"You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users

ANNA LENHART, University of Maryland, College Park, USA
SUNYUP PARK, University of Maryland, College Park, USA
MICHAEL ZIMMER, Marquette University, USA
JESSICA VITAK, University of Maryland, College Park, USA

Fueled by Internet-of-Things technologies and spanning a wide range of sensors, speakers, and cameras, smart homes promise to make our lives easier and automate routine tasks. From speakers to security cameras, smart home devices (SHDs) answer our questions, monitor our home environment, and conserve energy. They also collect significant data, ranging from on/off commands to audio and video data, and they do this in some of our most private spaces. In this paper, we explore the privacy risks associated with SHDs by focusing on privacy-conscious smart home power users—those who spend significant time and money to research, install, and integrate devices throughout their homes and engage in advanced device and network management strategies to mitigate privacy concerns. Drawing on data from 10 focus groups with 32 privacy-conscious power users, we identify the key privacy risks they perceive from this technology, as well as how they mitigate those risks through increasingly complex strategies. Our findings reveal that navigating the technical landscape that makes up the smart home environment—including what data is collected, what options are available for managing or restricting data flows, and who has access to data collected by SHDs—is complex and often confusing, even for people who spend significant time researching devices and integration options. We use these findings to argue for further development of tools that are transparent, easy to use, and aligned with the privacy needs of a diverse userbase.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; *Privacy protections*

Additional Key Words and Phrases: privacy, internet of things, IoT, smart homes, security, power users, trust

ACM Reference format:

Anna Lenhart, Sunyup Park, Michael Zimmer and Jessica Vitak. 2023. "You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 7, CSCW2, Article 247 (October 2023), 34 pages, https://doi.org/10.1145/3610038

Corresponding author's address: Jessica Vitak, jvitak@umd.edu, University of Maryland, 4130 Campus Drive, College Park, MD 20742, USA.

2573-0142/2023/10 – Art 247. https://doi.org/10.1145/3610038

1 INTRODUCTION

The last decade has seen tremendous advances in computing, from smartphones and wearables to sensors and apps. Much of this technology falls under the broad umbrella of the Internet of Things (IoT) which Mattern and Floerkemeier [67] define as "a vision in which the internet extends into the real world embracing everyday objects…. An Internet of Things makes computing truly ubiquitous" (p. 242). IoT is driven by "smart" objects that use sensors to collect data about their environment and share that data with other devices, end-users, or third parties through embedded networking capabilities.

As these technologies have proliferated, they have become mainstays in the home, where sensors, cameras, and microphones are now commonplace. When a home contains multiple IoT-enabled devices, it may be referred to as a "smart home," which Gram-Hanssen and Darby [31] describe as spaces that "incorporate digital sensing and communication devices" that "communicate with each other seamlessly" (p. 94). They further note that smart home devices provide four primary services: energy control, home security, entertainment/ambience, and health monitoring. Popular smart home devices (SHDs) include speakers, TVs, security cameras, locks, lights, thermostats, and appliances, and all are designed to provide utility and convenience. Users can further enhance this utility by building ecosystems of connected devices [65]; this process is typically achieved by using an integration platform to connect and manage devices through a central hub. The most popular integration platforms include corporate (Apple, Google, Amazon) and open-source (Homebridge, Home Assistant) options.

As smart home technology continues to grow in popularity—the global market in 2021 was expected to reach US$100 billion [94]—it is critical to evaluate the privacy and security risks SHDs pose, and identify strategies to mitigate those risks. A significant amount and diversity of data are collected from SHDs and, importantly, that data collection happens in the home, which Mallett [63] defines as "a private, often familial realm clearly differentiated from public space and removed from public scrutiny and surveillance" (p. 71). By this definition, SHDs violate core assumptions of the home as a safe space away from surveillance; this contradiction was highlighted in 2015 when journalists discovered a line in Samsung TV's privacy policy stating that conversations near a TV would be collected and shared with third parties [36].

When data collection happens in the background or in unexpected ways—like in the Samsung TV example—it raises concerns about what data is collected, where that data is stored, and who it is shared with. Researchers have highlighted both technical (e.g., [9,40,43]) and social (e.g., [54,108,111]) privacy risks raised by SHDs, including adversaries using daily patterns to identify when a person is not home [28]. To make matters worse, users may have limited or incomplete threat models to assess risks associated with these technologies [111].

In this paper, we build on prior work by analyzing how privacy-conscious smart home power users think about and manage the data generated by devices in their smart homes. "Power users" refers to people who "exploit the devices to the fullest extent… they use the devices more innovatively, efficiently, and thoroughly than ordinary users" [112] (p. 1743). Power users are an important but understudied subset of technology users; because they are often at the leading edge of technology development, they are likely among the first to identify potential risks raised by technology use and think creatively about how to manage their devices and data. By further focusing on *privacy-conscious* power users, we can surface a wide and deep range of perceived risks, as well as more complex approaches concerned users take to limit unwanted access to their data. Therefore, we focus our analysis on two research questions:

RQ1: What concerns do privacy-conscious smart home power users have regarding their SHDs and the data they generate?

RQ2: How do privacy-conscious smart home power users mitigate these concerns through their purchasing decisions and their device/network management?

We present findings from 10 focus groups with 32 U.S. adults—who we describe as privacy-conscious smart home power users—identifying four major categories of perceived privacy risks to using SHDs and two major categories of risk mitigation strategies participants employ in their homes. Notably, we identify several advanced strategies that are rarely discussed in prior work (e.g., setting up a Pi-hole or multiple routers to isolate devices), which we attribute to the nature of our sample.

These findings extend prior work on privacy and security risks associated with IoT and smart homes in several notable ways. First, we focus on people who have built out a smart home ecosystem with many interconnected devices, rather than those who are using a single device like a smart speaker. This shift is important because smart home technology is getting more popular—and more devices in the home means more data collection and more security risks (via device vulnerabilities). Second, we provide insights from privacy-conscious power users, who think about and use these devices in creative and advanced ways, giving insights into a future where smart home technology is more fully integrated into living spaces. Third, we capture a range of strategies employed to mitigate privacy and security risks from SHDs, something that few studies have addressed, and never in detail (e.g., [89,109]).

In the following sections, we first describe the smart home environment to help situate our findings, as our participants set up complex ecosystems that often comprised many devices and one or more integration platforms. We then summarize prior research on smart homes and privacy/security before detailing our data collection. In the findings, we address our RQs by exploring the risks and mitigation strategies articulated by our sample of privacy-conscious power users. We conclude by reflecting on the complex and often confusing technical landscape that surrounds the smart home environment—a landscape that even highly engaged power users found challenging. Given that most people do not have the skills or motivation our participants displayed, we argue that these findings highlight the critical need for smart home tools that are transparent, easy to use, and aligned with users' privacy needs.

2 OVERVIEW OF SMART HOME TECHNOLOGY ENVIRONMENT

Before we review prior research on privacy considerations for smart homes, this section provides a brief overview of the smart home technology environment. As the market expands, consumers are increasingly faced with a complex array of devices, integration platforms, and communication protocols that are often surprisingly difficult to set up and automate [104]. This complexity influences how people mitigate privacy concerns and underscores the importance of our findings. For a more complete introduction to smart home technologies, architectures, and services, see [15,28]. Figure 1 summarizes the various ways people may manage their devices.

2.1 Smart Home Devices

SHDs are the physical hardware that makes smart homes work. The most common are smart speakers (e.g., Amazon Echo and Google Home) that provide voice-activated interfaces to relay information and perform basic automations through their virtual assistants. Smart speakers may also act as a "hub" in a smart home, allowing for centralized control of other devices. Voice

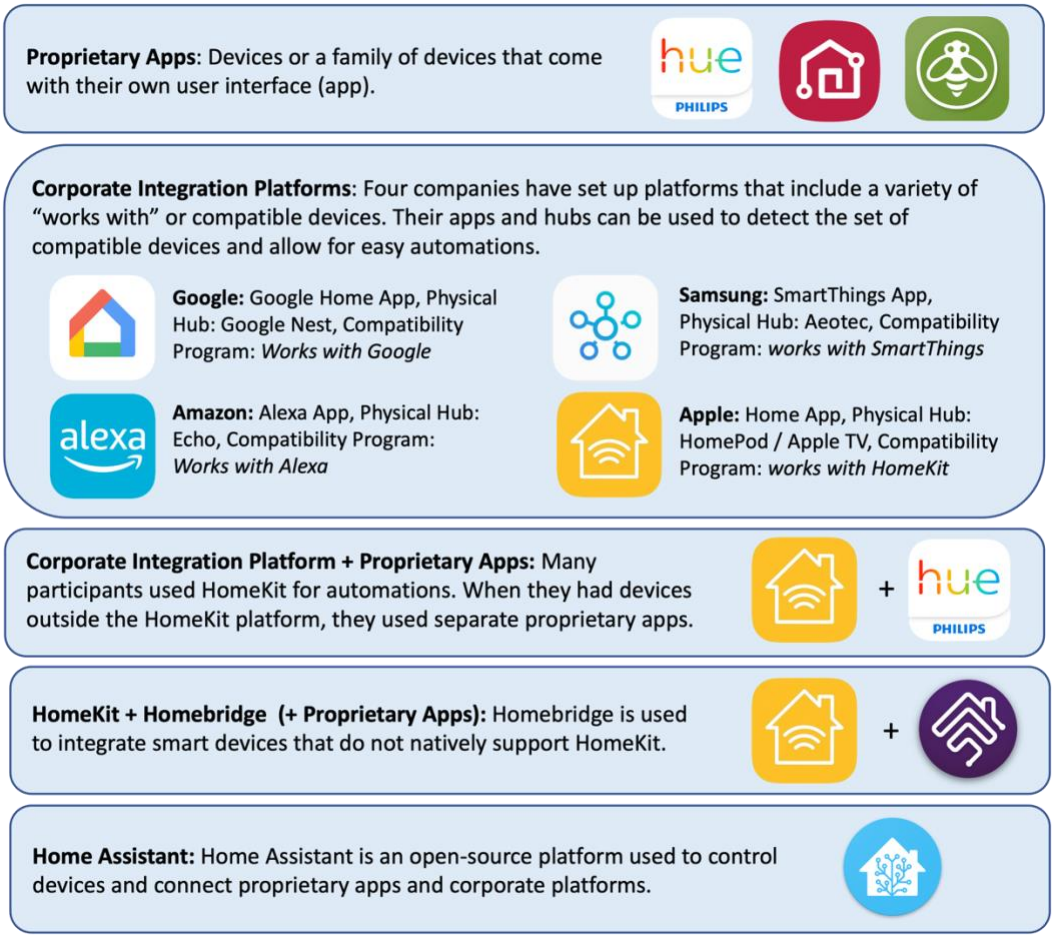

Fig. 1. Approaches for integrating smart home devices, applications, and automations.

SHDs are the physical hardware that makes smart homes work. The most common are smart speakers (e.g., Amazon Echo and Google Home) that provide voice-activated interfaces to relay information and perform basic automations through their virtual assistants. Smart speakers may also act as a "hub" in a smart home, allowing for centralized control of other devices. Voice assistants require an internet connection to answer most general requests and queries but can also be used for home automation commands when set up on a local network. Other popular SHDs include switches and light bulbs, internet-connected doorbells and security cameras, smart garage doors and locks, thermostats, and internet-connected appliances.

Generally, SHDs connect to the internet or some other central hub within the house and respond to programmed automations or voice commands. Nearly all modern TVs include internet connectivity features to run streaming apps natively, and many integrate with Amazon or Google assistants. Less common SHDs include internet-connected sensors to detect air quality or water leaks, utility meters, blinds and window treatments, and even automated devices to physically turn otherwise "dumb" switches on and off within the house. Most SHDs have a mobile app with a user interface to manage and control functions remotely.

2.2 Integration Platforms

Most of our participants relied on an integration platform to help coordinate and manage the multiple SHDs in their home. Integration platforms act as a "command center" for managing devices, allowing them to communicate with each other and enabling automated actions, often across different manufacturers. The most popular integration platforms used in smart homes have been developed by Amazon, Google, and Apple.

Integration platforms typically consist of a physical hub, an application providing a user interface, and a common software and/or networking framework to ensure devices can communicate and work with each other. For example, Apple's physical hub is usually a HomePod or an Apple TV, supported by the Apple Home App and Siri Voice Assistant; it operates on Apple's proprietary HomeKit connectivity framework. Compatible devices within each integration platform are programmed to be easily recognized by the physical hub or application. Devices are typically sold with labels indicating which integration platforms and communication protocols they support, such as "Works with Alexa" or "Works with HomeKit." Thus, integrated platforms have helped consolidate the diverse SHD market into a handful of ecosystems.

Integration platforms vary in their openness. It might be easy to add a smart garage door opener if you use the Amazon Alexa ecosystem, but Apple takes more of a "walled garden" approach to their HomeKit platform [93], and thus many SHDs are difficult to integrate into their framework. Third-party, open-source gateway products such as Homebridge and Home Assistant have emerged to help users control SHDs that are not engineered to work with one's preferred integration platform. These gateways typically must be installed on a separate computing device (e.g., a spare laptop or a low-cost Raspberry Pi) to become a hub for the SHDs, and they often require more effort and skill than simply relying on the standard integration platforms and proprietary apps.

2.3 Communication Protocols

Communication protocols allow SHDs to "talk" to the hub or other devices within a smart home. They enable hubs to control other devices, provide remote device management when away from the home, and allow cross-device automations (e.g., turning an interior light on when the front door's smart lock is activated). Some communication protocols are short-range; devices connect to hubs through close-range and low-power wireless network protocols like Bluetooth, Z-Wave, and Zigbee [23], which do not require internet access. Apple's HomeKit Accessory Protocol and Google's Weave are other examples of short-range protocols used to connect SHDs within an ecosystem. Other devices may be configured to connect to each other via a home Wi-Fi network, but without necessarily connecting to the internet itself.

In contrast, some devices require an internet connection to function. Smart speakers, hubs, and integration platforms typically rely on internet-connected communication protocols, most commonly through Wi-Fi or wired internet access. Other SHDs connect directly to the internet through a home Wi-Fi network rather than short-range connections to a hub, including devices with heavy data transfers (e.g., smart TVs), common appliances like washing machines, or SHDs too far removed for short-range protocols to be effective (e.g., external cameras). Figure 2 shows a typical SHD network.

2.4 Network Configuration and Management

Various customizations could be made to the network in Figure 2 to provide additional privacy protections. For example, virtual network routers can provide local connectivity for devices without directly connecting to the primary network router. Additional wired routers and Wi-Fi subnetworks can be used to segregate SHD traffic from other household internet use [50]. For example, a second network router could be added to Figure 2 to segregate the washing machine and TV data from other internet traffic. Another advanced techniques is "flashing firmware" to override a device's default settings and force it to connect to a custom network configuration [92].

Smart home users can also monitor and manage network traffic through various means. Network monitoring tools, including specialized ones such as IoT Inspector [40], allow users to view network connections and traffic among SHDs in their homes [37]. More advanced network management techniques include utilizing blocklists, DNS relays, or Pi-holes to prevent internet traffic from flowing to unwanted domains or IP addresses [7,33,46].

3 RELATED WORK

In this section, we summarize prior work related to our two research questions. We use these findings, which largely focus on non-power users (or users with a mix of skill levels) as a baseline from which to compare our findings with privacy-conscious power users. Marathe and colleagues [64] define power users as a combination of four components: *competence* (ability to set up and manage devices), *motivation* (to learn more about the technology), *expertise* (technical skill), and *desire* (to use a given technology to its full potential). Researchers have suggested that smartphone power users are more privacy-conscious because they install fewer apps and grant fewer dangerous permissions on their phone [48,70]. Kang and Shin [48] also found that power users

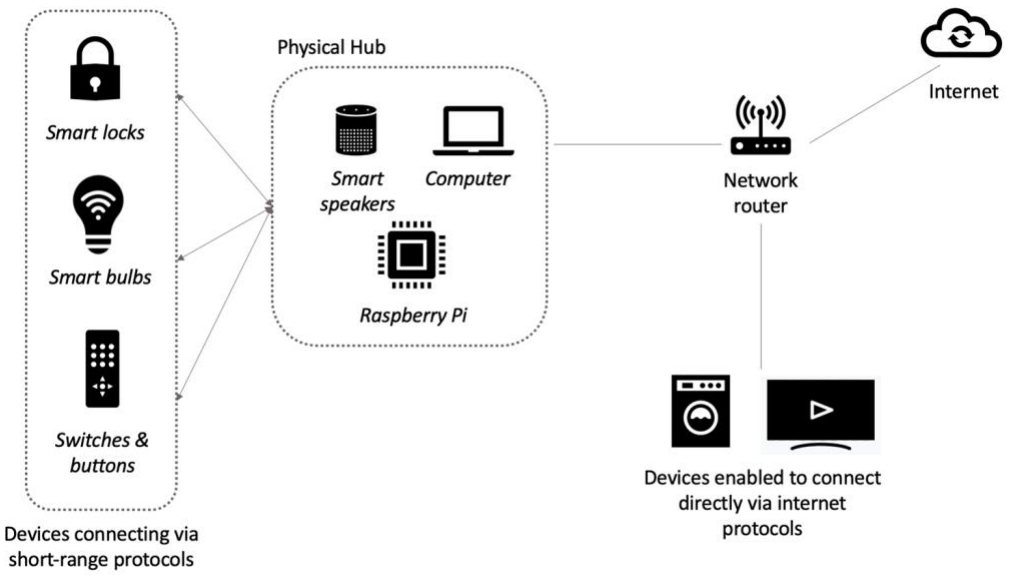

Fig. 2. Smart home devices using a range of communication protocols within a smart home.

expressed greater concerns about privacy intrusions related to their smartphone use, but they also expressed higher trust in mobile companies and services. On the other hand, Cho et al. [20] found that offering privacy customization options decreased power users' trust in smart speakers; they argue that power users are likely interested in saving/analyzing commands, and features like automatically deleting voice data may feel like "extra work without clear benefits" (p. 9). This suggests a tension between the core characteristics of power users—the desire to learn about, use, and adapt technology for the greater personal benefit—and privacy considerations. We explore this more in our findings.

3.1 Perceived Risks and Concerns Associated with IoT and Smart Home Devices

Since IoT devices must collect data from users and/or their environment to work, researchers have explored contextual factors that influence users' perception of data practices in the IoT environment. Although these factors are often difficult to separate, studies have highlighted *what* kind of data is being collected, *where* the data is being collected, and *who* is collecting the data as important factors.

First, considering *what* types of data are being collected, users are most concerned with audio and video data [18]. For example, Dunbar and colleagues [25] found that people's perspectives on SHD audio privacy fell into three categories: pragmatists, who accepted risks to get benefits and trusted companies to protect their data; guardians, who confidently engaged in strategies to reduce privacy risks; and cynics, who expressed uncertainty about data collection but lacked the knowledge to effectively manage their data. On the other hand, people are unconcerned with non-audio/visual data, which Kurze et al. [52] refer to as "simple data," due to a lack of understanding of potential privacy risks and thinking that nothing interesting could be derived from those data. As such, users' perceptions of the types of data being collected relate to how sensitive users are to that data, which is often related to the type of device it was collected on. For example, Zimmer and colleagues [113] found that many people using fitness trackers had little to no concerns about their step data, viewing that as non-sensitive. Kwon et al. [53] found that intimate data (from a smart shower) only becomes sensitive when it is discussed with others (e.g., partners, researchers), suggesting that data sensitivity is difficult to define and highly contextual.

Next, when considering the location of data collection (*where*), researchers have found that people are skeptical or concerned about data collection in their homes [8,21,26,56,68,99]. Emami-Naeini and colleagues [26] found that privacy preferences varied significantly by the location of data collection; participants were significantly less comfortable with data collection happening in the home than any other location. It is important to note that SHDs can be deployed within different areas or rooms, and researchers have found that location within the home also affects people's privacy concerns. For example, bedrooms [21] and bathrooms [68] are viewed as the most concerning spaces in the home because they are places related to self-appearance and intimacy.

Third, researchers have found that *who* is collecting the data is important to users [8,55,56]. Multiple studies have demonstrated that people generally regard the government with skepticism and may be unwilling to share personal information with government entities [8,35,56,111]. Zheng and colleagues [111] found that "technically skilled early adopters" trust manufacturers to use collected data for legitimate purposes (i.e., improve products and user experience), but have expressed significant distrust regarding government and internet service providers (ISPs) accessing their data. Likewise, trust in technology companies and brand reputation plays a role in decisions to use smart speakers [59,91,109].

When considering specific smart home devices, three of the most popular—and therefore most studied—are speakers, TVs, and cameras. Smart speakers are extremely popular: a 2022 NPR/Edison Research survey found that 35% of U.S. adults have one or more in their home, likely due to their low cost, functionality, and ease of use [72]. Trust also plays an important role in determining smart speaker privacy concerns: Lau et al. [54] found that smart speaker users trusted the companies not because of their privacy and security measures, but because of their prior positive experience with the companies in other contexts. Both users and non-users have expressed concerns about the evolution of these devices; many smart speakers now come with cameras and have features (e.g., Amazon's "drop in" feature) that make them feel more invasive, especially when placed in spaces like bedrooms [99].

Smart TVs are also widespread in homes, and Malkin et al. [62] found consumers often purchase TVs without knowing they are "smart," given their widespread availability in the marketplace. This is concerning, as Ghiglieri et al. [29] found a general lack of awareness of privacy risks related to smart TVs, including their ability to collect audio, video, and viewing history data. Further, Rutledge et al. [80] warn that the data collection practices of smart TV makers are largely unchecked by policy or regulation, and their privacy policies are often misaligned with consumers' needs and preferences. Malkin et al. [62] found users were willing to "dumb down" their TVs (i.e., disconnecting them from the internet) if data was being shared with third parties, but Ghiglieri et al. [29] noted users are unwilling to disconnect their smart TVs unless clear privacy risks are present.

Internet-connected smart cameras—including Amazon's Ring devices—are also increasingly popular. Tan et al. [90] found that people use smart cameras to enhance everyday activities such as managing guests and packages, monitoring pets and kids, and casually spying on neighbors. Some smart cameras not only collect video data but also audio and environmental data. For example, some are configured to detect motion, noises, persons (including via facial recognition), and "unusual activities" [90]. Pierce [77] notes that smart cameras are "foot-in-the-door devices" that take small steps to gain acceptance over time, fitting with Oulasvirta et al.'s [74] previous findings that people gradually came to accept camera surveillance in their homes, even if they initially opposed it. Researchers have also highlighted privacy implications for bystanders and others captured by cameras. Ahmad et al. [5] found that bystanders often want physical privacy controls to manage their exposure to smart cameras, a desire complicated by the fact that primary owners manage device settings and deployment [78].

3.2 Strategies to Mitigate Smart Home-Related Privacy Concerns

Few studies have explored users' specific strategies to mitigate privacy concerns in smart homes. Frequently, gaps in user awareness of data practices and security risks translate into a failure to engage in *any* mitigation strategy [89,109]. On the other hand, users with a technical understanding of smart homes are able to identify network-related vulnerabilities and threats and engage in technical strategies to mitigate their privacy concerns [109]. In other cases, users fail to take protective actions because they lack a fundamental awareness that their devices are "smart" [29,62,103].

When users do act, their mitigation strategies vary greatly, and they can be roughly categorized into non-technical and technical strategies. Non-technical mitigation strategies include altering one's behavior or interaction with the devices, adjusting device location [89,109], or limiting use by avoiding certain functions or providing only necessary information during setup [89]. This practice seems to be common with smart speaker users [2,41,54]; for example,

Huang et al. [41] found that smart speaker users avoid making purchases through voice command and do not share sensitive information with their voice assistant to mitigate their concerns, even though this may lessen their user experience.

Technical mitigation strategies focus on adding security protections or modifying data flows on devices. These approaches may be less common because they generally involve more knowledge about devices and how they interact with one's larger smart home network. In fact, Jin et al. [45] found that only 1% of respondents in their study managed their smart speaker data through technical strategies. These strategies include traditional, device-level security practices like changing default passwords, using two-factor authentication [89], turning off features such as microphones, or deleting past video recording or behavior logs [103]. Network-based strategies—again, rarely, if ever, mentioned—include isolating devices from one another or from the internet completely [80,103,109], using short-range protocols to prevent their physical hub from communicating with cloud servers [103,109], and using tools to monitor and block traffic [43,80,103,109].

People who do not employ mitigation strategies may be unaware of privacy threats, lack the knowledge and/or tools to do so, or be unwilling to take the time to enact them [1,45]. For example, Abbott et al. [1] deployed IoT devices in eight households of people who reported interest in purchasing IoT devices; over a three-week period, they found that two-factor authentication was not used by participants, despite its privacy preserving functions, because of low perceived usability (e.g., inconvenient and unnecessary). Smart security systems (e.g., cameras) were used despite participants' privacy concerns, and while the researchers provided a Raspberry Pi Safe Router and Home Assistant dashboard, participants chose to use devices they were familiar with over the Safe Router, foregoing network-level mitigation strategies.

While this lack of engagement in robust privacy management is not surprising for non-power users—who may be more focused on the benefits and convenience the technology brings—we would expect that power users' approach to privacy management will reflect their drive to master the technology and customize it to their needs, while also considering how to best protect the data generated from the multiple, interconnected devices in their smart home ecosystem.

4 METHOD

To address our research questions, we conducted 10 online focus groups with 32 U.S. adults in August 2021. We chose semi-structured, virtual focus groups because they allow for a wide variety of perspectives in a setting that allows for immediate follow-up from other participants and facilitators [51]. Focus groups also work well for exploring perceptions and generating ideas [88], which were key goals for this study. In addition, our use of Zoom allowed us to recruit users from across the country. Prior work also suggests that virtual participation—from the comfort of one's home—can lead to richer conversations [86]; in our case, given we were discussing smart home technologies, this may also have offered a further benefit of reminding participants of their use of SHDs. Finally, virtual participation (versus in-person sessions) may have put some participants at ease and reduced power differentials between participants and researchers [51].

We provide details on recruitment, study design, and data analysis below. See the Supplemental Files for the recruitment text and where messages were posted, as well as the screener survey instrument, focus group protocol, and final codebook. See Park et al. [75] for a separate analysis of this data that explores design limitations of current SHD setups and recommendations from our power users on ways these systems can improve privacy and usability for all types of users.

4.1 Recruitment

Because we were interested in talking with people who used multiple smart home devices and we wanted a demographically diverse sample, we created a short screener survey for potential participants to complete and indicate their interest in participating in a focus group discussion. The survey asked about living environment (e.g., whether they lived with other people, whether they rented or owned their home), what categories of SHDs they used, and demographic questions. We also asked them to indicate their concerns about data collected by smart technologies and their comfort and confidence in managing SHDs in their homes.

After receiving institutional review board (IRB) approval, the survey was deployed in July 2021 using Qualtrics. Recruitment messages were shared via two of the authors' social media accounts and were posted on relevant Reddit forums and public Facebook group pages. In one week, we received 441 responses; after data cleaning and quality checks, we were left with 277 potential participants.

We then created a prioritized list of prospective participants using criterion and maximum variation sampling, two forms of purposeful sampling detailed by Patton [76] that involve selecting participants based on predetermined factors related to the research goals and selecting participants who are different across a set of specified characteristics. We included the following criteria for participation that connected to our goal of understanding how privacy plays a role in decision-making and use of SHDs:

1. **Smart home device usage.** Our screener survey asked participants which SHDs they used from a list of 12 categories (Q10). This led us to exclude those who only selected one device and to prioritize those who used multiple types of devices.
2. **Data concerns and mitigation behaviors.** A primary goal of this study was to understand what concerns smart home users expressed and how they mitigated those concerns. Therefore, we reviewed open-ended responses to survey questions regarding changes in SHD use and hesitation to use certain devices (see Q15-Q17). We also reviewed the four items included in Q9, which included statements regarding data privacy attitudes (e.g., "I'm concerned that 'smart' devices collect too much information"). We chose to look at multiple items because privacy is a multi-faceted concept and interacts with other factors. For example, someone could express relatively low concerns because they have high confidence in their ability to manage their devices and protect their data. We prioritized inviting respondents who shared examples of stopping or changing their use of SHDs and/or hesitancy toward using SHDs.
3. **Participant diversity.** We captured both demographic (gender, race, age) and living environment characteristics (renting vs. owning, living alone vs. with others) in the survey and included these factors in our decision-making. After narrowing our potential participant pool to 129 people based on the first two criteria, we then used these factors to create a prioritized list of participants that maximized diversity. For example, we prioritized female and non-binary respondents, as they represented a small percentage of the pool (14/129). We also prioritized non-white respondents for similar reasons (24/129).

We contacted 82 people based on the process above, emailing in batches and sending out new invites as needed to ensure we achieved saturation. From this, 38 people signed up to participate and 32 attended one of 10 Zoom focus groups during August 2021. Each session lasted approximately one hour and included 3-4 participants to ensure all had ample opportunity to

speak. At least two authors attended each session, with one acting as moderator while others took notes and occasionally asked follow-up questions. Each focus group opened with an ice breaker question regarding "a day in the life" of their SHD use, then transitioned into questions about their likes and dislikes with their SHD setup, thoughts on data collected by their devices, and concerns they had about SHD technology. We then transitioned to a virtual whiteboard activity using Google Jamboard, where each participant spent time individually mapping their devices onto an empty grid that accounted for perceived data sensitivity (x-axis) and desired control over data (y-axis). Prior to starting, the moderator described the activity and shared an example grid (see Figure 3); participants were then directed to find and fill out the blank grid (on subsequent slides) with their name on it. The session concluded with a discussion of desired design features to make SHD data flows more visible and accessible to users. All participants received a US$30 Amazon gift card in thanks for their participation.

4.2 Participants

Participant data is detailed in Table 1. Participants were likely to be male (n=25), white (n=23), and 36 years old on average (*SD*=9.26). Most owned their home (n=21), and 11 participants had children under 18 living with them, while seven participants lived alone. Nearly all participants used one or more smart speakers (Amazon Alexa, Google Home, or Apple HomePod; n=30) and some form of smart lighting (e.g., Phillips Hue lightbulbs; n=31). Other common SHDs used were sensors (n=27), TVs (n=23), thermostats (n=19), connected security cameras (n=18), and door locks (n=18). While we recruited from online forums for a variety of smart home platforms, many participants (n=21) were Apple HomeKit users, which had implications for our findings—something we detail below.

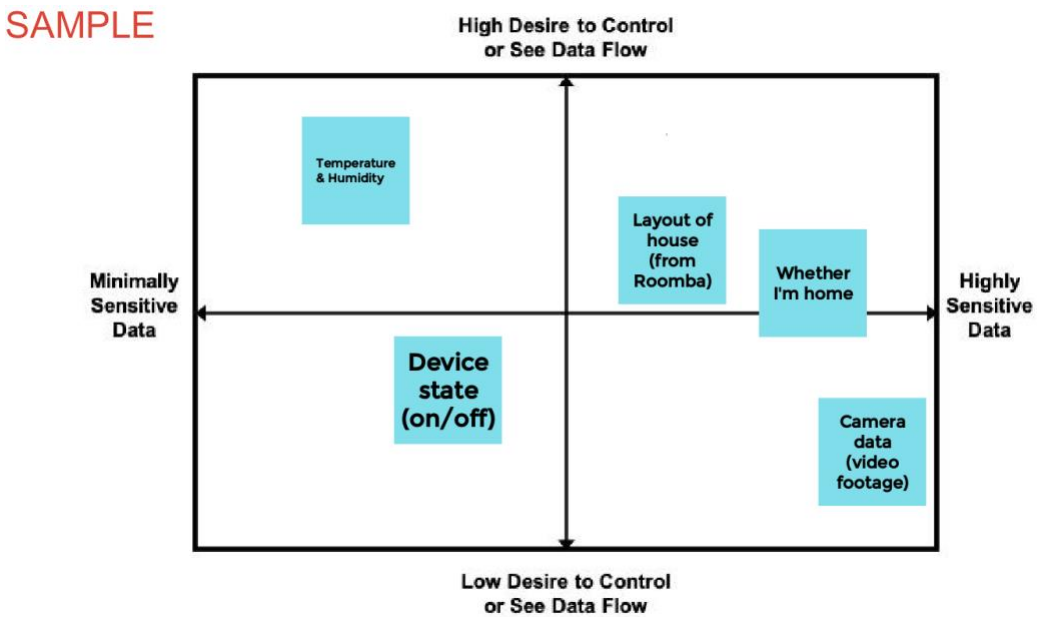

Fig 3. Sample Jamboard grid shown to participants before they completed the activity.

Table 1. Participant IDs, Descriptive Data, Data Concerns, and Smart Home Details

ID	Gender	Race	Age	Data Collection Concern[1]	Confidence Managing Data[1]	Comfort Using Devices[1]	Devices Used[2]	Integration Platform[3]	Advanced Network Mgmt?[4]
P1	M	White	37	6	6	5	1,5,6,8,11	HK	No
P2	M	Black	37	5	5	7	1,2,3,5,6,7,8,11	HA, HK	Yes
P3	F	Black	45	6	5	7	1,2,4,5,6,8,10,11,12	HK	No
P4	M	White	48	7	5	5	1,8	none	Yes
P5	M	White	52	6	5	7	1,2,3,4,5,6,7,8,10,11	HK	No
P6	M	White	52	3	5	7	1,6,11,12	ST	No
P7	F	White	37	6	6	5	1,2,3,6,11	HK	No
P8	M	White	38	7	6	7	1,2,4,5,6,10,11	none	No
P9	M	White	35	5	7	7	1,2,3,4,5,6,7,8,10,11	HK	Yes
P10	n/a	n/a	39	5	5	7	1,2,3,4,5,6,7,10,11	HK	No
P11	M	White	34	5	4	5	2,3,4,6,7,11,12	HA	Yes
P12	M	White	27	5	6	7	5,6,8	HK	Yes
P13	M	East Asian	55	5	6	5	1,2,5,6,10,11	HK+HB	No
P14	M	White	40	5	4	5	1,6,8,11	HA	Yes
P15	M	White	33	5	5	7	1,3,4,5,6,7,8,10,11,12	HA	Yes
P16	M	E Asian, White	38	6	2	5	1,2,3,4,5,6,8,10,11,12	HK+HB	Yes
P17	M	White	24	6	6	7	1,2,6,8,11	none	No
P18	M	White	47	5	5	5	1,5,6,10,11,12	ST	Yes
P19	M	White	20	7	6	7	1,5,6,8,11,12	HK	Yes

Table 1 (continued)

ID	Gender	Race	Age	Data Collection Concern[1]	Confidence Managing Data[1]	Comfort Using Devices[1]	Devices Used[2]	Integration Platform[3]	Advanced Network Mgmt?[4]
P20	M	White	39	4	6	7	1,2,3,4,5,6,8,9,10,11,12	ST, HA	Yes
P21	F	White	29	4	4	5	1,2,6,8,10,11,12	HK, HA	No
P22	M	White	32	7	5	7	1,4,6,8,10,11,12	HK, HA	No
P23	NB	East Asian	25	5	1	4	1,6	none	No
P24	M	White	32	6	6	7	1,3,5,6,7,8,10,11	HK+HB	Yes
P25	M	White	40	5	3	7	1,2,4,6,8,10,11	HK+HB	Yes
P26	M	White	28	5	5	7	1,2,4,5,6,8,10,11,12	HK	No
P27	M	American Indian	36	6	5	7	1,2,5,6,8,10,11,12	HK	Yes
P28	M	E&S Asian	20	6	6	7	1,3,4,6,8	HK	No
P29	F	White	30	5	2	7	1,2,3,6,7,8,10,11	none	Yes
P30	F	White	42	6	6	7	1,2,3,4,6,10,11	HA, HK	Yes
P31	M	White	23	6	2	5	1,2,6,8	HK+HB	No
P32	M	E Asian, White	47	5	3	7	1,4,5,6,8,11	HK+HB	No

[1] For these items, people were asked their level of agreement on a seven-point scale (1=Strongly Disagree to 7=Strongly Agree).

- I'm concerned that "smart" devices collect too much personal information.
- I'm confident in my ability to control how much personal information I share online and through my phone.
- I am comfortable using most of the smart devices in my home.

[2] Participants were asked to check off all SHDs in their home from a list of 12 types. Numbers in the table correspond to devices as follows: 1) speaker, 2) thermostat, 3) vacuum, 4) doorbell, 5) security camera, 6) lighting, 7) blinds, 8) TV, 9) refrigerator, 10) door locks, 11) sensors, 12) other.

[3] Participants who directly mentioned using one or more of the following hubs to manage their SHDs are labeled as follows: HK (Apple HomeKit), HB (Homebridge), HA (Home Assistant), ST (Samsung SmartThings). Note: several participants mentioned using Amazon or Google products but always in the context of integrating with or working alongside the listed platform, never as the physical hub.

[4] "Yes" is assigned to any participant who said they engaged in one of more of the following network management strategies: 1) setting up a Pi-hole or private DNS, 2) flashing devices with custom firmware to make them run locally, 3) setting up multiple routers to isolate devices, 4) setting up firewalls.

We describe our full sample as being privacy-conscious power users based on two criteria. First, our selection criteria led us to select participants who expressed data concerns, valued data privacy, and/or engaged in specific actions to reduce data flows from devices. Second, all participants qualify as power users based on Marathe et al.'s [64] four factors (competence, motivation, expertise, desire). Beyond that, we note that a subset of participants (n=16) displayed highly advanced technical skills; we labeled such participants as having *advanced network management* skills (denoted in Table 1 and described further in Section 5.2) if they said they engaged in one or more of the following network management strategies: setting up a Pi-hole or private DNS, flashing devices with custom firmware to make them run locally, setting up multiple routers to isolate devices, and/or setting up firewalls.

4.3 Data Analysis

After each session, the authors present on the call held a short debrief, sharing initial reactions and reflecting on the session in relation to prior sessions. This process enabled the team to discuss saturation throughout data collection. By Session 9, we agreed we had reached data saturation, which Saunders et al. [82] define as "the degree to which new data repeat what was expressed in previous data" (p. 1897); however, we chose to hold the final scheduled session because it included two female and one non-white participant, and we wanted to expand the perspectives of these groups.

All sessions were recorded with participant consent, and the audio files were transcribed via Rev.com. After reviewing for accuracy, transcripts were uploaded into Atlas.ti for qualitative coding by the research team. Using the qualitative analysis approach detailed by Miles, Huberman, and Saldaña [69]—which involves first- and second-cycle coding—the team developed an initial codebook based on the protocol and our research questions using "protocol" and "provisional" coding. Each team member coded one transcript from a session they did not participate in using this codebook and making notes about questions and suggestions for new or collapsed codes. The team then met to discuss their notes and refined the codebook and code definitions. Following this, each transcript was reviewed and coded by two authors.

Coded excerpts were then exported to Excel for second-cycle coding. Following Saldaña's [81] process of "theming the data," each team member selected two codes and categorized excerpts from each code to extract themes. This process of categorization involved reading and rereading the excerpts for a given code, assigning descriptive phrases for each excerpt, then organizing excerpts based on emergent themes. For each code, a team member wrote a detailed analytic memo to identify meta themes and provide examples from the data for each theme from that code [13]. These memos were discussed by the full team before writing up the findings. The first author also reviewed the Google Jamboard grids to identify notable differences between grids that belonged to advanced network management skills users and other participants.

5 FINDINGS

5.1 Privacy Risks and Concerns Regarding Smart Home Devices (RQ1)

Four interconnected themes emerged regarding the privacy risks and concerns our participants identified when buying and using smart home devices: 1) perceived trustworthiness of particular SHD platforms, 2) broader uncertainty about the type and amount of data collection, 3) concerns related to specific types of data collected, and 4) tradeoffs between utility and privacy concerns. We detail each of these below.

5.1.1 (Dis)trust in Platforms Influences Device Purchasing and Use. Because of the quantity and nature of data collected by smart home devices, it is unsurprising that concerns about trust were common when discussing purchase and use decisions. For example, P23 had a long list of "devices I would never use or that I'm strongly against," including Facebook Portal ("I absolutely would never live with anyone who has one of those and I would never allow that in an apartment with me"), Ring cameras, Nest cameras, and Amazon products. P29 was uncomfortable with Amazon's business model, saying, "I'm not crazy about the fact that they are coming into your home with the intention to sell to you." P27 became frustrated upon learning his smart thermostat came with an Alexa feature, and he disabled the feature, then did additional research to confirm there was no way for Amazon to collect audio data. Likewise, P13 said he was annoyed when Amazon bought the company Eero shortly after he purchased an Eero router. P5 noted that early on, when he was choosing an ecosystem, "the one I was most worried about from a security standpoint is Amazon…Their devices are plentiful, they're cheaper, generally, than what you would buy from Apple, but I just worried about that creeping intrusion." These sentiments align with and extend previous work on the role trust plays in the use of smart speakers [59,91,99,109].

Most participants opted for HomeKit's integration platform, with many noting that they chose Apple because they trust the company and its commitment to data privacy and security—even if that meant losing some functionality or spending more money. Apple has long positioned itself as a technology company that designs products with privacy in mind, as highlighted through privacy and encryption features in their hardware [32], intelligent tracking prevention in its Safari browser [85], and privacy nutrition labels that provide standardized information on data collected by apps [71]. This focus on consumer privacy protections resonated with participants: P19 said he selected HomeKit because "it's supposed to be really secure," and P13 noted that when comparing the three primary ecosystems, "Apple was the one that had the most privacy built into it." Similarly, P2 noted, "I think I trust Apple's privacy the most."

However, this trust in Apple was not absolute. P3 said, "I trust Apple to some degree, not blindly. But that was my way of trying to stay as privacy conscious as I could where I'm not thinking about it all the time." Likewise, P10 said he had done his "due diligence" and reviewed information from Apple on how the technology works, but he said there was only so much he (as a consumer) could do: "At some point, you do just have to trust and say, hopefully the system is designed the way they say it is and security researchers are looking at it and I'm just going to trust that that's safe."

Nonetheless, numerous participants commented that they were willing to pay more for HomeKit devices and/or deal with less functionality because of concerns that companies who made cheaper devices routinely collected and/or sold user data. P24 noted that while he previously owned some Echo Dot devices ("because they were cheap"), he became more concerned over time, especially after learning more about Amazon-owned Ring cameras, which he described as turning the doorbells "into a mesh network of video surveillance cameras for the police." P24 continued: "Just seeing how easy it was for that footage to be given up gave me a lot of pause around having those Amazon devices in our home listening." He later stopped using the Amazon devices. P5 said, "It [Apple] costs you more, but you have that little bit more of a peace of mind that there's a little bit more control." These sentiments are a departure from other smart home studies, where participants tend to focus more on usability and less on enhancing data privacy [6,42,83,110].

5.1.2 Concerns Due to Uncertainty About Data Flows and Lack of Control. Participants expressed a strong desire for greater information and transparency about smart technologies and grew concerned when they felt like they had limited control over their data. These concerns are not

entirely surprising, given media stories in recent years about devices recording conversations [38], companies and third parties using voice data for advertising [79], concerns about devices sharing data with police [16], and, shortly before our data collection, news that Amazon was experimenting with mesh networks and would, by default, automatically share Amazon device users' internet with their neighbors [30]. P6 noted that he was familiar with this new Amazon feature (Sidewalk) because he's a "geek" who had read up on it and was able to turn it off; that said, he noted it's probably unlikely that "average" users of these devices are as well-versed on these changes.

While our participants sometimes spent significant time learning about SHDs, even they felt uncertainty regarding what happened to their data. In talking about the various apps he used, P25 highlighted this uncertainty, saying, "you don't know exactly what they're getting access to, so when you give any company access to your information, it's always kind of scary what exactly they're grabbing." P20 shared the example of people discovering that energy companies could access and control Nest thermostats after several Texas companies adjusted residents' thermostats during a heat wave to reduce strain on the electric grid [84]; he said, "I don't participate in those programs. I don't like the idea that a vendor can reach into my house and adjust my knobs without me being aware of it. That is concerning—that's a level of control that I don't want somebody else to have." And even though P5 said he was satisfied with Apple's protections, he added the caveat that "I don't feel that it's 100% secure or that I can see into what it's doing."

5.1.3 Some Data Types Are More Concerning Than Others. The privacy risks our participants associated with their smart home devices varied significantly based on the *type* of data collected. Overall, participants were most concerned about interior cameras (video data collected in private spaces), followed by some concerns with devices that collected audio data. Participants were also very concerned about any data that needed to be shared externally with company servers.

While more than half of our participants said they used some form of camera in or around their home, these devices also raised the biggest concerns, especially for indoor cameras. P19 said he had "no problem" with exterior cameras, "but inside the house, [my kids] don't want to feel like they're just being watched. Not that I'm watching them or anything, but they just don't want that feeling of an invasion of privacy." P20 shared a similar sentiment, saying, "I'm not putting [cameras] in my house. I have lots outside the house…but I don't want interior cameras. That's too much of an invasion of privacy. Everything in my house is monitoring me, but that's where I draw the line at." Likewise, P29 said she was "not quite comfortable with having them in my house," while P31 said, "I don't think I'd ever get to the point where I feel comfortable having smart cameras either, even outside my home."

Participants also expressed considerable concern with microphone-enabled devices, especially smart speakers and smart TVs. P30 said she and her husband had enough concerns about their smart speakers that they carefully thought about where they put them and avoided rooms where the devices might pick up work-related conversations. P20 said he was "not a fan" of smart speakers and didn't like "when I'm talking about something and I start getting ads about the places that we discussed or a product that we mentioned that I didn't search for." When it came to smart TVs, participants were concerned with the amount of data they collected. P24 found the practice of smart TVs tracking and selling data "creepy as hell." P9 said he tells family and friends who are buying a new TV to not connect it to the internet. He was concerned that many people don't understand that "the reason you are buying a $500 72-inch TV is because we [the company] are going to be scraping everything and making a ton of money off [of] that."

While most of our participants expressed concerns about their SHDs, only one (P7) actively expressed little to no concern about the data these devices collect. Her comments resonated with the oft-voiced "nothing to hide" view of privacy; she said, "I don't really have anything to hide. We're not doing anything crazy. If they want to track how many times I open my garage door, then, okay…at this point, I feel that they were probably going to find the information out anyway."

5.1.4 Evaluating Tradeoffs Helps the Decision-Making Process. P7's comments in the previous section highlight one way in which participants thought about using SHDs as a tradeoff between the benefits the devices provided and the potential privacy risks they posed by using them in a private space. Tradeoffs came up when talking about decisions to purchase or use a device, and many of our participants described taking time, "doing research," and spending more money to balance their desire for functionality with that for privacy—or they acknowledged that, in some cases, they gave up one for the other. Because we spoke with power users, these evaluations of tradeoffs look different than what has been found in prior work (e.g., [89,109,111]); our participants were less willing to trade their data for convenience and more willing to spend time and money finding the best balance.

Tradeoffs were frequently mentioned when participants discussed their decision-making process around purchasing new devices for their home. In many cases, the primary tradeoff was between spending more money for privacy-friendly devices or getting greater functionality without those protections built in. Because our sample included many HomeKit users, it was unsurprising that many people chose privacy over functionality. P13 captured this sentiment when he noted, "To a certain extent, I'm sacrificing a lot of potential functionality and incurring greater cost, for the sake of being in a 'more private' environment." Others similarly preferred Apple HomeKit and its "walled-garden" approach, such as P30, an information security professional, who said she was slowly purchasing devices based on privacy-related features, even though a lot of the devices were more expensive, because "privacy is important and I really am interested in what data is being sent to what parties."

On the other hand, some of our participants chose to use non-Apple products to get increased functionality and interoperability. P4 used an Amazon Echo for streaming music, saying, "It wasn't my first choice for a smart device, but its capabilities were better than what I could find with my first choice [HomePod]. So yeah, that was a privacy tradeoff for me." HomeKit's lack of interoperability frustrated other participants when they couldn't connect certain devices in the Apple ecosystem. For example, P21 noted that all the SHDs in her home were part of HomeKit except the Nest thermostats. She said, "It was a little frustrating because I wanted to get those [Nests] in HomeKit, which isn't super easy to do. So we've been using Home Assistant to bridge everything together." P3 said she avoided getting locked into a single ecosystem because she found it "problematic," and it might require her to "rethink how you do a personal workflow." P7 also described being frustrated with Apple's walled-garden approach; after buying Sonos speakers (which are Alexa supported), she and her partner discussed switching ecosystems but decided against it "because then we're going to have to have separate devices just to run our things or 27 apps on the phone."

In the end, our participants described a core dilemma between privacy and convenience, a tension frequently highlighted in privacy research [4,24,99,102]. And while many participants described themselves as privacy-conscious and made purchasing decisions based on their desire to minimize data collection, they recognized that they sometimes had to sacrifice some privacy to get benefits from the devices. P17 encapsulated this sentiment when he said, "The key thing

that we've been trying to figure out is, how do we balance doing more of this [adding more devices] without it being a burden for ourselves. If something's not working at one point or is a burden in terms of privacy, we still want to make sure that we're keeping our stuff private as much as possible in this day and age."

5.2 Mitigation Strategies for Managing Smart Home Device Data (RQ2)

As P17 noted above, our participants often sought a balance between the utility gained by using SHDs within the home and managing the data that could be collected and shared. Throughout our sessions, participants shared varied approaches to manage the flows of SHD data. These mitigation strategies tended to take one of two forms: device-level actions, which tended to be simpler to enact, and network-level actions, which tended to require more technical proficiency. Across all participants, we observed higher engagement in mitigation strategies than has been reported in other smart home studies; outside of brief mentions in prior work [109,111], the depth and breadth of advanced network management strategies we report here have not been seen in smart home studies.

5.2.1 Device-Level Actions. Device-level actions generally represent simpler strategies used to manage devices and related data flows. Our participants described five categories of device-level actions, which we roughly organize by increasing amounts of complexity.

Strategic placement of devices. As noted above, participants considered data sensitivity when deciding where to locate SHDs in their home. P30 said, "[W]e keep Echos out of the rooms that we know potentially sensitive conversations are going to be happening. We know, if we want to have a conversation that we know is not overheard, we know where we can go in the house." P30 later added that "none of [our cameras] point inside the house in any way, shape, or form." Similarly, P16 noted, "In certain rooms we'll have Echo Shows, but the only reason we went with those was because they have the little cover—you can turn off the camera physically. However, in the kids' bedrooms, they have [Echo] Dots. I will not let a camera be in there at all."

Utilizing physical switches and buttons. In line with P16's comments, another common technique for addressing privacy concerns is ensuring that devices have physical means for ensuring privacy, such as a shutter or "kill switch." P17 explained, "I think if we were to add a camera, we'd want to make sure it had a physical privacy shutter." Physical shutters provide users with certainty that video data is not being collected. P22 described wanting a physical option for guests to manage devices, saying, "I actually went and got an Alexa for just the guest room…the Alexa has a nice button on top, where you can mute it, so I keep it muted whenever a guest is in there." P2 said he liked his Google Home Mini's functionality because they "have a physical button that will keep the microphone off."

Users can also add smart buttons or switches to their network and use automations set up through their hub to create a device that works like a remote with one-touch feature activation. P22 described needing to keep work conversations private, so he placed his HomePod on a smart outlet: "I have a button on my desk that I can hit whenever I have a meeting and that removes power from the HomePod which, at least to me, seems good enough that it won't be listening directly." This technique not only gives users a physical switch, but it also makes it easier to replace voice commands that may have required an internet connection. For example, P30 replaced Alexa commands with a Z-Wave button (i.e., a button connected to the network using a Z-Wave protocol) "so I can control what I need to from a button instead of from voice."

Changing device settings. Only a few participants mentioned adjusting device settings to protect their privacy. P1 mentioned that he "turned off a lot of stuff [that collects analytics] on

his TV." Additionally, participants described disabling Alexa, Amazon's voice assistant that both collects voice recordings and is connected to the internet. P27 noted that while he owned an Ecobee thermostat, he had turned off Alexa. Similarly, P26 purchased a thermostat that integrated with his HomeKit, "but it comes with an Alexa feature on it… not only did I disable it, but I did a lot of research to make sure that it wasn't a hidden Alexa kind of snooping device because I know how crazy Amazon is with things, putting them in your home, they hear basically everything."

Purchasing devices enabled for short-range protocols. By disabling Alexa, P26 not only limited the collection of voice data, but he also restricted the device to only operate on HomeKit's short-range protocol. Many participants took a similar approach when purchasing devices, selecting those that can run locally versus those that require an internet connection to operate. For example, P22 described installing lights in his guest room that "are connected over Bluetooth so I feel confident that they're local." Taking advantage of this technique requires the user to review the documentation or labels accompanying the new devices and look for compatibility with short-range protocols. As P6 noted, "There are some devices that do require cloud access…and you just want to be aware of whose cloud that is and what traffic is going there and what's being sent."

The ability for devices to *not* connect to the internet was one of the most cited reasons for purchasing HomeKit devices because all "Works with HomeKit" devices include the ability to interconnect via the HomeKit Accessory Protocol. P10 explained, "I think the big draw for me with HomeKit is that a part of the spec is that everything needs to work locally. So if the devices don't have a connection to the internet, they still function. And that's been huge." Similarly, P29 said she only uses HomeKit-compatible devices because "once the device is set up, it should be able to work without having to contact company servers... You shouldn't need to share your data."

Modifying device firmware to enable short-range protocols. Some participants took additional measures to force devices that otherwise required an internet connection to be controlled over a local network. This process of "flashing firmware" forces a device to connect to a local hub instead of the internet. P14 explained, "If I'm looking to buy something, it has to be easily connectable to Home Assistant, or it has to be something that I can flash with a different firmware to make it so. …then I just use utilities within Home Assistant to rewrite the firmware so it's something that's just working locally." Similarly, P6 explained how firmware provides options when he is considering adding sensors to his smart home, and how it allows people to purchase SHDs that are cheaper while still maintaining a secure environment in which data remains on the home network.

5.2.2 Network-Level Actions. Network-level actions can be utilized to further manage whether and how data flows outside of the home, and the 16 participants who engaged in advanced network management skills (see last column in Table 1) exhibited particular proficiency in this domain. These actions typically require additional knowledge and skills beyond what is needed for device-level actions; P29 noted how users often need to go "down the tech hole" to understand "which servers are being pinged and how much data is going through." We describe two main categories of network-level actions that were employed by participants: isolating devices on the network and monitoring and controlling network traffic.

Isolating devices on the network. Participants discussed "isolating" devices on their network, either by disconnecting them from the internet completely or partitioning them on separate Virtual Local Area Network (VLANs) or other subnetworks. Disconnecting a device from the internet was a common tactic for dealing with privacy and security concerns. As noted above, several participants described making their smart TV "dumb" because of concerns related to the quantity and variety of data these devices collect. To address these concerns, P24 noted he only

connected his TV to the internet for an occasional software update, while P9 said he gave his family very specific instructions for setting up smart TVs, saying, "You should set it up with a wired network connection, then you should unplug it when it is done being set up so that it does not understand that you have a network."

Numerous participants also mentioned isolating devices on separate network routers or subnets. Some, like P2, sought to simply keep internet-connected devices separate from their other devices: "For my Wi-Fi devices, I typically try to segregate them on my network." Others were motivated by concerns over whether the device manufacturer could be trusted with their data, with P15 noting, "I separate all my devices out via VLAN to keep things separate because I am ordering a lot of [devices] from not necessarily the most reputable companies that I don't have much way to trust what is going on." Similarly, P27 explained, "Amazon or some one-off devices where I've not heard of the brand before, I'm not so likely to allow [them] onto my major network at home."

Some participants also segregated particular devices onto different networks based on the sensitivity of the data being transmitted. For example, P5 indicated that "cameras and microphones are the most obvious things that…could reveal data that you want to keep private. So, yeah… I really do want to know about the data flow. That's why I looked into how HomeKit processes that on a local HomePod or an Apple TV, instead of sending it over the internet." P16 took similar steps to segregate video data, noting, "My house is pretty wired. I have three routers that control different aspects of the internet, but all of the home automation equipment is on one router and my camera is on another router."

Monitoring and controlling network traffic. Beyond managing how SHDs connect to a home network or the internet, participants also discussed protecting their privacy by monitoring and controlling network traffic to block data transfers to domains they do not trust or recognize. Home network routers that support HomeKit include software that provides users the ability to manage devices' Wi-Fi access, and some participants found these features useful. P1 noted it was "pretty easy to block that stuff [camera data] from the router from calling out and still keep it locally functional when you use something like HomeKit." P19 similarly found HomeKit-enabled routers helpful in this regard: "What it does offer is really, really important in the sense that it gives you a little control panel where it shows you all of your accessories, all of your hubs, everything. Each accessory has the option to let it communicate freely, let it communicate to only a specific subset of domains that are strictly relevant to its operation or only let it communicate locally."

Other participants used even more advanced traffic management techniques to provide a detailed level of monitoring and control of where their smart home data was flowing. For example, P25 began using traffic blocking software (Pi-hole) after noticing that his TV soundbar—which included a microphone and speaker—was making "3000 pings per day" to an "unnecessary" endpoint; he became concerned and "eventually went and just [denylisted] it from my router so that it can only talk within my network, but it can't reach out and talk to anybody outside." Similarly, P12 had a private DNS server in his home, allowing him to know when his "data is accessed" and "so we can see, basically in terms of advertising, we can block certain things. So like TikTok, things like that, we can block because we don't trust any of that." And P4 decided to isolate his smart TV after using a network sniffer (i.e., software for monitoring the flow of data packets over computer networks); he noted, "It was interesting to see the number of calls that were unrelated to the television that the device was making [which]...gave me ammunition to

then go ahead and start blocking those in various points on my network once it had done what it needed to do. That was very disturbing."

Related to the discussion of trust in Section 5.1.1, participants using advanced traffic management strategies often said these tools helped them be less dependent on promises made by a device company. P18 used a Pi-hole with "1.5 million domains" on his denylist, noting that while companies publish privacy policies and occasionally offer users "toggles to opt out of that data collection," the user is dependent on the company, "whereas me, I can look at my block query list and see that this data was actually blocked and not just it's in the writing on the app that says, we're not going to collect it." Importantly, these participants were able to see if devices were behaving in (un)expected ways. For example, P9 described how his home DNS relay helped him "see stuff" and manage his network traffic: "My garage door opener is making hundreds of calls an hour to trafficmanager.net. And it's like, okay, I didn't buy it from those guys. …I can turn that off and I can manage that."

6 DISCUSSION

Given the proliferation of IoT technology into one of the most private spaces—the home—privacy and security scholars have begun exploring both social and technical aspects of the privacy risks these technologies pose, as well as various approaches to mitigate those risks. In this study, we focus on the experiences of privacy-conscious power users to capture the most important risks they perceive from using SHDs in their homes and to understand how they manage those risks. Power users represent an important, but understudied, population of users; by speaking with privacy-conscious power users, we surface their approaches to using SHDs and highlight risks that might not be identified by talking to a general population. Because power users often spend significant time researching different approaches to optimize their devices, their experiences also showcase a wider range of strategies employed to manage risks. In addition, power users can help bridge the gap between developers' and users' understandings of privacy, since developers often think about privacy passively (e.g., when new APIs, policies, or laws are introduced) [57], while we found that power users actively sought out privacy-enhancing solutions.

The findings detailed above highlight that the technical landscape surrounding IoT—including what data is collected, what options are available for managing or restricting data flows, and who has access to data collected by smart home devices—is complex, complicated, and often confusing, even for knowledgeable users who spend significant time researching devices and integration options. This is a concerning finding, especially given that many people who use smart home devices have limited knowledge of or skills in managing devices and data [54,89,109]. Our findings also highlight the important—and often defining—role that trust plays in decision-making, and how tenuous user trust in companies can be. In the rest of this section, we expand on these findings and consider how various design decisions, both in terms of devices themselves and how information about them is communicated—may help in both surfacing potential risks and simplifying the process of managing devices and data flows.

6.1 Numerous Challenges to Managing Smart Home Device Data

A key—and perhaps surprising—takeaway from our findings is that even the power users in our study found it challenging to manage their privacy and sufficiently control data flows from their SHDs. Prior studies of IoT privacy-related behaviors have focused on non-power users, finding that while they express some concerns about data collection by SHDs [8,56], many users have a limited understanding of how the technology works [109,111] and fail to take protective actions

[89]. Even when they take actions, most non-power users stick to non-technical, device-level strategies, such as adjusting the location of devices or limiting engagement with them [54,89,109]. While our participants also performed device-level actions to mitigate privacy concerns, many described spending significant time researching devices and integration platforms to become better-informed about how their SHDs communicated and shared data.

Participants also noted that some of their strategies required technical skills and advanced network management to achieve meaningful results that protected their privacy—something they worried most people wouldn't be willing or able to do. As P6 noted, it is unlikely "average" users would take similar steps when selecting and installing SHDs in their own homes. People who receive a smart speaker as a gift or just want the cheapest smart doorbell to track package delivery might not fully understand the privacy risks inherent in such devices, know what questions to consider when deciding to use them, or possess the skills to take meaningful action.

If power users, who are taking extra time to research devices and make informed decisions, still feel like they need to make tradeoffs when using SHDs, this has troubling implications for those who may not have the time, knowledge, or desire to become as informed or technically proficient. And if even a non-power user could duplicate the extraordinary steps of the power users in our study, our participants noted this very well might not be sufficient. To repeat P25's concern noted above, "you don't know exactly what they're getting access to, so when you give any company access to your information, it's always kind of scary what exactly they're grabbing."

This point leads us to three additional insights provoked by our findings: the continued importance of *trust* in SHD companies, the need to *reduce uncertainty* about data flows, and the need for *tools to easily manage* one's smart home. Below, we discuss each and provide recommendations for moving forward.

6.2 Trust in Smart Home Device Companies

Our first research question explored the concerns smart home power users have regarding their SHDs and the data they generate. We found that even with these users' advanced research, knowledge, and technical skills, their comfort with SHDs still depended heavily on trust in the companies who manufacture and support the devices. Many participants were openly hostile to companies like Amazon due to concerns about what the company might do with their data. As a result, and despite the increased cost and decreased interoperability, most of our participants were HomeKit users because they trusted Apple and its commitment to data privacy and security.

However, this trust was not absolute. At the time of data collection (August 2021), Apple had recently announced its plans to scan iPhone users' photos (through iCloud) to identify potential cases of child sexual abuse [10]. While this move was applauded by many, it also raised concerns among privacy and security researchers regarding potential misuse [60]. A few participants commented about this news in reference to their perception of Apple. For example, P29 said, "They've made some privacy decisions that I'm not a fan of. I don't know what I'll do if I lose faith in that company." P12 described the policy as well-intentioned, but said it also raised concerns for him: "By announcing they have this software, I feel like it could open a lot of doors that we don't really want opened. Especially as we're a HomeKit house, that's a big concern."

These comments are in line with Martin's [66] finding that violations of privacy expectations, specifically secondary data use, reduce trust in web-based applications. She found that selling data to a data broker (third-party aggregator) or using data to retarget advertisements based on social connections are viewed as major violations of data privacy expectations. Our study reiterated these concerns when participants discussed smart TVs and voice data being sold for ad targeting.

Concerns over targeted advertising was a key driver in our participants' trust in Apple over Amazon and Google. P29 explained, "It's a bit of a 'pick the lesser of two evils', which is why the listening devices that I do have are Apple. Simply because of the three major home systems, they're the only one that's not in the business of advertising." Yet, Apple's increasing focus on advertising [87] raised questions regarding how changes in business models impact user trust in a company's data practices.

Our findings contribute to a growing recognition that trust plays a critical role in SHD adoption [44,106]. Our participants' focus on trust—and their distrust of certain device providers—aligns with Lau et al.'s [54] findings that trust must be "actually warranted" (p. 18). Moreover, this trust can be precarious. Recall P10's remark that "at some point, you have to trust and say, hopefully the system is designed the way they say it is." This dilemma led our participants to engage in numerous strategies to mitigate privacy risks—as basic as relocating devices and as advanced as installing custom network software to block certain data transfers—even when they generally trusted their SHD ecosystem. Thus, while prior work has found that users tend to trust that their SHDs include adequate privacy protections and will not misuse their data [89,111], the power users in our study recognized that such trust needs to be supplemented by additional strategies to monitor and manage data collection and use.

A key motivation for our participants to take such extraordinary steps was a lack of clarity about exactly what data SHDs were collecting and where it was flowing, with a specific emphasis on monitoring and controlling traffic used for advertising. As we discuss next, reducing this uncertainty is a key opportunity for SHD manufacturers to retain consumer trust.

6.3 Reduce Uncertainty about Data Flows

Technological change often spawns consumer uncertainty that prevents adoption [39], a reality that is only accentuated by the astonishing pace of the evolution of digital technologies. Within the smart home ecosystem, uncertainties emerge about how devices monitor and collect data, what that data is used for, and who might have access to it [89]. While some smart home platforms, such as Apple's HomeKit, have worked to build consumer trust that their "walled-garden" approach will protect users' privacy, our findings suggest that even the most engaged users have significant uncertainty about data flows. In fact, the power users we studied felt compelled to take extraordinary steps to manage data flows within their smart homes because device companies do not provide sufficient transparency in their data practices. Furthermore, if the power users in our study remained uncertain despite the embrace (by most) of the HomeKit ecosystem, then non-power users will experience even greater uncertainty, or worse, assume their data is sufficiently protected. For example, P32, a participant not as technically proficient as some in our study, worried about what he might be missing when using SHDs, saying, "for somebody like me who's not a security professional, it's hard to understand and determine…what data is Google and Apple and all that other stuff collecting on us."

Numerous participants noted this uncertainty could be reduced for *all* users through the widespread adoption of privacy nutrition labels [27,49,58]. Building on prior academic research, Apple unveiled these labels for all App Store apps in late 2020 to provide consumers a standardized and easy-to-understand glimpse into how apps collect, use, and share data [71]. P10, for example, praised Apple for this innovation in standardizing language about data collection and wanted to see it applied to SHDs, "distilling it down to something that's easily digestible and easy to compare one app to another in the same way for smart home devices," while P13 suggested that "having something like that [nutrition label] stamped onto the back of a device that you're considering

would be just wonderful." Research has shown that a standardized approach to communicating privacy practices and implications can have significant positive effects on the understandability of privacy policies, and prompt users to read them and make informed decisions [26,49].

While we agree that privacy nutrition labels can help reduce uncertainty about the data practices promised by smart home device manufacturers, they still require users to trust the claims made. To account for this, many of our participants took a "trust but verify" approach to monitor and manage data flows directly. These advanced strategies, which we have not seen in this frequency or complexity in prior studies of smart home data management, included technical modifications to device firmware, customized network configurations, and software to monitor and control internet traffic—tactics not all users can perform. There is an emergent need to give non-power users simpler means of reducing the uncertainty of data flows through monitoring tools. Work by Huang et al. [40] on IoT Inspector, an open-source desktop app that provides real-time visualizations of data traffic from all SHDs on one's home network, is an important example of new initiatives focused on increasing users' awareness around data flows. Importantly, visualizations have been shown to be particularly useful in reducing uncertainty about data privacy in smart home environments [12].

6.4 Looking Ahead: Developing Tools to Easily Manage Smart Homes

Tools like IoT Inspector [40] are designed to provide users with helpful insights about network traffic within their smart home environment—and to do so without the need for the technical proficiency possessed by many of our participants. This will become increasingly important over the next decade as SHDs become more commonplace and homes truly become "smart" through complex integrations of multiple devices and sensors. Our data, which details the practices of power users who are already building out complex ecosystems of SHDs, highlights the need for further development of user-friendly tools to view and manage data flows within smart homes.

When it comes to integrating multiple devices through a single platform, our participants preferred the privacy tools and settings provided by Apple's HomeKit, including its exclusivity or walled-garden approach and the ability to keep data local. However, Apple's limited interoperability means there are fewer devices with the "Works with HomeKit" label on the market; paired with the higher costs of some of these devices, non-power users might seek cheaper options and/or those with increased functionality—and fewer embedded privacy and security features. Beyond that, integrating these devices with HomeKit is possible via HomeBridge or Home Assistant, but requires some level of technical knowledge and skills to integrate into Apple's privacy-protecting ecosystem.

When discussing the challenge of interoperability, several participants mentioned Matter, a common language that smart home devices can use to communicate regardless of the device manufacture. The standard is overseen by the Connectivity Standard Alliance (CSA) and version 1.0 was released in Fall 2022, a year after our data was collected [22]. Matter devices use an internet protocol that allows them to communicate directly to the internet without a hub and work with short-range network protocols, meaning that users can still use devices on local networks without cloud access (similar to most HomeKit users in our study). Matter may make it easier for smart home users to deploy the mitigation strategies outlined in Section 5.2.2, but privacy experts worry that without proper understanding of network management, users may unknowingly transmit *more* data to the cloud [97]. This is especially true for Apple HomeKit users who rely on HomeKit's default, local-only settings. These developments also highlight why it will be critical for smart home users to have a thorough understanding of when and why a device may be pinging the cloud and how to isolate sensitive devices.

When looking at the various strategies our participants employed to mitigate privacy risks, few people mentioned using native privacy settings to manage their devices. This mirrors findings from Lau et al. [54], who found that smart speaker privacy controls are rarely used, due largely to their design being misaligned with (non-power) users' needs. In our study, our more advanced users instead engaged in complex and diverse approaches to achieve their goals, but it is unlikely that non-power users would consider many of those options, let alone take the time to learn how to apply those strategies. This lack of engagement with privacy settings is not new; in fact, numerous studies have highlighted the importance of default settings. For example, Zimmer et al. [113] found that Fitbit users rarely—if ever—looked at the privacy settings once they set up their device, while other scholars have noted that most social media users have posted content that did not align with their privacy goals [47,61,101]. Even highly engaged users might not engage with privacy settings if they feel overly complex [98], and owners of SHDs have been shown to effectively forget their presence [106], which makes engaging with privacy settings less likely.

While our power users took extraordinary steps to monitor and manage traffic from their SHDs, non-power users currently have few options to visualize or manage data privacy beyond the basic apps and dashboards that might be available from a device manufacturer and the limited privacy settings presented when a device is initially set up. Our participants recognized the need for simpler tools and visualizations so all users could gain similar levels of control over their data. Thus, additional opportunities exist for device manufacturers to increase the visibility of data flows, provide notifications when unexpected data flows might occur, and provide users greater access and control over the data generated and shared across their smart home network. Researchers have explored numerous ways to improve smart home design [11,19,34,45,108] and have explored optimal user interfaces for visualizing IoT dataflows and control centers [40,83]; however, these efforts face challenges due to limited details within network traffic data. And while some researchers have used machine learning classifiers to better understand why devices ping a particular destination [3,73,95,110], our participants expressed the desire to not only better understand data flows, but also the need for tools to help them keep their data local. In light of this, we argue that designers and regulators need to consider factors that go beyond the information and controls currently available.

We also note that the sheer quantity and diversity of data collected by SHDs—and their tremendous popularity in the home—requires additional research to identify best practices and policy proposals for helping consumers understand what data is being collected and used by their smart home devices, and to help them make more informed decisions about whether and how to use these devices. The HCI/social computing community is uniquely positioned to ensure usable privacy options are embedded in the design of IoT technologies [105]. Early work highlighted the need for providing home automation users with simple privacy and security features that they can confidently configure [14], while more recently, a study with employees at a smart home company found that user experience is rarely considered in security design [17]. This is troubling, as poor design will likely translate into less use of security features. Given these findings and recent discussions at CSCW on challenges with data collection and management in smart homes (e.g., [5,54,100,108,111]), we call for a renewed focus on building smart home interfaces that are transparent, easy to use, and aligned with users' privacy needs.

7 LIMITATIONS

We note several limitations in our study. Participants were recruited largely through popular online discussion forums on Reddit and Facebook. While this allowed us to recruit power users, biases persist in the socio-demographic makeup of those who are active in such online spaces. Our

participants also tended to be the primary decision-makers who managed the SHDs in their homes, yet other household members and bystanders might have different perspectives and strategies that were not included in our study. While some researchers have begun considering the unique needs and experiences of non-primary users (e.g., [108]), more research is needed with this population.

Beyond that, these findings are limited because we purposefully recruited participants who were concerned about and/or engaged in various strategies to manage their data privacy. People who do not identify as privacy-conscious or power users likely have different priorities in making decisions about smart home devices. As we note in the discussion, they also may have limited skills to effectively mitigate privacy risks [109,111]. Future work should investigate privacy-protecting strategies of a more diverse set of owners and secondary users of SHDs, including a focus on how privacy needs might be negotiated among different stakeholders in diverse smart environments.

8 CONCLUSION

As smart home technologies have proliferated, companies have focused mainly on usability and smooth integration within ecosystems. Smart home devices have proven to be immensely popular and useful, but along with their popularity comes a tendency for them to fade into the background; users grow so accustomed to voice-enabled commands, always-on cameras, and automations that they neglect to manage device settings or monitor data flows after initial set up.

Drawing on data from 10 focus groups with 32 privacy-conscious smart home power users, we describe the key privacy risks they identify, as well as how they mitigate those risks with increasingly complex strategies that have not been identified in studies with non-power users. Power users think about and use these devices in creative and advanced ways, giving insights into a future where smart home technology is more fully integrated into living spaces.

As with all technology, of course, things evolve quickly. At the time of data collection, the smart home industry had recently announced Matter, a short-range connectivity standard that will provide seamless interoperability across devices from Amazon, Google, Apple, and dozens of other providers [96]; the initial version of Matter launched in fall 2022 and the first Matter-certified devices were released by the end of the year [97]. Unified connectivity standards like Matter hold promise to make SHDs easier to install and keep secure; that said, privacy concerns remain [107]. Even after Matter is fully deployed and more devices benefit from short-range connectivity, we will still be confronted by the question of whether P29's desire—that "you shouldn't need to share your data"—is attainable in our increasingly data-driven world.

Finally, this study highlights how complex and challenging managing data flows is becoming as more and more objects include sensors to collect and share sensitive data. The power users in our study resorted to extraordinary measures to address the tensions between the benefits of SHDs and data privacy; their insights will help focus future research and design to ensure usable privacy features are embedded in future smart home standards and technologies.

ACKNOWLEDGMENTS

We offer deep thanks to our focus group participants for their time and thoughts on their experiences with the smart home landscape. We also thank our anonymous reviewers, as well as Pooja Upadhyay and Amanda Lazar, who provided feedback on the original manuscript.

REFERENCES

[1] Jacob Abbott, Jayati Dev, Donginn Kim, Shakthidhar Gopavaram, Meera Iyer, Shivani Sadam, Shrirang Mare, Tatiana Ringenberg, Vafa Andalibi, and L. Jean Camp. 2022. Privacy Lessons Learnt from Deploying an IoT Ecosystem in the Home. In *Proceedings of the 2022 European Symposium on Usable Security* (EuroUSEC '22), Association for Computing Machinery, New York, NY, USA, 98–110. DOI:https://doi.org/10.1145/3549015.3554205

[2] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. Privacy Norms for Smart Home Personal Assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ACM, Yokohama Japan, 1–14. DOI:https://doi.org/10.1145/3411764.3445122

[3] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. 2020. Peek-a-boo: i see your smart home activities, even encrypted! In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (WiSec '20), Association for Computing Machinery, New York, NY, USA, 207–218. DOI:https://doi.org/10.1145/3395351.3399421

[4] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (January 2005), 26–33. DOI:https://doi.org/10.1109/MSP.2005.22

[5] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2 (October 2020), 1–28. DOI:https://doi.org/10.1145/3415187

[6] Iftikhar Alam, Shah Khusro, and Mumtaz Khan. 2019. Usability Barriers in Smart TV User Interfaces: A Review and Recommendations. In *2019 International Conference on Frontiers of Information Technology (FIT)*, 334–3344. DOI:https://doi.org/10.1109/FIT47737.2019.00069

[7] Arun Ananthanarayanan, T. Sivasai, Dinesh D Gowda, Ganya H T, and K S Shreyas. 2021. Smart Mirror Using Rasberry Pi for Human Monitoring and Intrusion Detection. In *2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C)*, 207–210. DOI:https://doi.org/10.1109/ICDI3C53598.2021.00049

[8] 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 (July 2018), 1–23. DOI:https://doi.org/10.1145/3214262

[9] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the Age of Mobility and Smart Devices in Smart Homes. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 819–826. DOI:https://doi.org/10.1109/SocialCom-PASSAT.2012.108

[10] Frank Bajak and Barbara Ortutay. 2021. Apple to scan U.S. iPhones for images of child sexual abuse. *AP NEWS*. Retrieved July 4, 2022 from https://apnews.com/article/technology-business-child-abuse-apple-inc-7fe2a09427d663cda8addfeeffc40196

[11] Nata Barbosa, Zhouhao Zhang, and Yang Wang. 2020. Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. *Usenix The Advanced Computing Systems Association* August 10–11, 2020 (August 2020). Retrieved January 11, 2023 from https://www.usenix.org/conference/soups2020/presentation/barbosa

[12] Carlos Bermejo Fernandez, Petteri Nurmi, and Pan Hui. 2021. Seeing is Believing?: Effects of Visualization on Smart Device Privacy Perceptions. In *Proceedings of the 29th ACM International Conference on Multimedia*, ACM, Virtual Event China, 4183–4192. DOI:https://doi.org/10.1145/3474085.3475552

[13] Melanie Birks, Ysanne Chapman, and Karen Francis. 2008. Memoing in qualitative research: Probing data and processes. *Journal of Research in Nursing* 13, 1 (January 2008), 68–75. DOI:https://doi.org/10.1177/1744987107081254

[14] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Vancouver BC Canada, 2115–2124. DOI:https://doi.org/10.1145/1978942.1979249

[15] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2018. Smart Connected Homes. In *Internet of Things A to Z*, Qusay Hassan (ed.). John Wiley & Sons, Inc., Hoboken, NJ, USA, 359–384. DOI:https://doi.org/10.1002/9781119456735.ch13

[16] Albert Fox Cahn and Justin Sherman. 2021. Your "smart home" is watching – and possibly sharing your data with the police. *The Guardian*. Retrieved July 4, 2022 from https://www.theguardian.com/commentisfree/2021/apr/05/tech-police-surveillance-smart-home-devices

[17] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–9. DOI:https://doi.org/10.1145/3334480.3382850

[18] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ACM, Yokohama Japan, 1–16. DOI:https://doi.org/10.1145/3411764.3445691

[19] Chola Chhetri and Vivian Genaro Motti. 2022. User-Centric Privacy Controls for Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (November 2022), 349:1-349:36. DOI:https://doi.org/10.1145/3555769

[20] Eugene Cho, S. Shyam Sundar, Saeed Abdullah, and Nasim Motalebi. 2020. Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–13. Retrieved July 6, 2022 from http://doi.org/10.1145/3313831.3376551

[21] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a glass house: a survey of private moments in the home. In *Proceedings of the 13th international conference on Ubiquitous computing - UbiComp '11*, ACM Press, Beijing, China, 41. DOI:https://doi.org/10.1145/2030112.2030118

[22] Connectivity Standards Alliance. 2022. Matter Arrives Bringing A More Interoperable, Simple And Secure Internet Of Things to Life. *CSA-IOT*. Retrieved January 14, 2023 from https://csa-iot.org/newsroom/matter-arrives/

[23] Salim Jibrin Danbatta and Asaf Varol. 2019. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. DOI:https://doi.org/10.1109/ISDFS.2019.8757472

[24] Roy Dong, Lillian J. Ratliff, Alvaro A. Cárdenas, Henrik Ohlsson, and S. Shankar Sastry. 2018. Quantifying the Utility--Privacy Tradeoff in the Internet of Things. *ACM Trans. Cyber-Phys. Syst.* 2, 2 (June 2018), 1–28. DOI:https://doi.org/10.1145/3185511

[25] Julia C. Dunbar, Emily Bascom, Ashley Boone, and Alexis Hiniker. 2021. Is Someone Listening?: Audio-Related Privacy Perceptions and Design Recommendations from Guardians, Pragmatists, and Cynics. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 3 (September 2021), 1–23. DOI:https://doi.org/10.1145/3478091

[26] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* (2017), 399--412.

[27] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2022. An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy* 20, 2 (March 2022), 31–39. DOI:https://doi.org/10.1109/MSEC.2021.3132398

[28] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. 2017. Security and privacy issues for an IoT based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1292–1297. DOI:https://doi.org/10.23919/MIPRO.2017.7973622

[29] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. 2017. Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In *Human Aspects of Information Security, Privacy and Trust*, Theo Tryfonas (ed.). Springer International Publishing, Cham, 656–674. DOI:https://doi.org/10.1007/978-3-319-58460-7_45

[30] Dan Goodin. 2021. Amazon devices will soon automatically share your Internet with neighbors. *Ars Technica*. Retrieved July 4, 2022 from https://arstechnica.com/gadgets/2021/05/amazon-devices-will-soon-automatically-share-your-internet-with-neighbors/

[31] Kirsten Gram-Hanssen and Sarah J. Darby. 2018. "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science* 37, (March 2018), 94–101. DOI:https://doi.org/10.1016/j.erss.2017.09.037

[32] Andy Greenberg. 2015. Apple's Latest Selling Point: How Little It Knows About You. *Wired*. Retrieved July 4, 2022 from https://www.wired.com/2015/06/apples-latest-selling-point-little-knows/

[33] Aznor Hanah, Rohani Farook, Shamsul Jamel Elias, M R A Rejab, M Fairuz M Fadzil, and Zulkifli Husin. 2019. IoT Room Control And Monitoring System Using Rasberry Pi. In *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*, 1–4. DOI:https://doi.org/10.1109/ICRAIE47735.2019.9037759

[34] Julie M. Haney, Susanne M. Furman, and Yasemin Acar. 2020. Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. *NIST* (July 2020). Retrieved January 11, 2023 from https://www.nist.gov/publications/smart-home-security-and-privacy-mitigations-consumer-perceptions-practices-and

[35] Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer. 2020. Americans' willingness to adopt a covid-19 tracking app. *First Monday* 25, 11 (October 2020), online. DOI:https://doi.org/10.5210/fm.v25i11.11095

[36] Shane Harris. 2015. Your Samsung SmartTV Is Spying on You, Basically. *The Daily Beast*. Retrieved July 4, 2022 from https://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically

[37] Alan Henry and Emily Long. 2019. How to Tap Your Network and See Everything That Happens On It. *Lifehacker*. Retrieved July 6, 2022 from https://lifehacker.com/how-to-tap-your-network-and-see-everything-that-happens-1649292940

[38] Aaron Holmes. 2019. Google exec says Nest owners should probably warn their guests that their conversations are being recorded. *Business Insider*. Retrieved July 4, 2022 from https://www.businessinsider.com/google-exec-nest-owners-should-tell-guests-theyre-being-recorded-2019-10

[39] Chun-Lung Huang and Peter Haried. 2020. An Evaluation of Uncertainty and Anticipatory Anxiety Impacts on Technology Use. *International Journal of Human–Computer Interaction* 36, 7 (April 2020), 641–649. DOI:https://doi.org/10.1080/10447318.2019.1672410

[40] 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 Interact. Mob. Wearable Ubiquitous Technol.* 4, 2 (June 2020), 1–21. DOI:https://doi.org/10.1145/3397333

[41] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–13. DOI:https://doi.org/10.1145/3313831.3376529

[42] Haris Isyanto, Ajib Setyo Arifin, and Muhammad Suryanegara. 2020. Performance of Smart Personal Assistant Applications Based on Speech Recognition Technology using IoT-based Voice Commands. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 640–645. DOI:https://doi.org/10.1109/ICTC49870.2020.9289160

[43] Andreas Jacobsson and Paul Davidsson. 2015. Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 727–732. DOI:https://doi.org/10.1109/WF-IoT.2015.7389144

[44] Esther D. T. Jaspers and Erika Pearson. 2022. Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research* 142, (March 2022), 255–265. DOI:https://doi.org/10.1016/j.jbusres.2021.12.043

[45] 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*, ACM, New Orleans LA USA, 1–19. DOI:https://doi.org/10.1145/3491102.3517602

[46] Yong Jin, Masahiko Tomoishi, and Nariyoshi Yamai. 2017. A Secure and Lightweight IoT Device Remote Monitoring and Control Mechanism Using DNS. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 282–283. DOI:https://doi.org/10.1109/COMPSAC.2017.33

[47] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. 2012. Facebook and privacy: it's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (SOUPS '12), Association for Computing Machinery, New York, NY, USA, 1–15. DOI:https://doi.org/10.1145/2335356.2335369

[48] Hyunjin Kang and Wonsun Shin. 2016. Do Smartphone Power Users Protect Mobile Privacy Better than Nonpower Users? Exploring Power Usage as a Factor in Mobile Privacy Protection and Disclosure. *Cyberpsychology, Behavior, and Social Networking* 19, 3 (March 2016), 179–185. DOI:https://doi.org/10.1089/cyber.2015.0340

[49] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, ACM Press, Mountain View, California, 1. DOI:https://doi.org/10.1145/1572532.1572538

[50] Kanitkorn Khanchuea and Rawat Siripokarpirom. 2019. A Multi-Protocol IoT Gateway and WiFi/BLE Sensor Nodes for Smart Home and Building Automation: Design and Implementation. In *2019 10th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES)*, 1–6. DOI:https://doi.org/10.1109/ICTEmSys.2019.8695968

[51] Richard A. Krueger and Mary Anne Casey. 2014. *Focus Groups: A Practical Guide for Applied Research* (5th edition ed.). SAGE Publications, Inc, Los Angeles London New Delhi Singapore Washington DC.

[52] Albrecht Kurze, Andreas Bischof, Sören Totzauer, Michael Storz, Maximilian Eibl, Margot Brereton, and Arne Berger. 2020. Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–12. DOI:https://doi.org/10.1145/3313831.3376273

[53] Hyosun Kwon, Joel E. Fischer, Martin Flintham, and James Colley. 2018. The Connected Shower: Studying Intimate Data in Everyday Life. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4 (December 2018), 1–22. DOI:https://doi.org/10.1145/3287054

[54] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (November 2018), 1–31. DOI:https://doi.org/10.1145/3274371

[55] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03 extended abstracts on Human factors in computing systems - CHI '03*, ACM Press, Ft. Lauderdale, Florida, USA, 724. DOI:https://doi.org/10.1145/765891.765952

[56] Hosub Lee and Alfred Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 407–412. DOI:https://doi.org/10.1109/WF-IoT.2016.7845392

[57] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW3 (January 2021), 1–28. DOI:https://doi.org/10.1145/3432919

[58] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (CHI '22), Association for Computing Machinery, New York, NY, USA, 1–24. DOI:https://doi.org/10.1145/3491102.3502012

[59] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2019. Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. In *Information in Contemporary Society* (Lecture Notes in Computer Science), Springer International Publishing, Cham, 102–113. DOI:https://doi.org/10.1007/978-3-030-15742-5_9

[60] Michael Liedtke and Matt O'Brien. 2021. Apple delays iPhone photo-scanning plan amid fierce backlash. *AP NEWS*. Retrieved July 4, 2022 from https://apnews.com/article/technology-business-d796d5ca2ca5932790ad806b9c119d71

[61] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 340–345. DOI:https://doi.org/10.1109/PerComW.2012.6197507

[62] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?": Privacy Expectations about Smart TVs in the U.S. In *Proceedings 3rd European Workshop on Usable Security*, Internet Society, London, England. DOI:https://doi.org/10.14722/eurousec.2018.23016

[63] Shelley Mallett. 2004. Understanding Home: A Critical Review of the Literature. *The Sociological Review* 52, 1 (February 2004), 62–89. DOI:https://doi.org/10.1111/j.1467-954X.2004.00442.x

[64] S. Marathe, S. Sundar, M. Bijvank, H. C. V. Vugt, and J. Veldhuis. 2007. Who are these power users anyway? Building a psychological profile. San Francisco, CA. Retrieved July 6, 2022 from https://www.semanticscholar.org/paper/Who-are-these-power-users-anyway-Building-a-profile-Marathe-Sundar/1455563bf9242612c36f08e5a295aa139b8a1f04

[65] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (HotMobile '19), Association for Computing Machinery, New York, NY, USA, 117–122. DOI:https://doi.org/10.1145/3301293.3302371

[66] Kirsten Martin. 2018. The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research* 82, (January 2018), 103–116. DOI:https://doi.org/10.1016/j.jbusres.2017.08.034

[67] Friedemann Mattern and Christian Floerkemeier. 2010. From the Internet of Computers to the Internet of Things. In *From Active Data Management to Event-Based Systems and More: Papers in Honor of Alejandro Buchmann on the Occasion of His 60th Birthday*, Kai Sachs, Ilia Petrov and Pablo Guerrero (eds.). Springer, Berlin, Heidelberg, 242–259. DOI:https://doi.org/10.1007/978-3-642-17226-7_15

[68] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The Contextual Complexity of Privacy in Smart Homes and Smart Buildings. In *HCI in Business, Government, and Organizations: Information Systems*, Fiona Fui-Hoon Nah and Chuan-Hoo Tan (eds.). Springer International Publishing, Cham, 67–78. DOI:https://doi.org/10.1007/978-3-319-39399-5_7

[69] Matthew B. Miles, A. Michael Huberman, and Johnny Saldana. 2018. *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications.

[70] Moses Namara, Reza Ghaiumy Anaraky, Pamela Wisniewski, Xinru Page, and Bart P. Knijnenburg. 2021. Examining Power Use and the Privacy Paradox between Intention vs. Actual Use of Mobile Applications. In *European Symposium on Usable Security 2021*. Association for Computing Machinery, New York, NY, USA, 223–235. Retrieved July 11, 2022 from http://doi.org/10.1145/3481357.3481513

[71] Lily Hay Newman. 2020. Apple's App "Privacy Labels" Are Here—and They're a Big Step Forward. *WIred*. Retrieved July 4, 2022 from https://www.wired.com/story/apple-app-privacy-labels/

[72] NPR and Edison Research. 2022. Smart Speaker Ownership Reaches 35% of Americans. *NPR*. Retrieved July 6, 2022 from https://www.npr.org/about-npr/1105579648/npr-edison-research-smart-speaker-ownership-reaches-35-of-americans

[73] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. 2019. HomeSnitch: behavior transparency and control for smart home IoT devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (WiSec '19), Association for Computing Machinery, New York, NY, USA, 128–138. DOI:https://doi.org/10.1145/3317549.3323409

[74] Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. Long-term effects of ubiquitous surveillance in the home. In

Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12, ACM Press, Pittsburgh, Pennsylvania, 41. DOI:https://doi.org/10.1145/2370216.2370224

[75] Sunyup Park, Anna Lenhart, Michael Zimmer, and Jessica Vitak. 2023. "Nobody's Happy": Design Insights from Privacy-Conscious Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, USENIX Association, Anaheim, CA, 543–558. Retrieved from https://www.usenix.org/conference/soups2023/presentation/park

[76] Michael Quinn Patton. 2005. Qualitative research. In *Encyclopedia of Statistics in Behavioral Science*. John Wiley & Sons, Ltd, Hoboken, NJ. DOI:https://doi.org/10.1002/0470013192.bsa514

[77] James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, Glasgow Scotland Uk, 1–14. DOI:https://doi.org/10.1145/3290605.3300275

[78] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *Designing Interactive Systems Conference*, ACM, Virtual Event Australia, 26–40. DOI:https://doi.org/10.1145/3532106.3535195

[79] Michael Potuck. 2022. Report: Amazon and third parties use Alexa voice data for ads while Siri respects privacy. *9to5Mac*. Retrieved July 4, 2022 from https://9to5mac.com/2022/04/29/amazon-alexa-voice-data-used-for-ads/

[80] 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)*, 261–270. DOI:https://doi.org/10.1109/REW.2016.050

[81] Johnny Saldana. 2021. *The Coding Manual for Qualitative Researchers* (Fourth edition ed.). SAGE Publications Ltd, Los Angeles London New Delhi Singapore Washington DC Melbourne.

[82] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Qual Quant* 52, 4 (July 2018), 1893–1907. DOI:https://doi.org/10.1007/s11135-017-0574-8

[83] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–14. DOI:https://doi.org/10.1145/3313831.3376264

[84] Tyler Sonnemaker. 2021. Texas power companies automatically raised the temperature of customers' smart thermostats in the middle of a heat wave. *Business Insider*. Retrieved July 4, 2022 from https://www.businessinsider.com/texas-energy-companies-remotely-raised-smart-thermostats-temperatures-2021-6

[85] Nick Statt. 2020. Apple updates Safari's anti-tracking tech with full third-party cookie blocking. *The Verge*. Retrieved July 4, 2022 from https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking

[86] David W. Stewart and Prem Shamdasani. 2017. Online Focus Groups. *Journal of Advertising* 46, 1 (January 2017), 48–60. DOI:https://doi.org/10.1080/00913367.2016.1252288

[87] Chris Stokel-Walker. 2022. Apple Is an Ad Company Now. *Wired*. Retrieved January 13, 2023 from https://www.wired.com/story/apple-is-an-ad-company-now/

[88] Roger A. Straus. 2019. *Mastering focus groups and depth interviews: a practitioner's guide*. Paramount Market Publishing, Rochester, NY.

[89] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. 2019. "I don't own the data": end user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (SOUPS'19), USENIX Association, USA, 435–450.

[90] Neilly Tan, Richmond Wong, Audrey Desjardins, Sean Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *CHI*

Conference on Human Factors in Computing Systems, ACM, New Orleans LA USA, 1–25. DOI:https://doi.org/10.1145/3491102.3517617

[91] J Tassone, PZ Yan, M Simpson, C Mendhe, V Mago, and S Choudhury. 2020. Utilizing deep learning and graph mining to identify drug use on Twitter data. *BMC MEDICAL INFORMATICS AND DECISION MAKING* 20, (December 2020). DOI:https://doi.org/10.1186/s12911-020-01335-3

[92] Tech-FAQ. 2019. Flashing Firmware. *Tech-FAQ*. Retrieved July 6, 2022 from https://www.tech-faq.com/flashing-firmware.html

[93] Cadie Thompson. 2015. Apple is running into some problems with its big smart home plans. *Business Insider*. Retrieved July 6, 2022 from https://www.businessinsider.com/why-there-arent-many-apple-homekit-devices-available-2015-7

[94] Bergur Thormundsson. 2022. *Smart home: Statistics and facts*. Statista. Retrieved July 4, 2022 from https://www.statista.com/topics/2430/smart-homes/

[95] Rahmadi Trimananda, Janus Varmarken, Athina Markopoulou, and Brian Demsky. 2020. PingPong: Packet-Level Signatures for Smart Home Device Events. DOI:https://doi.org/10.48550/arXiv.1907.11797

[96] Jennifer Pattison Tuohy. 2022. Matter has been delayed, again. *The Verge*. Retrieved July 12, 2022 from https://www.theverge.com/2022/3/17/22982166/matter-smart-home-standard-postponed-fall-2022

[97] Jennifer Pattison Tuohy. 2022. Matter is here to save the smart home. *The Verge*. Retrieved January 14, 2023 from https://www.theverge.com/22787729/matter-smart-home-standard-apple-amazon-google

[98] Jessica Vitak, Stacy Blasiola, Sameer Patil, and Eden Litt. 2015. Balancing Audience and Privacy Tensions on Social Network Sites: Strategies of Highly Engaged Users. *International Journal of Communication* 9, 0 (May 2015), 20.

[99] Jessica Vitak, Priya Kumar, Yuting Liao, and Michael Zimmer. 2023. Boundary Regulation Processes and Privacy Concerns With (Non-)Use of Voice-Based Assistants. *HMC* 6, (July 2023), 183–201. DOI:https://doi.org/10.30658/hmc.6.10

[100] Jessica Vitak, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. 2021. Designing for Data Awareness: Addressing Privacy and Security Concerns About "Smart" Technologies. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing* (CSCW '21), Association for Computing Machinery, New York, NY, USA, 364–367. DOI:https://doi.org/10.1145/3462204.3481724

[101] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. "I regretted the minute I pressed share": a qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (SOUPS '11), Association for Computing Machinery, New York, NY, USA, 1–16. DOI:https://doi.org/10.1145/2078827.2078841

[102] Bruce D. Weinberg, George R. Milne, Yana G. Andonova, and Fatima M. Hajjat. 2015. Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58, 6 (November 2015), 615–624. DOI:https://doi.org/10.1016/j.bushor.2015.06.005

[103] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. 2017. Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 181–18109. DOI:https://doi.org/10.1109/PST.2017.00029

[104] Owen Williams. 2022. The average person doesn't have a chance with the smart home. *TechCrunch*. Retrieved December 29, 2022 from https://techcrunch.com/2022/02/18/the-average-person-doesnt-have-a-chance-with-the-smart-home/

[105] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, Glasgow Scotland Uk, 1–17. DOI:https://doi.org/10.1145/3290605.3300492

[106] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust Me: Doubts and Concerns Living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (DIS '16), Association for Computing Machinery, New York, NY, USA, 427–434. DOI:https://doi.org/10.1145/2901790.2901890

[107] Daniel Wroclawski. 2022. Matter Smart Home Standard FAQ. *Consumer Reports*. Retrieved July 12, 2022 from https://www.consumerreports.org/smart-home/matter-smart-home-standard-faq-a9475777045/

[108] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW (November 2019), 1–24. DOI:https://doi.org/10.1145/3359161

[109] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (SOUPS '17), USENIX Association, USA, 65–80.

[110] Wei Zhang, Yan Meng, Yugeng Liu, Xiaokuan Zhang, Yinqian Zhang, and Haojin Zhu. 2018. HoMonit: Monitoring Smart Home Apps from Encrypted Traffic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (CCS '18), Association for Computing Machinery, New York, NY, USA, 1074–1088. DOI:https://doi.org/10.1145/3243734.3243820

[111] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (November 2018), 1–20. DOI:https://doi.org/10.1145/3274469

[112] Bu Zhong. 2013. From smartphones to iPad: Power users' disposition toward mobile media devices. *Computers in Human Behavior* 29, 4 (July 2013), 1742–1748. DOI:https://doi.org/10.1016/j.chb.2013.02.016

[113] Michael Zimmer, Priya Kumar, Jessica Vitak, Yuting Liao, and Katie Chamberlain Kritikos. 2020. 'There's nothing really they can do with this information': unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society* 23, 7 (June 2020), 1020–1037. DOI:https://doi.org/10.1080/1369118X.2018.1543442

Received July 2022, revised January 2023, accepted March 2023.