the bubble, the home cameras pause recording. The same user also "routed home internet traffic through a Pi-Hole ad blocking device so that web traffic can be filtered as needed to minimize the amount of data that leaves my home". P13 programmed smart plugs to power off his cameras at certain hours.

A unique aspect of smart home privacy is that users have more physical control over their devices. Indeed, the majority of reported SH-PPBs (57/80) leverage this fact to protect users' privacy. For example, users can position cameras to face and record less privacy-sensitive areas, such as doorways and windows (P8). P34 reported that they "enter through the garage to avoid the doorbell camera showing what time they get home each day." Many participants stated that they often unplug, turn off, block smart home devices when not in use, even though these devices are designed as always-on devices. We observed two interesting patterns in SH-PPBs for always-on devices: on-demand turn-on and on-demand turn-off. The first group keeps the devices off and only turns the devices on when necessary. For example, multiple participants mentioned that they only use Alexa to play music, or use cameras when they are out of town. In contrast, the other group leaves the devices on by default, but only turns them off when there is a guest or a private discussion. Both patterns are common for speakers (5 vs. 4) (Table 1) and cameras (13 vs. 9) (Table 2).

Ad hoc physical blocking is another common approach to stop devices running in the background. For example, P3 reported throwing a towel over her partner's Alexa when she wanted to discuss private things. P55 stated that he manually covered the camera in the hallway whenever he was at home and removed the cloth when he left. An extreme example of physical control leads to hardware modification. P31 complained that "it is becoming virtually impossible to find TVs without an Alexa in it," so he "physically removed the microphone/camera aspect of the device."

4.1.4 Implicit SH-PPBs: Many participants who did not explicitly report SH-PBBs still implicitly referenced them. In elaborating the difference between SH-PPBs and online PPB experiences, participants often described that they do not fully adopt smart home technologies (N=9), where participants limited the number of devices and/or only adopt more privacy-friendly smarts home products. For example, P102 decided "not to use smart technology because he fears that someone else has access to it and can see/hear what he is doing." P80, who only adopts smart TV sticks and binary sensors, explained that he chooses not to utilize smart home devices to "keep his life simple and avoid hidden problems, albeit much more devices are available." Another important category of implicit PPBs is ad hoc physical privacy control (N=11), which has been discussed above. Since the descriptions of these implicit SH-PPBs are casual and often incomplete, we did not include them in Table 1, 2, 3.

4.1.5 Protection from whom and for whom: For each SH-PPB, we asked participants to explain their associated privacy concerns in free text. We then coded the attackers and the protected subjects,

Table 1: Privacy-protective behavior primitives for cameras. The numbers in parentheses are the number of occurrences for individual categories. 68% of participants who own smart cameras reported a camera SH-PPB.

Time-based on/off	Examples
Using built-in features (3)	"I schedule my smart camera security system to automatically arm at our normal bedtime and disarm just before we get up each morning."
Using third-party solutions (1)	"I have my smart cameras set to be powered off at certain hours by programming smart plugs."
Location-based on/off	
Using third-party solutions (1)	"I setup a geo-bubble around my home so that when me or my wife's cellphone enters (about 50 feet around) our home cameras pause recording. I use an app called Ropr to accomplish this."
Manual on/off switch	
On-demand turn-on (5)	"I set up Blink mini cameras when I leave the house, but I unplug them when I am at home."
On-demand turn-off (4)	"Turn off device in some parts of the home when I'm at home."
Avoiding being captured	
Dodging cameras (3)	"I enter through the garage to avoid the doorbell camera showing what time I get home each day."
Positioning cameras (5)	"I have them positioned so that they face and record relevant areas - essentially doorways and windows - but I have my seating positions and 'workspace' areas (depending on the room) out of view from these cameras."
Configuring exclusion areas (2)	"I use exclusion areas on home security cameras to prevent unintentional recording in certain areas of my house."
Deadening sound (1)	"I purposefully keep the sound down on the TV so that the smart camera cannot pick up on it in case my wife is watching and hears what I am doing."
Temporarily turn off cameras	
Ad-hoc physical blocking (5)	"I put tape over the camera or unplug the device if I feel necessary."
Using built-in shutter (1)	"I close the shutter on Amazon Echo Show devices to prevent unintentional viewing."
Powering off (3)	"I unplug them (cameras) when I am at home."
Misc	
Deleting video footage (2)	"I delete footage from Ring doorbell (once a month), in case there is anything I do not want to be out there".
Account management (2)	"I encrypt my smart camera with passwords so no one can get into it."

Table 2: Privacy Protective Behaviors for Smart Speakers. The numbers in parentheses are the number of occurrences for individual categories. 29% of participants who own smart speakers reported a speaker SH-PPB.

Manual on/off switch	Examples
On-demand turn-on (13)	"I always leave my Amazon Echo on mute unless I need to tell it something and then ask it to delete previous requests."
On-demand turn-off (9)	"Unplugging my partner's Alexa when I am casually hanging out."
Temporarily turn off speakers	
Through mute-button (8)	"I hit the mute button on the device so it's no longer listening to me."
Through the app interface (3)	"Disable Google assistant in smart devices using smart phones."
Through speech commands (1)	"Tell alexa not to listen."
Powering off (15)	"Unplug smart speaker to avoid audio recording."
Physical blocking (2)	"Throwing a towel over it when I want to discuss private things."
Avoiding being captured	
Dodging speakers (3)	"When I want to discuss private things, I let my partner go to the bathroom to talk in there."
Positioning speakers (2)	"I moved Alexa to an area of the home, where I am confident my voice cannot be picked up when I am in my home office taking phone calls."
Limiting usage scenarios (2)	"I just unplug it when not in use and plug it in when I want to use it for its timer or to play music."
Data management	
Disabling cross-device syncing (1)	"I turn off the syncing of the Alexa to the smart tv's at night so the Amazon account isn't broadcasting shared results from one device to another on what the family watches in separate rooms."
Deleting previous requests (1)	"... ask it (i.e., Alexa) to delete previous requets."
Network management (2)	"I route home internet traffic through a Pi-Hole ad blocking device so that web traffic and web requests can be filtered as needed to minimize the amount of data that leaves my home."

to surface users' goals in SH-PPBs. We observed five types of imagined attackers: general (50), service providers (11), remote hackers (10), physical intruders (7), and other residents (4). The majority of the mentioned PPBs (50/80) do not articulate who the attacker is. Instead, they often describe that they feel uncomfortable about potential risks due to undesired data collection, usages, and inadequate security protections. While both service providers and remote hackers are commonly reported attackers, none of the participants mention any actual negative experiences. Indeed, a few participants (N=6) ascribe these concerns to the privacy-related news and discussions with tech-savvy friends. In contrast, participants often associated "physical intruders" and "residents" with more concrete threats, such as "a thief can infer whether they are at

Table 3: Unique SH-PPBs for other devices: thermostat, lights, lock, and Robot vacuum. The numbers in parentheses are the number of occurrences for individual categories. Only 7% of participants who own these devices reported a corresponding SH-PPB.

Noisifying personal data	Examples
Changing the schedules (2)	"I change up the schedules on the smart lighting so they don't show such a consistent schedule of when there is someone home."
Changing the configurations (1)	"I change the names of the settings on the smart thermostat so they aren't labeled 'home' and 'sleep' etc."
Misc.	
Disabling intelligent features (2)	"We have turned off the learning mode for our nest that tries to predict when you are home and turning on and using the thermostat."
Disabling cross-device syncing (1)	"I turn off the syncing of the Alexa to the smart tv's at night so the Amazon account isn't broadcasting shared results from one device to another on what the family watches in separate rooms."
Modifying the hardware (1)	"I intentionally avoid purchasing items that include putting a live microphone and/or video camera in my house.... In the few cases where I can't (no available "non-smart" options for example), I physically remove the microphone/camera aspect of the device and/or disconnect it from power when not in use."
Powering off (4)	"In the few cases where I can't (no available 'non-smart' options for example), I disconnect them (smart TV, Fire stick) from power whenever not in use".

home" or "another family member can see his TV viewing history or Alexa requests".

Besides, participants were most interested in protecting themselves (22/80) and their families (34/80). Only one participant mentioned that their guests feel uncomfortable with cameras that are turned on. None of the participants reported any SH-PPBs to protect passersby on the street or their neighbors. What's worse, some SH-PPBs may impose privacy attacks on other people. For example, P40 stated, *"I don't want to be captured on the cameras around my home... I bought them to capture other people/animals."*

4.1.6 SH-PPB frequency: Our results suggest that participants are actively performing SH-PPBs, despite the limited support and tedious effort required. Notably, 17 reported SH-PPBs were performed more than once a day. For example, P48 stated that "it has become a daily habit to unplug any devices with microphones when not in use." Furthermore, 16 reported SH-PPBs that were conducted on a weekly basis, such as moving a camera setup for a guest. Only 2 SH-PPBs were conducted on a monthly basis. For example, P20 stated that she "delete[s] footage from Ring doorbell once a month." Finally, 20 SH-PPBs are performed at installation time, which are mainly one-time setups. For example, P12, who set up a Pi-Hole to route home internet traffic, stated that "I set up the system to work passively, and it has been running for 8 months now continuously."

4.2 RQ2: What types of needs do users wish to support?

We also captured users' needs of SH-PPB supports from the first survey, by understanding (1) the features participants wished to have to address their privacy concerns better and (2) the barriers that prevent participants from conducting SH-PPBs. We then sought privacy protection concepts to address these observed needs and concluded with a list of 11 concepts used in the later speed dating experiment.

4.2.1 Most wanted features: Our analysis identified 18 types of wishlist features, summarized in Table 4. These desired privacy features expose three limitations of the widely adopted ad hoc physical approach. First, changing the configuration through the physical layer is inconvenient. For example, multiple participants expressed the desire to have an option to mute Alexa in a mobile app, so they do not have to move to unplug and plug it back in later. Second, these ad hoc approaches can only enable some basic, and often binary control. In contrast, participants want more intelligent privacy features, such as "a lid to cover the camera that gets automatically activated when I am at home," or "filtering family members in the video streams." To enable these types of features, we need more third-party solutions and built-in features. Finally, the ad hoc physical approach does not scale. For example, while P54 wants to "protect his home using smart cameras fully," he ends with only pointing the cameras to places he does not visit frequently. P54's wished-for feature was "Selectively turn off the cameras when at home. I mean easily." Similarly, P57 wished to "Have a hub application where you can put on privacy mode for all devices with a click of a button."

Beyond control, another important theme behind these desired features is better awareness. For example, three participants wanted to receive a weekly review of the audio logs. In addition, two participants wanted the smart speakers to light up when it is listening for wake words, so they would not forget to turn the microphone off. Finally, participants also wish to have a third-party privacy-rating system that can assess and rate smart devices.

4.2.2 Barriers to SH-PPB adoption: To elicit factors that prevent participants from conducting SH-PPBs, we asked the 87 participants who did not report having any SH-PPBs but did report online PPBs to "Compare and elaborate on any differences between managing online browsing privacy and smart home privacy" (Fig. 3). We excluded 10 participants who only discussed online PPBs and 20 participants who described implicit SH-PPBs, and reported on the themes that emerged from analyzing the remaining 57 responses. We organized these themes using a security sensitivity model [7], which argues that security features remain unused due to three reasons that we summarize in Table 5. These include: (1) **awareness**, i.e., participants who are either unaware or do not ascribe importance to privacy threats (24/57 participants); (2) **ability**, i.e., participants who are unaware of tools and methods (13/57 participants) and (3) **motivation**, participants who do not perform SH-PPB due to lack of trust in the tools, their cost, or effort needed (20/57 participants) .

Table 4: Most wanted features for managing smart home privacy. These features are reasonably easy to implement but do not exist. The numbers in parentheses are the number of occurrences for individual categories.

Better on/off control	Examples
Remote turn off/power off (13)	"Remote control through apps", "Wireless power switches"
Built-in scheduled on/off (9)	"Auto power off so I do not have to program a smart plug."
Context-aware auto-off (5)	"Built-in location-based on/off", "Auto-mute function on incoming calls"
Built-in physical block (3)	"Built-in shutter for cameras"
More control of data collection	
Fine-tune data collection (4)	"Turn the microphone off on the camera", "Fine-tune what exactly is captured", "Disable always-on".
Intelligent filtering (3)	"Maybe not send information when someone of the household is coming into the home, only when strangers are by the doorstep"
Opt out options for tracking (2)	"The ability to stop tracking our (TV) programming. I don't want or need future recommendations."
Better awareness	
Data practice transparency (4)	"More clarity from the service providers (Google in this case) as to what is being sent/received and how my information is being used"
Weekly summary (3)	"A review of the audio logs each week"
Device live-status (2)	"I wish that the Echo Dot would light up and stay lit up whenever the microphone is active. We sometimes forget to turn the microphone off and seeing a visual reminder would be very helpful."
Privacy rating (1)	"Some kind of certification/rating system to assess and rate smart device."
Login alert (1)	"Alerts to notify if someone tries to sign into my camera account".
Other: usability, data management, unauthorized access, scale, etc.	
Easier to delete things (4)	"Automatic deletion", "Weekly reminder to delete", "An easy way to review the data that's gathered and the ability to remove it."
Complex wake word (2)	"Maybe it could have a more complex wake word. Alexa thinks a lot of other words are Alexa. Even then I don't know as I would trust it."
Guest session (2)	"Incognito mode similar to browser history", "Creating a guest session for smart speakers."
Local-only network (1)	"Easier ways to limit device to only connect to other, local devices."
Better tutorials (1)	"I'm not sure what types of functionalities are included in the products."
Centralized management (1)	"Have a hub application where you can put on privacy mode for all devices with a click of a button."

Table 5: Breakdown of main reasons that prevent users from conducting SH-PPBs (N= 57). We organized these reasons using the security sensitivity model [7]. Overall Cohen's kappa scores indicate very high agreement (0.85). The numbers in parentheses are the number of occurrences and Cohen's Kappa scores for individual categories.

Awareness: participants are unaware of relevant privacy threats.	
Unaware of SH Privacy threats (16 | 0.84)	e.g., trusting devices, never considering SH privacy threats
SH privacy not important. (8 | 0.75)	e.g., nothing to hide in SH, limited device intelligence.
Ability: participants do not know when, why and how to implement pro-Security and Privacy behaviors.	
Lacking ability for SH-PPBs (13 | 0.91)	e.g., unaware of potential tools and methods
Motivation: participants either do not trust in the efficacy of pro-Security and Privacy behaviors to defend against Security and Privacy threats or believe the costs of doing so are too high relative to its benefits.	
Doubting the efficacy of SH-PPBs (4 | 1.0)	e.g., desire to protect their privacy but feel unable to do so
"All or nothing" dilemma (6 | 0.76)	e.g., have to sacrifice privacy to use the service
Requiring too much effort (10 | 0.88)	e.g. more devices and data actions than online browsing

4.2.3 Privacy protection concepts to address SH-PPB needs: We searched for privacy protection concepts that can either enable the wishlist features or reduce barriers to adoption of SH-PPBs. Most concepts are from privacy research literature (e.g., privacy mirrors [28], privacy nutrition labels [9]) and online forums (e.g., guaranteed protection [35], privacy presets [31]). We then mapped these concepts to applicable needs and stopped the search process after covering all of the observed needs. For example, *Anthropomorphism Icons* is motivated by one response where a non-tech-savvy participant was interested in knowing the data collection capabilities, but in her case all of the devices were purchased and installed by her husband. This process outputs an initial list of 27 concepts. After merging the concepts that overlapped, we concluded with 11 promising smart home privacy protection technologies (Table 7).

4.3 RQ3: What are potential opportunities for building tools to support future SH-PPBs?

This section presents the results of our online speed dating experiment, in which we rapidly explored these 11 application concepts and their potential interaction with users.

4.3.1 Quantitative analysis: **Ranking and comparison**. In the speed dating survey, each participant ranked three randomly selected storyboards based on their general preferences. We then used the Plackett-Luce method [26] collated together these partial rankings to create a global preferred order of all 11 concepts (Fig. 5).

Table 6: The 11 privacy protection concepts we storyboarded and evaluated using speed dating. We analyzed users' SH-PPB needs from the first survey and then sought privacy protection concepts in the literature until we had covered all the identified needs. We present most storyboards in the Appendix due to space reasons.

#	Storyboard	Description
1	Anthropomorphism Icons	A third-party hub that displays devices' data collection capabilities in the look of a robot avatar (Fig. 9).
2	Privacy Presets	A third-party central hub that allows users to switch between pre-configured global privacy modes (e.g., party, business, out-of-the-town) and accordingly updates the settings across individual devices (Fig. 10).
3	Privacy Chatbot	A third-party chatbot that monitors outgoing network traffic requests and allows users to ask privacy-relevant questions through a chatbot (Fig. 2).
4	Guaranteed Protection	A smart plug that controls a device's power supply based on users' specified schedule of active hours for the device (Fig. 11).
5	Data Collection Live Monitor	A third-party application that monitors registered devices and enables users to view the live data collection status, including when, how, and where the data is going (Fig. 12).
6	Identity-based Data Management	A data management feature that associates captured audios and videos with residents' identities. A resident can not view the data associated with other residents (Fig. 13).
7	Privacy Mirrors	A data management feature that offers users a report about the company's knowledge of users and allows users to wipe some knowledge so that the company will forget them [28] (Fig. 14).
8	Privacy Diagnostics	A third-party mobile application that rates privacy settings of existing devices, provides explanations on deducted points, and gives step-by-step instructions on how to improve (Fig. 1).
9	Contextual Privacy Reminders	A built-in feature that reminds users to turn the devices off if the device guesses that the users might want to (Fig. 15).
10	Privacy Simulator	A third-party application that enables users to experiment with a smart home device's reactions and data collection practices to simulated actions in a virtual environment (Fig. 16).
11	Privacy Nutrition Labels	A table labeled on the packaging of a smart home device which contains concise data practice facts and a QR code linked to a website with detailed device information [9] (Fig. 17).

The Plackett-Luce method is based on a classic probability model that can predict the outcome of a paired comparison, similar to how the Elo rating system ranks chess players. Fig. 6 illustrates the probability distribution that a storyboard wins over another. *Privacy Diagnostics* was the most favored storyboard, where 63% of participants ranked it as the most preferred and 10% ranked it as the least preferred. In contrast, *Anthropomorphism Icons* was least favored, where only 25% of participants ranked it in the top, but 52% ranked it in the bottom.

Concept validation & need validation. In the storyboard critique stage (see Fig. 4), we validated the concept (i.e., whether the observed need is aligned with users' actual need) and the need (i.e., whether the proposed solution can address the described need) for each storyboard. Overall, participants acknowledged most observed needs (Fig. 7) but expressed more diverse perceptions regarding the effectiveness of different solutions (Fig. 8). One example is *Privacy nutrition labels* (see Appendix Fig. 17), which was ranked at 9th in the global ranking. While participants related the most to the described need, namely, users wanting to know more about smart home devices' data practices before making a purchase decision, they expressed multiple concerns (see §4.3.2) regarding the solution's effectiveness.

4.3.2 Qualitative results: Our thematic analysis suggested that participants had different privacy concerns, varied levels of trust towards developers, and the time/money they were willing to spend to protect their privacy. This may explain why we did not find any storyboard that was consistently the most preferred across the 228 comparisons. For example, participants expressed three different types of trust regarding *Guaranteed Protection*. The majority of the participants recognized the value of *Guaranteed Protection* since they did not trust smart home device developers and wanted to have an extra layer of protection. In contrast, a significant portion of participants felt it was unnecessary since they trusted the developers, and a few participants preferred to manually shut off the devices since they did not trust the smart plug either. As a result, the concept validation ranking of *Guaranteed Protection* was relatively low. Another example is *Privacy Nutrition Labels*, where participants expressed that they want different levels of details. A few participants complained that the label contained too much information and wished for an energy-efficiency-like rating instead. In contrast, other participants felt the most helpful part was the QR code to the product website and preferred to look for more details online. These distinct personal preferences towards solutions also make need validation ratings (Fig. 8) generally lower than need validation ratings (Fig. 7).

Despite the fact that many factors were subject to personal preferences, we witnessed rich evidence of four unanimously important factors in designing SH-PPB tools, as users prefer (1) simple, (2) preventative, (3) proactive solutions that (4) offer more control.

Simple. Participants frequently mentioned that the top 4 storyboards, namely, *Privacy Diagnostics*, *Data Collection Live Monitor*, *Guaranteed Protection*, *Privacy Presets*, were simple. For example, P302 stated *"I LOVE the idea for privacy presets. For a tech savvy person, it presents a perfect way to manage the settings of everything, to integrate them in an easy to understand way."* Indeed, these concepts have relatively simple mental models comparing to many lower-ranked ones, making it easy for participants to understand

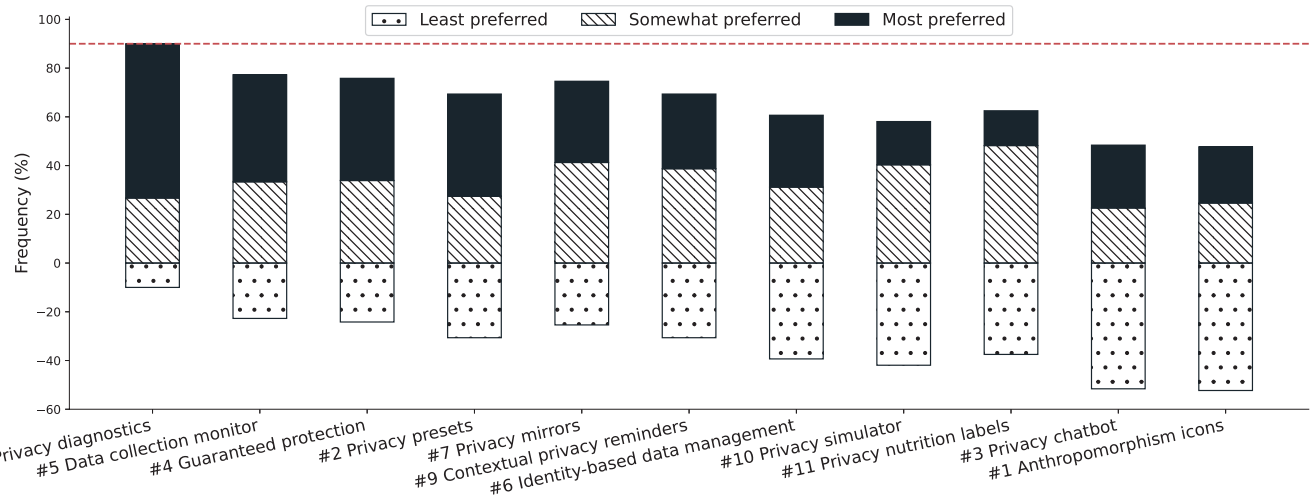


Figure 5: We used the Plackett-Luce method [26] to merge partial rankings into a global preferred order of 11 privacy protection concepts, similar to how the Elo rating system ranks chess players. From left to right, concepts are ranked in decreasing order of preference. A higher bar indicates more preferred responses. The dashed line facilitates the comparisons between other concepts and *Privacy Diagnostics*.

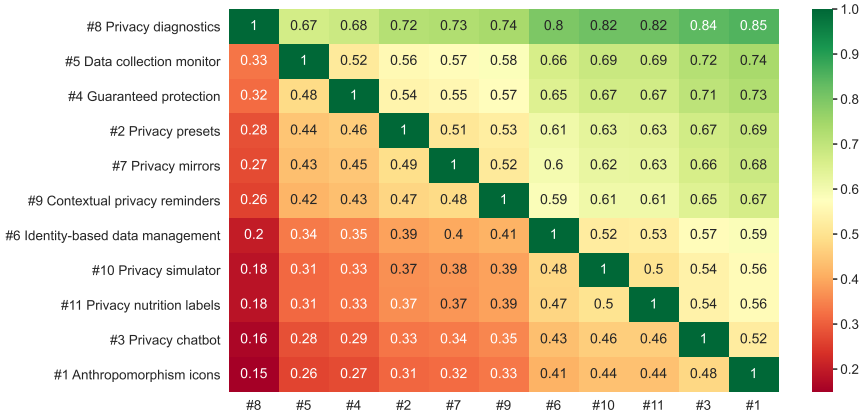


Figure 6: The probability distribution that a storyboard (row) wins over another storyboard (column). For example, a participant has a 85% chance to prefer *#8 Privacy Diagnostics* to *#1 Anthropomorphism Icons*.

the technologies and expect the output of using them. *Privacy Diagnostics* and *Data Collection Monitor* are similar to the widely adopted features in anti-virus software and firewall. *Guaranteed Protection* and *Privacy Presets* are based on the binary on-off mechanism, extending from the ad-hoc physical layer control. In contrast, participants were uncertain about the other concepts, such as how *Identity-based Data Management* handles images with multiple persons, who will enforce *Privacy Nutrition Labels*, what if developers lie to the *Privacy Simulator* platform.

More control. Another unanimous theme was that participants wished to have more control. Among the 11 technologies, six of them (#2, #4, #6, #7, #8, #9) offer some forms of control while the other five do not. Due to the isolation effect [43], whether the technology provides control options was rather salient when participants compared these two groups. Our coding process found that many participants explicitly mentioned the availability of control options in explaining their ranking rationale, and all of them viewed the option positively. For example, P255 stated that "*The (identity-based) data management actually allows you to do something about your privacy; you can exclude certain people from accessing your info. The (data collection) monitor is nice in that you can see where your data is going, but it doesn't let you do anything about it. The (anthropomorphism) icons are just for people who aren't very tech savvy and don't really do anything.*" Another strong evidence is that none of the bottom four technologies (#10, #11, #3, #1) in the global ranking offers control options.

Proactive. Participants also expressed the desire for proactive technologies that do not need active user interaction. Past research shows that system proactivity, which refers to the degree of initiative a system might take based on its understanding of the context, is a vital dimension to explore for ubiquitous computing technologies [8]. Therefore, in designing the concepts, we intentionally covered a large variety of proactiveness: (1) *Identity-based Data Management* and *Contextual Privacy Reminder* (high proactive), (2) *Privacy Diagnostics* and *Privacy Presets* (medium proactive), and (3)

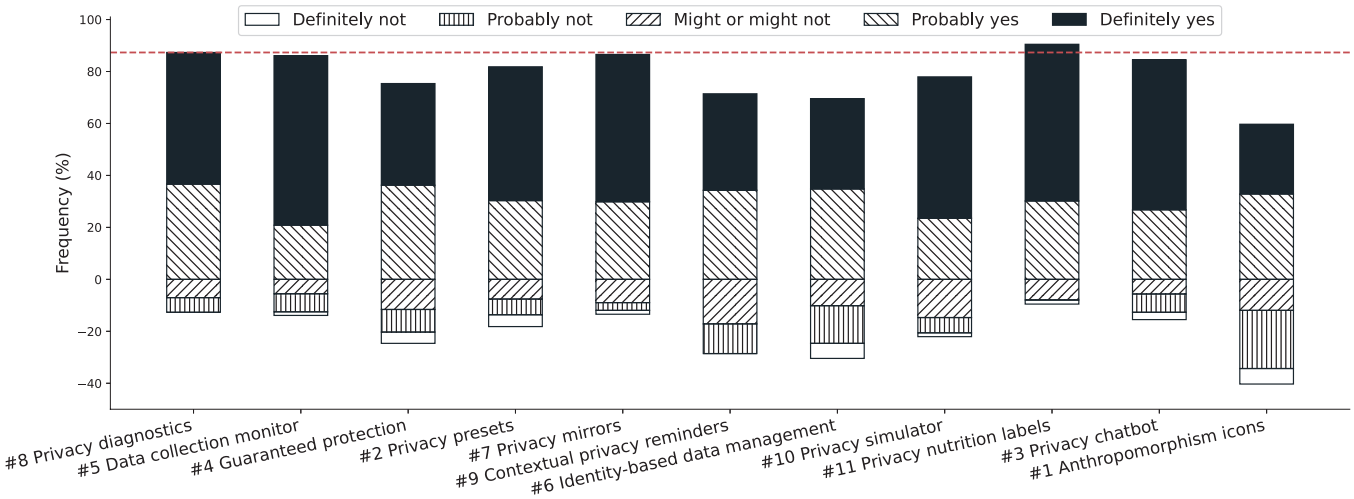


Figure 7: The distribution of answers to "Could you relate to the concern?" Participants reported that they could relate to the concerns described in *Privacy nutrition labels* the most, followed by *Privacy Mirrors* and *Privacy Diagnostics*. A higher bar indicates more preferred responses. The order from left to right is consistent with Fig. 5. The dashed line facilitates the comparisons between other concepts and *Privacy Diagnostics*.

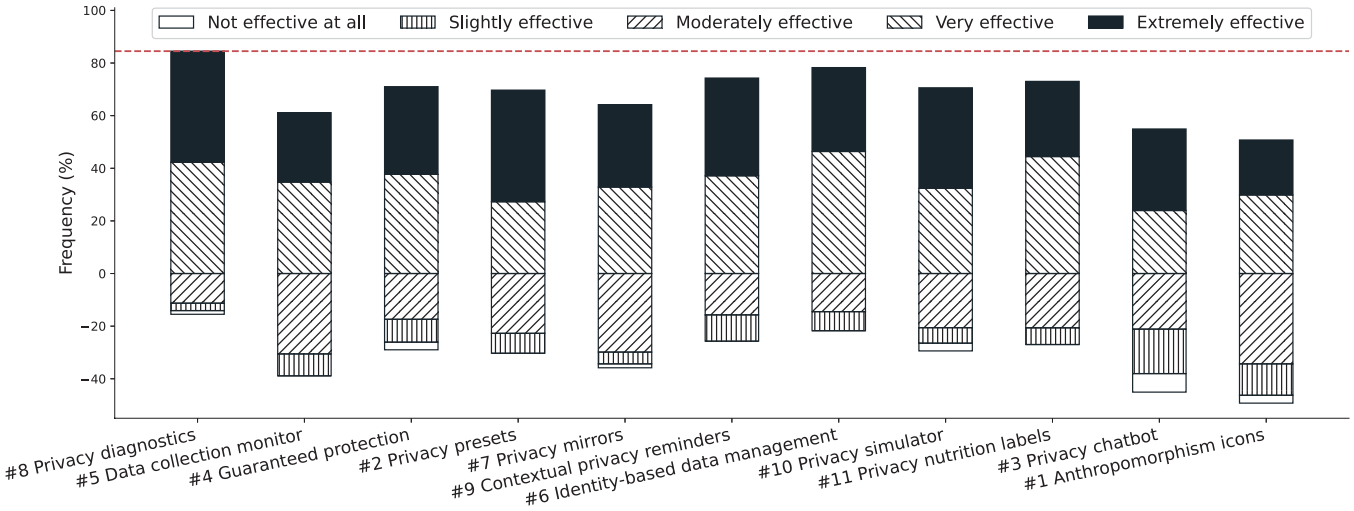


Figure 8: The distribution of answers to "How effective does this tech address the concern?" Participants reported that *Privacy Diagnostics* could most effectively address the corresponding needs, which may explain why it was ranked as the most preferred technology. A higher bar indicates more preferred responses. The order from left to right is consistent with Fig. 5. The dashed line facilitates the comparisons between other concepts and *Privacy Diagnostics*.

Data Collection Live Monitor, *Guaranteed Protection*, *Privacy Chatbot* (low proactive). We found that all the participants appreciated the automation enabled by these proactive scenarios. More specifically, a few participants ranked the high proactive storyboards higher than the rest because they do not need active interactions. On the other hand, the few participants, who did not rank *Privacy Diagnostics* as the most preferred, complained that it requires some manual interactions. Finally, many participants criticized these low proactive solutions since they might forget to use them over time. For example, P280 criticized "*This (Privacy Chatbot) is only effective because Annie asked for the information. sometimes I might forget or not notice to do that until after the data had been sent.*"

Preventative. Participants preferred early prevention technologies to after-the-fact solutions because fixing devices that do not respect privacy is hard. We designed the storyboards to cover multiple stages in users' privacy protection. *Privacy Nutrition Labels* and *Privacy Simulator* protect users' privacy by improving their purchase decision-making. *Privacy Diagnostics*, *Data Collection Live Monitor*, *guaranteed protection*, and *anthropomorphism icons* aim to help users establish successful routines in managing their privacy. Finally, *privacy chatbot* and *privacy mirrors* are after-the-fact solutions, assisting participants in tracing the data leaks and fixing the issues.

We found that participants often mentioned the preventative property in comparing solutions across these categories, and they all viewed it positively. For example, P236 stated, "The last option (Privacy chatbot) is least effective in that it does not actively prevent the problem from happening; it only makes you aware of what has

Table 7: Summarized pros and cons of 11 privacy protection concepts through our thematic analysis. We ordered the concepts based on the global preferred order in Fig. 5.

#	Storyboard	Top pros	Top cons
8	Privacy diagnostics	Easy to use, can use it at will, can prevent data leaks by avoiding wrong configurations, can motivate users.	Need manual interaction, too late for already purchased devices
5	Data collection live monitor	Centralized interfaces & awareness, developers cannot fake network traffic	Offering no control, may forget to use it
4	Guaranteed protection	Can protect privacy even if developers are not trusted, helpful in a few sensitive conditions (e.g., bedroom sensors)	Too much efforts, prefer ad-hoc approaches if the plug is not trusted, limited binary control, not useful if developers are trusted
2	Privacy presets	Easy to use, simple and effective	Concerned about wrong configurations, need to trust the device developers
7	Privacy mirrors	Offering control to data on developers' cloud	Need to trust developers, may forget to use it
9	Contextual privacy reminders	No need for active interactions, offering control	Hard to generalize to other contexts
6	Identity-based data management	No need for active interactions, offering control, useful for people with roommates	Complex mental model regarding corner cases
10	Privacy simulator	Easy to understand the output, preventing from purchasing invasive products	Offering no control, need to trust developers, complex interfaces
11	Privacy nutrition labels	Preventing from purchasing invasive products	Hard to enforce and verify, too much information, too less information, offering no control
3	Privacy chatbot	Centralized and natural interfaces	Cannot prevent data leaks, may forget to use it, only useful for detailed questions
1	Anthropomorphism icons	Easy to understand	Offering no control, not enough information, better to use common icons

already happened." In analyzing these qualitative responses, we found it is because of the lack of solutions to fix devices with bad privacy practices. As a result, users either have to abandon the device or let the data leaks perpetuate. This negative opinion even applied to the most favored storyboard, *Privacy Diagnostics*. For example, P202 stated, "The Privacy Diagnostics seems somewhat unnecessary because most people will not buy a new replacement smart device just because it has a poor rating since most smart devices are quite expensive."

5 Limitations

Several limitations are important to mention. First, our samples were not representative of the general population. The population of Mechanical Turk workers is significantly less politically diverse, more educated, and younger compared to the US population [6]. Despite these limitations, past research suggests that online studies about privacy and security behavior can approximate behaviors of the wider population [36].

Second, participants may undervalue a few concepts that aim to manage smart home devices at scale. Most participants were using relatively few devices and had not hit many scale issues. Only 7 out of 386 participants have more than 20 devices, and relatively few participants expressed a need for scalability support (e.g., centralized user interfaces). While we included multiple concepts to cover the dimension of scalability (e.g., #1, #3, #5, #7), we found that few participants explicitly acknowledged the value of management scalability.

Third, social desirability may lead participants to over describe their SH-PPB experiences, especially the frequency of SH-PPBs. Therefore, we carefully avoided generalizing the results on frequency but only concluded that participants actively performed SH-PPBs. Asking participants to compare across a few reasonable promising privacy protection concepts also helped to alleviate this effect.

Fourth, the rankings of the 11 design concepts should not be used to discourage research in exploring these ideas. We used these concepts to elicit users' reactions, giving us more insights into the underlying problems, needs, and desires. But, these storyboards only cover limited usage contexts and design details, a minor change of these concepts may significantly improve users' preferences. For example, an important reason that users do not like *Privacy Nutrition Labels* is that they feel it would be hard to enforce and verify. A storyboard that states the law will enforce the labels may change users' preferences.

Finally, there may exist biases due to the genders of storyboards' protagonists [15]. We randomly assigned genders to the protagonists across storyboards, aiming to achieve a diverse set: five Male (#2, #5, #8, #10, #11), four Female (#1, #3, #7, #9) and two groups (#4, #6). The average rankings for female protagonists (average ranking μ: 2.11, standard deviation σ: 0.82) is slightly lower than male (μ: 1.92, σ: 0.80) and group (μ: 1.96, σ: 0.82). Future research may study the potential gender bias for using storyboards in UX experiments.

6 Discussion & Future work

6.1 The future of ad hoc privacy protection

We discuss three main limitations of ad hoc privacy protections in §4.2.1: they are inconvenient to change configurations, offer limited control granularity, and are hard to scale. However, there are also

Table 8: The coverage of 11 storyboards across two principal dimensions: lifecycle and system proactivity.

Lifecycle	Proactivity (High)	Proactivity (Medium)	Proactivity (Low)
Install/purchase	#6 Identity-based Data Management	#10 Privacy Simulator	#11 Privacy Nutrition Labels
Routine	#7 Privacy Mirrors #9 Contextual Privacy Reminders	#5 Data Collection Live Monitor	#1 Anthropomorphism Icons #2 Privacy Presets
Deviate	#8 Privacy Diagnostics	#3 Privacy Chatbot	#4 Guaranteed Protection

three important advantages of this ad hoc physical approach. First, it is cheap since participants do not need to purchase extra hardware or software. Second, it simplifies the trust model. For example, two participants expressed that they prefer manually unplugging devices to *Guaranteed Privacy*, since they do not need to purchase anything or trust the smart plugs. Finally, it has the simplest mental model. Although it can only offer limited functionality (e.g., binary on and off), our results suggested that users are very creative in appropriating simple technologies for various contexts. Therefore, we expect these physical ad hoc physical protections will coexist with specialized, built-in features and third-party features for a long time.

6.2 Building built-in and third party features

Our results call for more built-in and third-party privacy features for smart homes. However, implementing these features is challenging in today's ecosystem [22]. In contrast to online privacy protection, which has a few major points of leverage (e.g. web browsers, cookie management, etc), smart home users need features for the vast types of privacy-sensitive data that developers are collecting. Although each feature might be trivial to implement (e.g., turning off the microphone of a camera), developers require significant resources to implement the interfaces and control options for the heterogeneity of IoT devices. Further, smart homes lack a clear point of leverage to make third-party features work across multiple devices, similar to how Ad-blocker extensions help users manage privacy through the web browser. Future research should explore potential solutions to build these points of leverage, such as customizable DNS servers (e.g., Pi-Hole), smart home hubs (e.g., Peekaboo [18]), WiFi routers, and SNMP-like [44] protocols [18] for smart home devices.

6.3 The coverage of 11 storyboards

We used the IDEO brainstorming rules [16] to guide the storyboard generation & selection process. Three experienced privacy researchers first nominated individual ideas and then derived variations across two principal dimensions (similar to [8]): activity lifecycle (i.e., install/purchase, routine, and deviate) and system proactivity (i.e., high, medium, low). For example, an "install-time" *Privacy Chatbot* answers users' questions about the devices' potential behaviors before they make a purchase. By proactivity, we mean the degree of initiative that an intelligent system might take based on its contextual understanding. A "highly proactive" *Privacy Chatbot* monitors the network continuously and proactively asks users to verify these behaviors. After the process, we obtained over 50 candidates and merged them into 11 representative storyboards, ensuring a wide coverage for different ideas and dimensions (Table. 8). For example, we blended the "install-time" *Privacy Chatbot* into the *Privacy Nutrition Labels* (Fig. 17), and the "highly proactive" *Privacy Chatbot* into *Contextual Privacy Reminders* (Fig. 15). Besides, different concepts often introduce other dimensions, such as whether the feature offers control, serves multiple users.

6.4 Permuted combinations versus Factorial experiments

One alternative experiment design for the second survey is to run factorial experiments. For example, we may ask participants to rank *Privacy Chatbot* at different stages, such as purchase, install, routine, and when something goes wrong (deviate). But it has two limitations for our goal. First, the combinatorial explosion limits the number of test factors. Second, many enumerations may not necessarily be attractive.

In contrast, our ranking experiment differs in two key ways. First, we do not control the variables in each comparison task, but focus on the most promising concepts. Second, more than quantitative ranking, we also asked participants to explain their rationale in free text. In retrospect, at the core of our approach is the isolation effect [43]: when multiple homogeneous stimuli are presented, the stimulus that differs from the rest is more likely to be remembered. For example, when a participant ranks *Privacy Diagnostics*, *Data Collection Live Monitor*, and *Privacy Chatbot*, she may find that only *Privacy Diagnostics* can offer control and start to evaluate whether this is a positive factor. As we permuted the combination of storyboards in each comparison task, we implicitly guided participants to traverse the possible dimensions. This unique design allows us to compare more concepts than alternative approaches.

7 Conclusion

In this paper, we conducted two online surveys to understand existing SH-PPBs and explore potential opportunities to better support users' needs of performing SH-PPBs. Our first study identifies 33 unique types of smart home privacy-protective behaviors, and finds that users heavily rely on protections at the physical layer and on ad hoc approaches. Based on needs observed from our first study, we then speed dated 11 different privacy protection concepts and found that a relatively simple technology, *Privacy Diagnostics*, was preferred far above of the rest in our study. We also identify four important factors in designing SH-PPB tools: simple, preventative, proactive solutions, and more control.

References

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. *arXiv:1705.06805* (2017).

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 59 (jul 2018), 23 pages. https://doi.org/10.1145/3214262

[3] Sophie C Boerman, Sanne Kruikemeier, and Frederik J Zuiderveen Borgesius. 2018. Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research* (2018), 0093650218800915.

[4] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[5] Jeffrey T Child, Sandra Petronio, Esther A Agyeman-Budu, and David A Westermann. 2011. Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior* 27, 5 (2011), 2017–2027.

[6] Cloud Research. 2021. Strengths and Limitations of Mechanical Turk. https://www.cloudresearch.com/resources/blog/strengths-and-limitations-of-mechanical-turk/. (Accessed on 09/08/2021).

[7] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 143–157.

[8] Scott Davidoff, Min Kyung Lee, Anind K Dey, and John Zimmerman. 2007. Rapidly exploring application design through speed dating. In *International Conference on Ubiquitous Computing*. Springer, 429–446.

[9] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.

[10] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*. 483–500.

[11] Eszter Hargittai. 2010. Facebook privacy settings: Who cares? *First Monday* (2010).

[12] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home internet of things (IoT). In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 255–272.

[13] Pi hole. 2021. Pi-hole – Network-wide protection. https://pi-hole.net/. (Accessed on 09/04/2021).

[14] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proc. ACM IMWUT* 4, 2 (2020), 1–21.

[15] Janet Shibley Hyde. 2014. Gender similarities and differences. *Annual review of psychology* 65 (2014), 373–398.

[16] IDEO. 2022. 7 Simple Rules of Brainstorming – IDEO U. https://www.ideou.com/blogs/inspiration/7-simple-rules-of-brainstorming. (Accessed on 01/06/2022).

[17] IT Pro Team. 2018. How to stay anonymous online | IT PRO. https://www.itpro.com/privacy/30584/how-to-stay-anonymous-online. (Accessed on 08/13/2021).

[18] Haojian Jin, Gram Liu, David Hwang, Swarun Kumar, Yuvraj Agarwal, and Jason I Hong. 2022. Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[19] Haojian 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. *Proc. ACM IMWUT* 2, 4 (2018), 1–27.

[20] Haojian Jin, Hong Shen, Mayank Jain, Swarun Kumar, and Jason I. Hong. 2021. Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost. *ACM Trans. Comput.-Hum. Interact.* 28, 5, Article 34 (aug 2021), 55 pages. https://doi.org/10.1145/3463910

[21] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In *Pro. ACM Human-Computer Interaction CSCW*. ACM.

[22] Tianshi Li, Elijah B Neundorfer, Yuvraj Agarwal, and Jason I Hong. 2021. Honeysuckle: Annotation-guided code generation of in-app privacy notices. *Proc. ACM IMWUT* 5, 3 (2021), 1–27.

[23] Toby Jia-Jun Li, Jingya Chen, Brandon Canfield, and Brad A Myers. 2020. Privacy-preserving script sharing in gui-based programming-by-demonstration systems. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–23.

[24] Leib Litman, Jonathan Robinson, and Tzvi Abberbock. 2017. TurkPrime. com: A versatile crowdsourcing data acquisition platform for the behavioral sciences. *Behavior research methods* 49, 2 (2017), 433–442.

[25] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. *European Workshop on Usable Security (EuroUSEC)* (2018).

[26] Lucas Maystre and Matthias Grossglauser. 2015. Fast and accurate inference of Plackett–Luce models. In *Advances in neural information processing systems*. 172–180.

[27] 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*. ACM, 5197–5207.

[28] David H Nguyen and Elizabeth D Mynatt. 2002. *Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems*. Technical Report. Georgia Institute of Technology.

[29] 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*. 1–13.

[30] Reddit. 2021. Anyway to limit guests access to a shared device ie they can't hear sound, cams only available on a schedule I set etc? : wyzecam. https://www.reddit.com/r/wyzecam/comments/eqqqtq/anyway_to_limit_guests_access_to_a_shared_device/. (Accessed on 09/09/2021).

[31] Reddit. 2021. Guest Mode: An easy privacy control for your home devices. https://www.reddit.com/r/googlehome/comments/kwm1k2/guest_mode_an_easy_privacy_control_for_your_home/. (Accessed on 09/04/2021).

[32] Reddit. 2021. Is there a Robot vacuum cleaner that does not violate privacy? : privacy. https://www.reddit.com/r/privacy/comments/eruwpe/is_there_a_robot_vacuum_cleaner_that_does_not/. (Accessed on 09/09/2021).

[33] Reddit. 2021. Recommendations for a home camera respecting my privacy. https://www.reddit.com/r/homesecurity/comments/ctuvnx/recommendations_for_a_home_camera_respecting_my/. (Accessed on 09/07/2021).

[34] Reddit. 2021. use of wyze cams inside your home. https://www.reddit.com/r/wyzecam/comments/kochtt/use_of_wyze_cams_inside_your_home/. (Accessed on 09/07/2021).

[35] Reddit. 2021. Wyze Cam into a smart plug? https://www.reddit.com/r/wyzecam/comments/7u9jy6/wyze_cam_into_a_smart_plug/. (Accessed on 08/10/2021).

[36] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.

[37] Richard L Rutledge, Aaron K Massey, and Annie I Antón. 2016. Privacy impacts of IoT devices: A SmartTV case study. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*. IEEE, 261–270.

[38] Shruti Sannon, Natalya N Bazarova, and Dan Cosley. 2018. Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. In *Proc. CHI*. 1–13.

[39] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *UMBC Faculty Collection* (2021).

[40] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2019. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proc. ACM IMWUT* 3, 4 (2019), 1–23.

[41] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart home beyond the home: A case for community-based access control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[42] Monica T Whitty and Siobhan E Carville. 2008. Would I lie to you? Self-serving lies and other-oriented lies told across different media. *Computers in Human Behavior* 24, 3 (2008), 1021–1031.

[43] Wikipedia. 2021. Von Restorff effect - Wikipedia. https://en.wikipedia.org/wiki/Von_Restorff_effect. (Accessed on 09/08/2021).

[44] Wikipedia. 2022. Simple Network Management Protocol - Wikipedia. https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol. (Accessed on 01/06/2022).

[45] 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*. ACM, 427–434.

[46] 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 *Proc. CHI*. 1–12.

[47] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk models of online behavioral advertising. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 1957–1969.

[48] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*.

[49] 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.

[50] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[51] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, Smart Home'–Exploring End Users' Mental Models of Smart Homes. *Mensch und Computer 2018-Workshopband* (2018).

[52] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

A Appendix: Storyboards

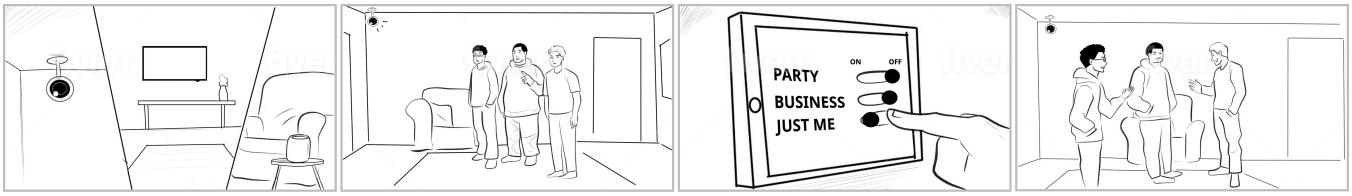
[Character, Context]
Mary has several smart home devices at her house. Some of them are bought by her husband, who seems tech-savvier; others are gifts from her friends and relatives.

[Problem]
Though she always wonders how and why these devices work so smartly, she doesn't want to read through those lengthy product descriptions.

[User Action, Technology]
Mary installs a central hub display that shows all her installed devices in a spreadsheet. Next to each device name, a robot avatar indicates the types of data each device can collect. For example, if the device has a microphone, the avatar would have two ears.

[Resolution]
Mary now has a better understanding of her devices. Whenever she wants to know how the devices work, she can refer to the central hub.

Figure 9: Storyboard #1 Anthropomorphism Icons



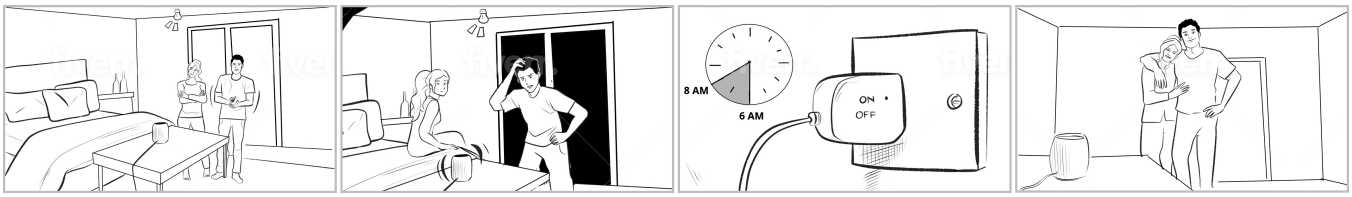
[Character, Context]
Carl lives in a house with many smart home devices. These devices keep running continuously throughout the day.

[Problem]
Carl works at home a lot, and he does not want these devices to monitor his business phone calls. Occasionally, Carl invites guests to parties at his place. His party mates also feel uncomfortable about being recorded.

[User Action, Technology]
He installs a mode switch sets up a few privacy modes to manage all the devices. For example, when hosting a party, he can switch to the "Party" Mode that stops recording the data of his guests. When working at home, he can switch to the "Business" mode that turns off all devices' microphones.

[Resolution]
Carl can now easily accommodate his and his guests' privacy with one mode switch and be assured that everyone's privacy need is met.

Figure 10: Storyboard #2 Privacy Presets



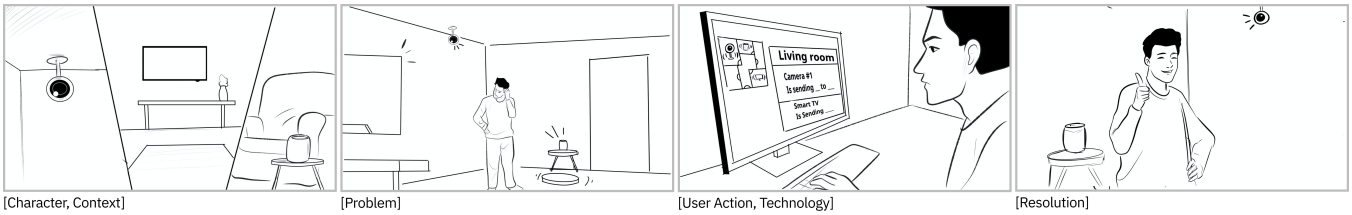
[Character, Context]
Charley and Lu have a smart speaker in their bedroom. They also have a set of motion detectors and smart switches to control their bedroom lighting.

[Problem]
The couple is concerned that the smart speaker, smart switch, and motion detectors might be actively working at night while making love.

[User Action, Technology]
The couple installs smart power plugs to control the devices' power supply. For example, they only use the smart speaker in the morning to wake them up, so they specify that the plug only powers the smart speaker between 6 AM and 8 AM.

[Resolution]
In doing so, the couple feels more comfortable placing these smart home devices in their bedroom.

Figure 11: Storyboard #4 Guaranteed Protection



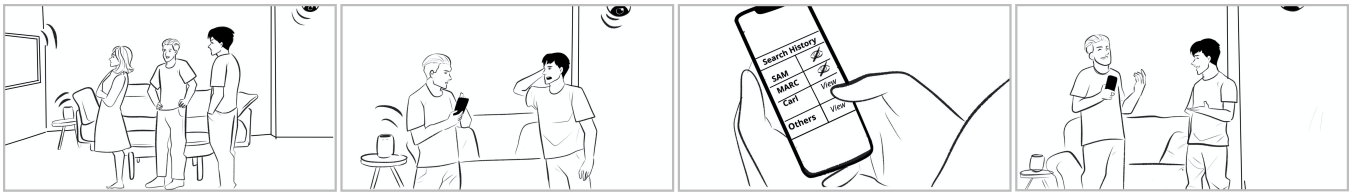
[Character, Context]
Charley installed numerous smart home devices at different places in his house.

[Problem]
He feels overwhelmed because these devices can collect personal data and send it to external servers without his awareness.

[User Action, Technology]
Charley installs a tool that enables him to view devices' data collection attributes including when, how, and where his data is going.

[Resolution]
Charley now feels much safer because he is no longer blinded from the data collection behaviors of his smart home devices.

Figure 12: Storyboard #5 Data Collection Live Monitor



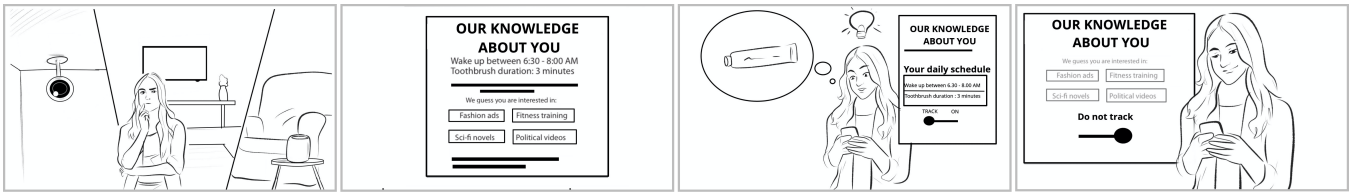
[Character, Context]
Sam rents a house with housemates, and they share smart home devices for security, temperature control, light control, etc. These devices record their voices, photos, setting preferences, etc. The residents use a mobile app to manage these devices using their accounts, respectively.

[Problem]
Sam is concerned that his collected by these shared devices will be accessible to other residents. For instance, his search history recorded by the voice assistant and images recorded by the smart camera in the front door is available to his housemates.

[User Action, Technology]
The mobile app now offers a new feature: the app will associate these personal data with residents' identities. By default, a user can only view one's personal search history and video recordings.

[Resolution]
Sam now feels relieved and secured about his privacy and is not worried about his friends viewing his data anymore.

Figure 13: Storyboard #6 Identity-based Data Management



[Character, Context, Problem]
Amy doesn't go through a single day without using smart home products from a single company. Though these devices improve her life quality, Amy begins to wonder what information the company knows about her.

[Technology]
Due to legal regulation, companies offer users a report about their knowledge of users and allows users to wipe some information so the company will forget them. For example, the report might tell Amy that her smart home vendor knows when she wakes up, brushes her teeth, and goes to sleep.

[User Action]
After reviewing the report, Amy understands why she gets the toothpaste advertisement when it runs out. However, since she is not interested in political videos, she requests the company to forget that information.

[Resolution]
Later, she finds fewer political video recommendations in her video feeds. She enjoys the transparency and control in the process and starts to read such a report every few weeks.

Figure 14: Storyboard #7 Privacy Mirrors

[Character, Context]
Lisa is cautious with her smart home device usage. She usually turns her smart speaker off during work hours, dinner time, and sleeping periods. She would turn the device back onto listening mode after work.

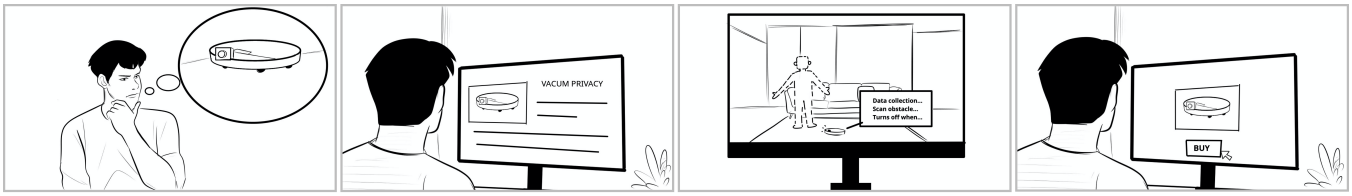
[Problem]
However, it's hard to remember to change the settings. Lisa feels frustrated when there is no response from her voice assistant or when her phone call is interrupted by the voice assistant because she forgot to turn on/off the device.

[Technology]
The smart home system recently offers a new feature, enabling users to set contextual reminders (e.g., remind one to turn off the speaker when having a family dinner, alert one to turn off the camera if found naked).

[User Action, Technology]
After Lisa turn on the feature, the device would now ask, "Lisa, would you like to turn me off for an hour?" around dinner time. And Lisa would readily confirm after receiving the notification.

[Resolution]
Lisa feels much relieved to manage her device settings.

Figure 15: Storyboard #9 Contextual Privacy Reminders



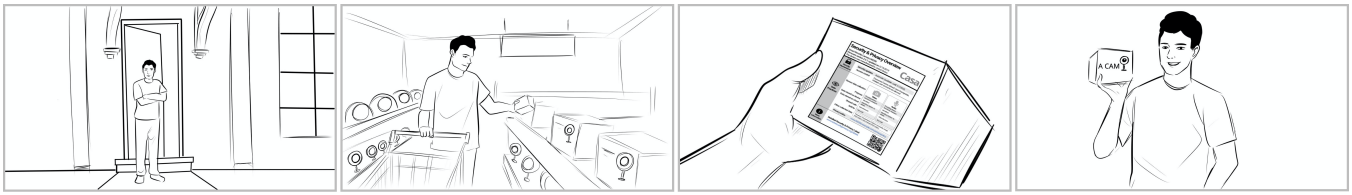
[Character, Context]
John is considering purchasing a vacuum robot, which searches for dirty spots to clean up with a camera. However, he feels skeptical and concerned that the camera might capture image/video data about people in his family.

[Problem]
Through exhaustive online searches, John found that the manufacturer's statement about data collection is very vague. Customer reviews and product testing reports barely touch on that topic either.

[User Action, Technology]
John uses a third-party tool that offers a simulation feature. He can drag an object into a simulated environment to see how the vacuum will react in the virtual setting and verify what data the robot might send out.

[Resolution]
John learns that the robot actually turn-off the camera automatically when it detects a person in the scene. He is now assured and decides to purchase the robot.

Figure 16: Storyboard #10 Privacy Simulator



[Character, Context]
Adam wants to purchase a smart camera to guard his front door for hours away from home.

[Problem]
While Adam is browsing through all types of security cameras at the store, he wonders how these cameras would handle the data they collect.

[User Action, Technology]
Later, he notices a privacy label on the packaging of each device. The label concisely informs him of the actual data practice and contains a QR Code that directs him to more detailed information on a website.

[Resolution]
Adam feels relieved as he can quickly understand how the devices work with his data. Furthermore, he can easily compare this information between different devices and purchase the one that suits his needs.

Figure 17: Storyboard #11 Privacy Nutrition Labels

B Appendix: Survey instrument

The appendix material is formatted differently from what participants saw in the survey. Sections correspond to the components in Fig. 3 and 4.

B.1 Generic privacy index questions and online PPB

Q1 Having companies collect my online behavior is a problem for me. ○ Strongly agree ○ Agree ○ Somewhat agree ○ Neither agree nor disagree ○ Somewhat disagree ○ Disagree ○ Strongly disagree
Q2 Having companies use my online behavior to show me advertisements is a problem for me. (Same options as Q1)
Q3 Having companies share my online behavior with other companies is a problem for me. (Same options as Q1)
Q4 Do you ever use some of the following behaviors to protect your personal information and privacy on the internet?

□ Use an ad blocker
□ Delete cookies
□ Decide to refrain from visiting a website because it is only accessible when you accept cookies
□ Decline to accept cookies when a website offers the choice
□ Use the private mode in your browser
□ Delete browser history
□ Use opt-out websites (such as www.youronlinechoices.com) to configure whether ads are based on personal data
□ Use the "Do Not Track" function in your browser
□ Use special software in your browser (such as Ghostery and Abine Taco) that makes it harder for companies to collect personal data
□ I don't use any of the behaviors above.

B.2 Smart home status questions

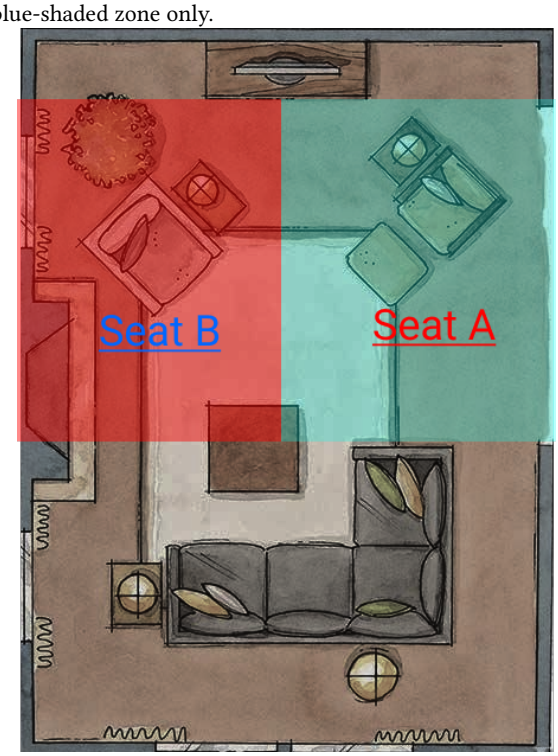
Q1 What best describes your living situation? ○ Rent ○ Own
Q2 Who do you live with at your home? ○ Alone ○ With family member(s) ○ With roommate(s)
Q3 Please check all types of smart home devices you have deployed in your home.

□ Smart Lighting (e.g., Philips Hue, LIFX, IKEA Tradfri, Xiaomi Yeelight)
□ Motion Sensor (e.g., Xiaomi Motion Sensor, Philips Hue Motion, Ecolink Motion Detector)
□ Smart Camera (e.g., Yi, Foscam, Xiaomi Xiaofang, Amrecst ProHD)
□ Smart Fan (e.g., Xiaomi Air Purifier, Dyson Link Air Purifier)
□ Robot Vacuum (e.g., Dyson 360 Eye, iRobot Roomba, Neato Robotics Botvac)
□ Door Sensor (e.g., Xiaomi Door Sensor, Ring Alarm Contact Sensor, Nest Detect Sensor)
□ Smart Switch/Button (e.g., Amazon Dash Button, Fibaro The Button, Xiaomi Button. Elko ESH)
□ Smart Temperature Sensor (e.g., Broadlink A1, Wink Relay, Fibaro Z, Xiaomi Temperature and Humidity Sensor)
□ Media (e.g., Amazon Echo, Google Home, Sonos PLAY, Apple TV)
□ Smart Power/Plug (e.g., Broadlink SP, TP-link Kasa Wi-fi Plug, Belkin Wemo Smart Plug, Fibaro Wall Plug)
□ IR Blaster (e.g., Broadlink RM, Xiaomi Universal IR Remote Controller)
□ Smart Smoke Detector (e.g., Nest Protect, Kidde Smoke Detector)
□ Smart Alarm (e.g., Dome Home Automation Siren and Chime, SimpliSafe Home Security System)
□ Smart Thermostat (e.g., Nest Learning Thermostat, Ecobee, GoControl Thermostat)
□ Smart Home Hub (e.g., Samsung Smart Things Hub, Wink Hub, Xiaomi Gateway)
□ I don't use any smart home devices.

Q4 Please estimate the number of smart home devices you have deployed in your home. ○ 0-5 ○ 5-10 ○ 10-20 ○ 20-40 ○ 40-80 ○ 80+

B.3 SH-PPB Definition Quiz

Bobby recently set up a smart camera in his living room for security purposes. You can see the layout of his living room below. The smart camera records and streams any video data it captures within the blue-shaded zone only.



Q1 Before setting up the camera, he used to sit on Seat A within the blue-shaded zone, but now he sits on Seat B more often to avoid being captured by the camera. Is this a smart home privacy-protective behavior? ○ Yes ○ No

Q2 Now, every time he gets into the blue-shaded zone, he receives an alert on his phone, which reports to him as "something has entered the camera's view." Before setting up the camera, he used to sit on Seat A within the blue shaded zone, but now he sits on Seat B more often to avoid receiving repetitive non-useful alerts. Is this a smart home privacy-protective behavior? ○ Yes ○ No

Q3 Bobby also routed the power to the smart camera through a smart plug. The smart plug would automatically turn off the power

for the camera when Bobby is at home. So the camera would not unnecessarily record him in the video streams. Is this a smart home privacy-protective behavior? ○ Yes ○ No

B.4 SH-PPB Inquiry Questions

Q1 Do you have any privacy-protective strategies, tricks, or experiences to share with us? We will review your answers manually. Note, for each valid unique PPB, we offer $1 bonus. ○ Yes ○ No

If the participant answers no: Q2 Here are the techniques you perform to protect your personal information and privacy on the internet: [we carry forward the choices the participants answered in online PPB questions]. Could you compare and elaborate on any differences in your privacy-protective behavior between online browsing and smart home usage.

If the participant answers yes: Q3 What do you actively do to mitigate the collection, usage, and sharing of your personal information from smart home devices to protect your online privacy? Please articulate the context of your tricks, the types of involved devices, if any, the types of privacy concerns you may have, and how they can address your privacy concerns.

Q3.1 What is your trick/PPB?
Q3.2 What device(s) is relevant to your trick/PPB?
Q3.2 What device(s) is relevant to your trick/PPB?
Q3.3 What is your privacy concern(s)?
Q3.4 When and how often would you perform this trick/behavior?
Q3.5 What device features would you wish to have to better address your privacy concern(s)?

B.5 Questions for each storyboard

Q1 Could you relate to the person's concerns shown in the storyboard? ○ Definitely yes ○ Probably yes ○ Might or might not ○ Probably not ○ Definitely not

Q2 How does this technology shown in the storyboard address the described concerns? ○ Extremely effective ○ Very effective ○ Moderately effective ○ Slightly effective ○ Not effective at all

If the participant considers the technology effective in Q2:
Q3 Could you describe some scenarios that you may use the technology shown in the storyboard?

If the participant does not consider the technology effective in Q2:
Q4 How can this technology be made more effective to address your need? For example, what would you like to change or add?

B.6 Storyboards ranking

Q1 Please rank the technologies shown in the following scenarios in order of effectiveness of addressing your privacy need in your smart home, where 1 is most effective and 3 is least effective.

Q2 Could you briefly explain the rationale for your ranking?