Privacy Lessons Learnt from Deploying an IoT Ecosystem in the Home

Jacob Abbott
Indiana University
Bloomington, Indiana, USA
jaeabbot@indiana.edu

Jayati Dev
Indiana University
Bloomington, Indiana, USA
jdev@iu.edu

DongInn Kim
Indiana University
Bloomington, Indiana, USA
dikim@indiana.edu

Shakthidhar Gopavaram
Indiana University
Bloomington, Indiana, USA
sgopavar@iu.edu

Meera Iyer
Indiana University
Bloomington, Indiana, USA
meeriyer@iu.edu

Shivani Sadam
Indiana University
Bloomington, Indiana, USA
ssadam@iu.edu

Shrirang Mare
Western Washington University
Bellingham, Washington, USA
shri.mare@wwu.edu

Tatiana Ringenberg
Purdue University
West Lafayette, Indiana, USA
tringenb@purdue.edu

Vafa Andalibi
Indiana University
Bloomington, Indiana, USA
vafandal@iu.edu

L. Jean Camp
Indiana University
Bloomington, Indiana, USA
ljcamp@indiana.edu

ABSTRACT

Studies of privacy perception in the Internet of Things (IoT) include in-laboratory evaluations as well as investigations of purchase decisions, deployment, and long-term use. In this study, we implemented identical IoT configurations in eight households to evaluate the installation and privacy concerns in the early adoption of IoT devices in our participants' homes. The specific contributions of this work are insights into privacy perceptions of and challenges to the adoption of networked smart home devices and privacy management of IoT devices. The focus in this work was on participants' privacy concerns about devices deployed in an IoT ecosystem influencing their gradual change of use. We detail how we use a three-week longitudinal interview protocol to compare user perceptions of privacy risk. We assessed users' comfort with devices, perceived benefits, and data sensitivity. We discuss the factors identified by participants as relevant to their personal security and privacy management of in-home devices. We close with recommendations for privacy preserving smart home devices grounded in our participants' experiences.

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3554205

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → User studies**.

KEYWORDS

Internet of Things (IoT), smart home, privacy, security, user interviews, 2fa

ACM Reference Format:
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 *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3549015.3554205

1 INTRODUCTION

A key focus on smart home devices, despite their widespread adoption, has been on their data gathering and sharing practices. Recent literature on smart home devices focuses not only on how to develop better technical interventions to make smart home devices more secure, but also increasingly looks at users' mental models of this new technology as it pertains to individual privacy. For example, Garg and Kim [20] have looked at how security and privacy factor into the purchase and adoption of smart home devices. This builds upon prior work by Zeng et al. [45] which explored privacy concerns around smart home devices that users had. However, a majority of privacy work focuses on particular categories of smart home devices. In other experiments, the method of choice was creating vignettes to understand how users think about smart device privacy and how they might modify their behavior (or not) to become more privacy-preserving [3, 16]. Thus, largely, studies

around smart home devices have been in isolation, even if they were in context of use. In this study, our goal was two-fold. First, to create an experimental user scenario with a network of actual devices so that we can understand actual user behavior beyond vignettes. Second, our goal was to understand these devices not in isolation, but as an *ecosystem* of devices where we can observe how users manage multiple devices and manage boundaries in an interconnected home.

Furthermore, our work builds on prior work [8, 46] which provides users with a quick visualization of different smart home devices which users might have installed. We include a smart home dashboard visualization as well, and test it's adoption as it pertains to our experimental ecosystem. The goal of the experiment was to answer two core questions:

RQ1 **What privacy trade-offs did users make when faced with a network of new smart home devices?** We report on how users were challenged with practical constraints not just by information context, but sometimes also due to the nature of their living situation, ability to manage their information, or existing device capabilities. We observed the reduced usage of two-factor authentication for network segregation as well as reduced dashboard (which consolidates devices in use) usage.

RQ2 **How did users manage their privacy options in a connected home?** We report on usage over three weeks to show that users gradually found devices less useful, the locations they chose to keep these devices in to manage boundaries, to what extent dashboard usage helped with privacy controls, and why they did not use some of the devices at all, even if they were beneficial to protecting their data.

To this effect, we recruited eight participants and provided instructions to install a smart home devices kit in their homes. In this paper, we report results from the installation phase and three weeks of interviews specific to our research questions.

Our users found smart home devices easy to install and dashboard easy to interpret, however quick adoption did not mean sustained usage. Rather we observed a decline in usage even in the first three weeks though users might have left the devices operational. Furthermore, interoperability (compatibility with other existing smart devices) was more desired over security options (like two-factor authentication) during the interviews. We also found that the locations chosen by participants reflected their privacy choices (not keeping a camera in the bedroom or the bath), echoing findings in prior research. We report on how our specific contributions can help understand how users interact with different kinds of such devices in their environment.

We also discuss how our research design integrated considerations of user autonomy and harm minimization through dashboard controls and two-factor authentication. The primary ethical focus for this experiment was ensuring privacy. Our specific contributions are threefold. (1) First, we report on device use and non-use, practical reasons for doing so, and users' areas of discomfort with the smart home ecosystem. (2) Second, we compare our findings with those of recent literature to confirm (or not) whether smart device privacy perceptions are the same for individual stand-alone devices or do these change when multiple new devices are integrated into a complex home network. (3) Finally, we make actionable recommendations on how smart devices can compliment each other in a network to provide improved utility for users.

2 RELATED WORK

In the section below, we discuss key findings in recent smart home device security and privacy inquiries to situate the contribution of our work.

2.1 Privacy Perceptions of Smart Home Devices

Experts have argued that the privacy and security dangers of smart devices are myriad, with users accepting or rejecting smart devices early on during the adoption phase [9]. In fact, privacy concerns and satisfaction from initial curiosity result in reduced usage of these devices over time [25] unless such use was incorporated into users' daily routines or saved them money [20]. There have been attempts to formalize the privacy norms people have around these devices to better understand the source of these phenomena. Apthorpe et al. designed a model based on Contextual Inquiry (CI) [29] illustrating that users' privacy concerns about smart devices can be understood through the lens of contextual privacy. Participants have been found to be particularly concerned when data was taken without consent and when it was used for targeted advertisements [3], especially for smart security cameras [19].

In multi-user smart homes, IoT devices were found to create or reify power differentials between the owner and other users of smart home devices [21]. The sender, receiver, attribute, and transmission principle were all important in *combination*. Even in situations that involved privacy tensions between the device owners and bystanders, users considered the context and that their responses depended on the context in which these devices were being used (home versus workplace for example) [10].

However, results differ for older adults, consider aging in place. In the case of older adults, loss of privacy may result in more autonomy through technologically-supported aging in place. In such cases, older adults would choose the former [39]. In fact, they were likely to be more concerned about the data recipient and the activity being captured, if the recipient were a family member than a third party advertiser [34]. Thus, demographics seems to influence privacy perceptions concerning smart devices.

Additionally, Abdi et al. found that mental models of smart assistants were not fully developed in terms of perception about data storage, processing, and sharing [1]. Furthermore, their participants would prioritize benefit over risk of data sharing through their smart home devices [47]. It was more likely that their privacy threat model was influenced more by their prior experiences with computers in a different context than data practices of the smart devices they used [38]. Expertise has been found to play a significant role in mental models of security and privacy perceptions [4, 48] and behaviors [41, 43].

Privacy concerns seem to be more salient during *usage* rather than when *purchasing* devices. Participants often indicate that they do not think about privacy during purchase, and a label might be useful to do so - but it was something that came up later when they thought about usage [16]. Thus, we can see privacy concerns as a possible reason which affects smart device usage, but the picture

is more nuanced. We can logically assume that it would become even more nuanced when there are multiple smart home devices interacting with each other in a home ecosystem.

We integrate these findings into our experiment explained in Section 3 to verify what privacy concerns are reflected by participants in terms of device choices, preferences, and location. (Please see RQ1).

2.2 Protection Mechanisms Wanted and Developed

Prior studies have also focused on developing security mechanisms for protecting people's privacy. Our experiment was informed by previous designs targeted at empowering users. Intractable threats to the users that have been studied include over-privileged mobile applications [17], compromised networks [30, 31], and insufficient sensitive information protection [18]. Demetriou et al. built *HanGuard* to protect smart home systems against malicious applications which connect to the network [13]. Castelli et al. found that data visualization through "open.DASH" gave participants a better idea of what data was being collected through various sensors. They also found the visualization helpful to keep track of the various sensors embedded in their home [8]. There have been similar efforts in building automatic security managers designed to protect smart networks [35, 36], sometimes with user-defined rules [28] for better access control [40].

Several studies have found specific recommendations around smart home ecosystem improvement, for both individual and multi-user scenarios. In one study, participants had trouble identifying routines they want to automate and mapping how the system might support those routines. Participants wanted information and awareness about what happens in the house, particularly historical data (e.g., utility usage). Participants also wanted (physical) security awareness information, such as whether doors/windows are open, is there any activity at home when nobody is home. Additionally, participants wanted their smart home interface as one central point in their home for everything, things other than smart devices (e.g., smartphones) and things outside the house, like a business dashboard but for the home [24]. Similarly, Zeng and Roesner found that when some of these recommendations were tested by redesigning a home IoT application that connects these devices, transparency and access control were important, and user control on a combined design system for smart devices was largely affected by social norms in the home [46].

Much of the management of IoT appears to remain under social management, where trusted family members or friends collectively manage privacy [14]. This suggests that in a networked system of smart devices, it is also likely that a combined design system might be useful and might be influenced by social norms. Brush et al. recommended removing structural barriers to installation and adding primitive security controls to address inflexibility and poor security management respectively [6]. Similarly we focus here on installation and initial use.

In one of the studies which tested indicators, over half the users did not notice the webcam light for their computer when it was in use - a similar scenario is likely for smart home devices as well [32]. Simple light indicators were not enough for smart device awareness. When selecting IoT devices, absent significant redesign, people focus on price and function, ignoring issues of security and privacy [22]. We integrate these suggestions into our dashboard system, as explained in Section 3.1 to test if participants use it to manage their privacy. (Please recall RQ2.)

In this work, we sought to go beyond the purchasing experience and evaluate how individuals interacted with IoT devices during installation and initial use.

3 STUDY DESIGN

We implemented a three week study to evaluate the experience of living in the IoT. We recruited participants using an internal university mailing list, NextDoor for the local college town, and internal classifieds within the university. We queried each respondent about interest in IoT, current housing situation, and demographics. We filtered the 48 responses, selecting participants who had complete responses and were able to access their home router. From the remaining 27 we sought diversity in employment, gender, education, and age with a bias against current students due to their over-representation in computing and information research. Due to constraints on equipment available, we could only field up to ten participants for the in-home study. While 19 of the 27 respondents were invited to participate the remaining 8 requested to not participate in further studies. Only 8 of the 19 responded as being able and willing to participate in the additional in-home study. All of the survey participants were provided with a $5 gift card. Only those who were selected for the in-home study were told the payment and provision of IoT devices that would be a component of that participation. All components of the research were reviewed and approved by the university's Institutional Review Board (IRB).

The resulting participant population consisted of 4 women and 4 men, ranging from 21 to 58 years in age (mean=33.43, s.d.=13.99), with two participants identifying as Asian, one participant identifying as Black, and five as White.

One filter for participation was interest in or ownership of IoT devices. Our investigation was explicitly targeted on management of privacy and security risks of IoT devices. Therefore in order to ensure minimization of risk, we sought not to induce interest in the devices but rather to select participants who were already engaged in the IoT market.

3.1 Description of System and Dashboard

Due to COVID-19, the researchers were unable to visit participants' homes in person and complete the installation. Thus, we created detailed setup notes and a router configuration file for participants to be able to easily setup the different smart home devices. This setup and instructions were tested by one of the researchers and another person external to the study. Our system is designed to replicate the home automation system so that we can proceed with the experiments of home IoT securities for each participant. It consisted of the following devices and they were connected as shown in Figure 1. These are a) One TP-Link Router; b) Two Raspberry Pis - Home Assistant and Safe Router; c) One extensible Philips Hue lighting system consisting of the controller and two smart bulbs; d) One Amcrest IP Camera; e) Components of a Ring Alarm

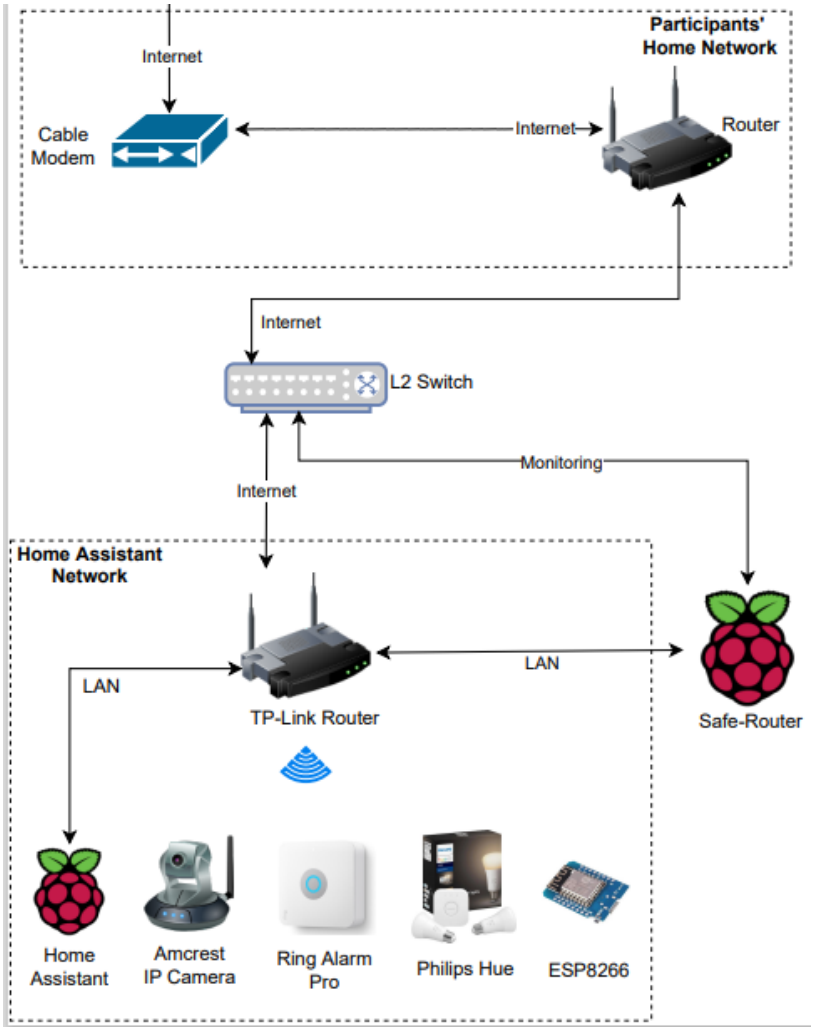

Figure 1: Diagram of IoT Devices and Home Network.

system consisting of an Alarm Base, Key Pad, Z-Wave extender, Z-wave motion sensor, and 4 Z-wave contact sensors; f) Two ESP8266 boards with motion, humidity, and temperature sensors; g) One TP-Link network switch (L2); h) a single Yubikey; and i) a USB-3 to RJ45 adapter. Necessary cables for installation and a power strip were also provided.

A TP-Link Router was used to provide an independent network (i.e., for Network Address Translation (NAT)) for participants who may have their own network already. Participants were asked to connect the router we supplied to their local network, in addition to the Pi Safe Router. The Pi-based Safe Router ran in parallel to monitor connections and ensure security.

Two Raspberry Pis were used, one to support the Home Assistant and one as a Safe Router system. The Safe Router implemented the functionality of the Home Assistant by enabling participants to disable devices (or the entire system) after installation. The decision to use the Safe Router in addition to the Home Assistant delayed the experiment and made installation more difficult. The Wizard of Oz approach, which is a common method for evaluating participants' preferences in interactions by showing people something that appears to function as intended but is inherently not [12, 15], while we were able to ensure that participants' desires to disable devices or block dataflows were in place through our implementation of the Safe Router. The widespread sharing of data, including when an app is uninstalled, required a local intervention to ensure the devices did not access the Internet after participants disabled them.

Participants were also provided with an Android tablet which was able to connect to the provided router's wireless network. The tablet was configured to interact with the Home Assistant and provide an overview of the different systems as a dashboard for participants. Participants had to login to the tablet and enter a specific URL to see the dashboard visualization. An example mock-up of a participant's dashboard is shown in Figure 2, as a screenshot of a participant's dashboard would reveal significant personal information.

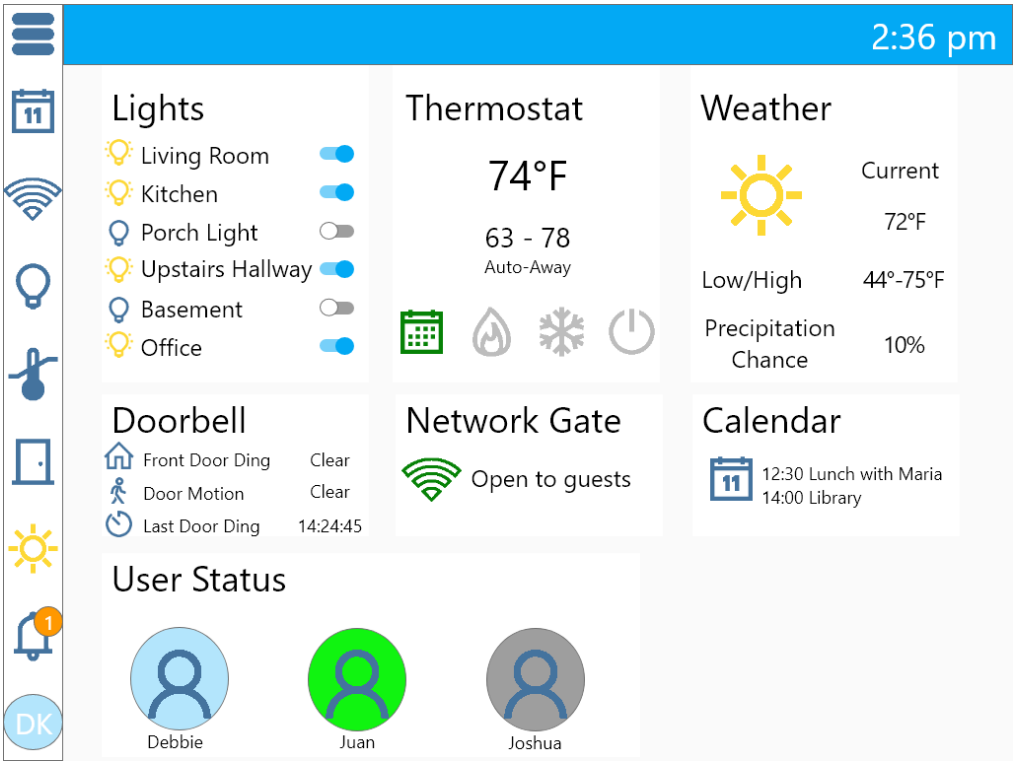

Figure 2: Mock-up example of participant's dashboard viewed on tablet screen.

3.2 Interview Protocol

To understand privacy trade-offs, we asked about participants' general experiences with the eight smart devices they were requested to set up. The first week of interviews was to check if the installation went smoothly and how participants were using the devices. Once they were more comfortable, we asked follow up questions about their experiences and privacy management strategies. We did not explicitly ask about privacy and security to avoid biasing participants views, but followed up with questions if they brought it up on their own.

To pilot our interview study we recruited four older adult participants from a large-scale IoT-in-the-home study who were already living in a setting similar to ours. Our initial interview pool was participants in the HomeSHARE project [33]. HomeSHARE is a test-bed of adult homeowners who have agreed to engage with researchers for the evaluation of in-home technologies. Any researcher or research group working on a smart home project is able to contact HomeSHARE researchers and request to conduct a study with the participants as long as there is IRB approval. As it was founded in 2015, this is a population that is particularly aware of issues that may emerge when using in-home technologies, and comfortable with interactions with researchers.

We interviewed them during the week of November 17-20, 2020 and asked questions for our pilot interview. Specifically, we sought individuals who were planning to purchase IoT devices or had some experience in IoT devices in order not to create a risk of data exposure. This is a potential limitation of this study, as early adopters may be more positive about technology [26]. Given current market penetration we chose this as a reasonable basis for exclusion with a recognition of the potential limiting effect.

Based on pilot interview responses, we modified the interview protocol slightly by adjusting the structure of weekly interviews to be semi-structured and all questions were open ended, excluding those directly pertaining to the Trust, Benefit, Satisfaction, Burden questions which were requested as true/false responses [11].

In the three weeks immediately following installation, participants were interviewed for approximately 30 minutes each week. The first week of interviews focused on the process of setting up the IoT devices and system along with the Trust, Benefit, Satisfaction, Burden questions [11]. Weeks 2 and 3 focused solely on check-in questions regarding the use of IoT devices, experiences participants had with those devices, reflections on behaviors, and their interests in other types of IoT devices.

Due to COVID-19 all participants communication before installation was remotely through email. A box containing all items, detailed in Section 3.1, was delivered to their homes. All interviews were conducted through Zoom, including the initial interview scheduled for the week after the devices were delivered. All interviews were audio recorded and initial automated transcriptions were created. Using the recorded audio, the automated transcriptions were extensively edited for correctness by four of the authors. The transcriptions were analyzed in an iterative, open, and axial coding process by four of the authors. We used an initial set of 8 transcripts from the first two weeks to identify emergent themes

and their related topics. From those themes, we developed an initial draft codebook and the four coders applied the codebook to an additional 8 interviews from weeks 1 through 3. New and emergent themes were added as appropriate before all 24 interviews from the three weeks were re-coded with the updated codebook. The four coders each individually coded 12 interviews so there was overlap with one other coder. Any conflicts in codes were brought to group consensus of all four coders.

4 FINDINGS

In this section we report our findings of the three-week study on deploying the IoT ecosystem in eight homes. Recall the first research question was on what privacy factors affected non-use for participants. We found that placement and continued usage were impacted by practical concerns (particularly benefits of use and difficulty of managing the devices) and privacy. The second research question addressed what privacy choices they made to influence their privacy relationship with the devices. Participants reported liking those devices which supported physical security, while also creating boundaries with the devices to manage their privacy discomfort. Privacy management took the form of physical placement, disabling services, and in one case removing a device rather than actively managing data flow with the privacy-preserving features that were enabled via the dashboard. Participants wanted to customize the operation and have privacy settings embedded into that customization. For example, they did not want video to be leaving the house when they themselves were home, but rather only when they were away and might want to access it. They expressed a greater interest in actively managing privacy than we observed in practice. These findings are discussed in greater detail below.

4.1 Participants

We first describe the recruited eight participants who installed the devices (described in Section 3.1) in their homes. These participants were selected from an exploratory survey of 48 participants based on diversity, network environment (e.g., have access to a router), and prior experience with smart devices. All activities were reviewed and approved by the IRB. Four of the eight participants lived alone and four others lived with at least one other person. Participants were split equally between men and women. All of them lived in apartments, with the exception of P4 who lived in a single-family house. Participants' demographics are summarized in Table 1.

4.2 Continued Utility and Use

Table 2 shows usage of each of the device over the three-week period as reported by participants during interviews. As we can see, the Yubikeys (provided as a second layer of authentication to protect the Safe Router against network attacks) were never used by any participant over the three weeks. A second layer of authentication was seen as both inconvenient and unnecessary since there were few people having access to their devices during the COVID-19 pandemic. We were unsure if this would change if there was a potentially large gathering of people at participants' home or a steady stream of guests as might occur in the absence of a pandemic. The Android tablet (dashboard) was setup by participants by Week 2, and applicants reported it as usable and acceptable. In the first week it was not used; in the second they reported looking at it; and by the third week they reported additional interactions. In the first week however, instead of using the dashboard, participants chose to use other applications that directly connected them to the devices (for instance, they used a Phillips Hue app to connect to Phillips Hue lights). The smart cameras were the slowest in adoption, with four of eight participants uncomfortable in their use during Week 1 and were concerned until they knew what data was being collected. For the two participants who started using the camera in Week 3, they reported installing it in a less frequently accessed location.

An interesting case was that of the Ring alarm system. Seven out of eight participants immediately installed it (one did not due to practical constraints discussed later) in the initial adoption phase. However, by the third week, three people had given up using it because it was either not useful to their situation or it made too much noise.

Participants seemed to search for a balance between installing too many devices to manage with obtaining all the possible benefits of home IoT. In one case, while the participant found the set of interconnected devices fascinating in the first week of receiving them, the excitement was replaced in the subsequent weeks by information overload and questioning about the benefit of multiple devices:

> "[I have a] hard time, at times, to learn all the functions and everything. So sometimes it feels like it's more work to use a smart device than to not. And what's the benefit, you know? Is it worth all that work in the long run so that you get a quarter less detergent used or something, you know? [recalling why they refused a smart washing machine]." *(P5, 47, Woman - Week 3)*

Thus, utility from some of the smart devices that was reported in the first week decreased over time. Initial utility was not the same as continued utility. In one instance, a participant reported not using most of the devices, even though all of the devices were setup and running, because it was not necessary for their everyday lives. Again, the study occurred during a pandemic when remote access was not a needed benefit.

4.3 Usage Restricted by Practical Concerns

More than balancing benefits of using the devices, there were practical problems that participants took into consideration while using the devices. For example, usage of smart devices was often restricted by lack of need or living situation. Even if a participant found utility in a device, they would not use it in context because it was not helpful to *their* unique situation. For instance, P4 mentioned that since they live in a safe neighborhood, they did not find utility in the Ring alarm system:

> "Honestly, I'm worried that it's going to be like loud. Okay. And when door opens, I don't like it. Well, let's say that alarm's really loud in my experience, a lot of tenants their alarms set off accidentally more often than they are actually in use. I live in what I think is a fairly safe neighborhood. I'm not really worried about somebody coming in." *(P4, 59, Man - Week 2)*

Table 1: Details regarding age, gender, educational background, number of people in participants' households, and home type are provided. * (Asterisk) indicates the number of people under the age of 18 living in the household.

Participant	Age	Gender	Education	# People in Household	Home Type
P1	22	Woman	Some college	2	Apartment
P2	22	Man	Some college	1	Apartment
P3	29	Man	Master's degree	1	Apartment
P4	59	Man	Some college	2	Single-Family Home
P5	47	Woman	Bachelor's degree	1	Apartment
P6	36	Man	Master's degree	2+2*	Apartment
P7	26	Woman	Bachelor's degree	1	Apartment
P8	22	Woman	High school diploma	2	Apartment

Table 2: Number of devices in use per week over the three weeks for all participants.

Devices	Week 1	Week 2	Week 3
Android Tablet	6	8	8
Router	5	7	7
Home Assistant	8	8	8
Safe Router	5	7	7
Yubikey	0	0	0
Ring Alarm	7	7	4
Philips Hue Hub	6	8	8
Camera	4	6	8

In another example, participant P2 said that since they live in a basement apartment, they did not need to install an alarm system since it was unlikely that intruders would use the window to enter.

There were also cases where participants' living situation, such as apartment restrictions, led to device non-use.

> "It's kinda difficult living in an apartment. And I'm always worried, like maintenance will come in or something like that. I don't really set it that often, but I do have the motion sensor setup in the habit. [...] Maybe don't make maintenance mad. And let's say if I forget that I have like one of the maintenance guys coming out here to fix like the oven or something. I am kind of terrified that if I alarm it and forget about it, and then everything starts going off, that could be a disaster." *(P2, 22, Man - Week 2 and 3)*

The participant in this case expressed a concern that installing the device could potentially cause maintenance to remove it and charge them for damage to the apartment.

With both second factor authentication and use of the devices, utility was defined by context. In both cases setup and configuration were identified as initial barriers. Participants expressed concerns with use based on physical (e.g., need for control over apartment entry) and social (e.g., disturbing neighbors) contexts.

4.4 Setup is Easy but "Learning Something New" is Intimidating

All participants were fairly comfortable with setting up the devices. Those who setup the devices themselves (seven of eight) expressed confidence that the process of installing and initializing the devices resulted in a better understanding of how the devices worked together in a network better. While there was one participant who perceived it would be easy at first, but found it somewhat more challenging in practice. All participants were able to follow instructions and setup the devices. As participant P7 commented, the "plug and play" nature of the devices were fairly easy. This was partially due to their self-confidence in setting up and using IoT devices that stemmed from their previous knowledge or usage of IoT devices. It was also due to confidence in their own technical skills. For example, P4 said that it was easier for him to setup the Raspberry Pis because he had "played around with them" before.

However, that sentiment was not shared by all participants for Raspberry Pis. Two of the participants had questions about what the Raspberry Pis did, and one participant asked for an explanation on how the Safe Router setup on the Raspberry Pi worked, what it did, and how it was connected to their router:

> "Like the Raspberry Pis, that seemed a little bit over my head. I was just plugging things in just because a piece of paper told me to. But then when it came to the more, I would say non-technical things like the Ring, the Hue, the camera - that kind of stuff - that was a lot easier to do." *(P3, 29, Man - Week 1)*

The services provided and use of the Pi were not immediately obvious to them; but others were simple to operate using the dashboard that was provided to them on the Android-based tablet. In contrast, the plug-and-play devices were viewed as less technical. In addition, one of the participants mentioned that it was somewhat of a learning curve for them to operate the Android-based tablet because they were an Apple user and not very familiar with the Android interface.

4.5 Physical Safety as a Driver

While participants provided several reasons for non-use, there was one particular utility that more than half of the participants wanted - smart devices that offered physical security. For participant P1 this meant a smart alarm system to help protect their car from

being stolen. Two of the four participants also said that smart alarm systems would help keep their doors secure when they were away. One of the participants also liked the smart camera with motion detection since it would help them keep aware of their pet when they were away from home:

> "We have a Google Home, and then we have another [...] it's just like a small little camera that connects to our phones so we can see our dogs from out there. I'm kinda like crazy dog mom, so I wanted to see what he does when I'm not there." *(P1, 22, Woman - Week 1)*

Home security was a desired feature, even to the extent of participants choosing to use the smart alarm system and the smart camera despite discomfort with the privacy implications.

4.6 Participants' Information Boundaries

Participants set up boundaries to both the physical devices and the information shared by them. These boundaries were either physical, informational, or both. For example, P1 said that they turned off notifications because they were receiving too many. This was a way of enforcing informational boundaries. Another type of information that participants were reluctant to share was location. P4 and P6 were skeptical of devices which shared their location and asked during the interview if their location was being shared in some way or expressed discomfort in devices that capture location.

Information boundaries were also created through physical separation with participants choosing specific locations for specific devices. When asked about the reasons for their decisions, they mentioned that they were not sure who were recipients of their data. This was consistent with the findings for privacy design for home-based aging devices [34]. Shankar et al. found that participants desired data transparency and information about who had access to their data; specifically, location of sensitive activity was important so that they chose to avoid placing certain ambient devices in the bedroom. This echoed in our findings as well.

A location map of where participants reported placing devices during the first week of installation is shown in Figure 3. While we do not know the exact layout of each participant's home, the location map is a generic home layout to provide visualization of how devices were spread throughout a home. Some placement of devices were limited by physical restraints and minimally reported or discussed by participants, such as that of the Safe Routers, Home Assistant, and network switches which were always located in close proximity to the TP-Link Routers due to the required wired connections. The clustering around the entry was found to reflect the privacy concerns through the weeks of interviews but not all locations indicate privacy concerns. For example, the participant who placed the camera in the hallway closet did not do so to avoid video surveillance but rather to watch, and potentially stop, their cat from eating the food in the closet which served as a pantry.

One of the findings of particular interest was that one of the participants had discomfort not for themselves but for the privacy violation of people around them [2]. This participant chose to not install the Ring alarm system not because they looked at possible usage, but because it could potentially do more harm than help due to the loud noise made by the system which would be troublesome for their neighbors.

We also found two opposing examples of boundary management, where two participants reported sharing *more* information with other people in their household so that they were able to use the smart devices they have. In one example, participant P1 had her partner setup the devices and reported on their partners' experiences as closely as possible. This pointed to a recurring theme in smart home device research where multiple users might be involved in the purchase [14] (i.e., receiving smart devices as gifts) and usage of the devices [21, 45]. The other participant reported how he has personal information to help setup devices for his grandparents. This multi-user situation was also reflected in the participant's comments, where he mentioned that even though he is not the person who uses the device, he knows all the passwords and other security settings for his family's smart devices:

> "I pretty much know all their username and passwords, which is kind of amazing because I have to remember. And both of my parents [...] text me and ask me the password But as far as like the privacy settings and everything, well, when I was living at home, I set it all up so I can access it as well. And then as soon as I moved out, I disabled that. [...] I set up their accounts and their usernames and everything like that. And then if I need to, I can get into it like remotely, which is kind of nice. Like if my grandma has a problem, so that's four hours north. So [it's easier] than driv[ing] four hours north to deal with it." *(P2, 22, Man - Week 3)*

While talking about his setup process, the participant also mentioned that their family would not change these credentials because it was inconvenient and involved a steep learning curve, especially for older adults like his grandparents.

Thus, in smart home ecosystems, sometimes a trusted third party (perhaps a family member) was helpful in setting up a complex home device system. This aligns with previously observed password behaviors in desktop and mobile environments as people use social strategies to manage the complexity of passwords, e.g. [23, 37], with older adults more likely to delegate such management [27].

4.7 Participants Perceptions of Media Type

One of the key concerns across all participants was video as a sensitive media type. Four participants expressed discomfort with the smart camera equipped with motion detection because of video capture. No participants placed the camera in their bedroom or bathing areas. For the participants who chose to leave their camera on, two of them placed the cameras so they could only view the outside of the house and ensured that it was easy to disable them via unplugging their devices. One participant choose to disable the camera on the basis that it had a microphone:

> "I can see the feed, what I didn't realize initially that, was that it was also going to be recording the audio. I thought it was just going to record the, you know, the visual feed. So I haven't used that very much. I don't want to be recorded the whole time I'm home." *(P5, 47, Woman - Week 2)*

During the interviews, one participant also had questions about who had access to their data that was being captured by the camera:

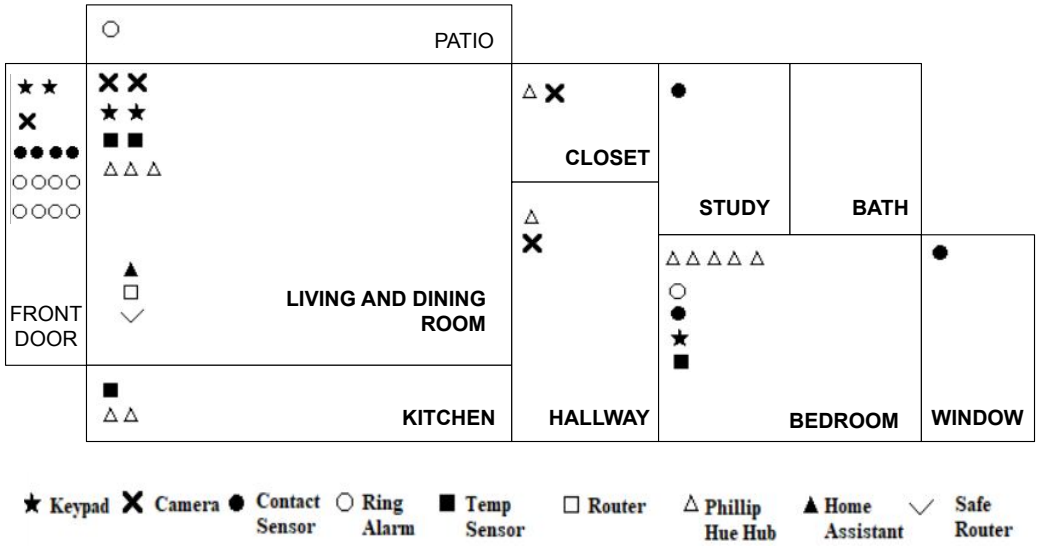

Figure 3: Participants chose where to place devices in the first week of installation. The symbols indicate the sum of participants placement of devices in a particular room as shown in the legend above. For example, the × symbol represents a camera, and one participant reported keeping the camera in the closet.

> "I'm also feeling like, I have a feeling that you guys have access to my information, which I'm not sure about." (laughs) *(P8, 22, Woman - Week 1)*

She knew that the researchers had committed to not accessing any raw data, but rather observe only periodical automated reports of devices being online and the recordings of our interviews. Yet the potential existence of the data flow of real-time audio beyond the house caused discomfort regardless of its use or recipient.

4.8 Interoperability and Participant Choices

Ideally any person seeking IoT devices should be able to select any functional device based on the services provided by that device. When natural market dynamics result in the emergence of a single standard, product, or producer, then the consumer is said to be locked-in, meaning their choices of products are limited. Lock-in can have many possible sources (e.g., increasing returns, economies of scale, network effects [42]) but the result is still loss of consumer choice. In this case, participants are facing high switching costs, meaning that changing from one family of products to another has a higher cost than simply continuing to purchase products compatible with those previously installed. Thus for two IoT items that appear to have the same cost, the one that is interoperable, is easier to install, certain to work, and will not require additional products, is cheaper for that participant. So it is not surprising interoperability and prior personal experience with devices were significant factors in device usage. For example, one participant said that instead of using the dashboard system, they preferred to connect their devices to Alexa:

> "I like the Amazon Alexa app. You can go through and see, like, what skills you can get or add. And then that pretty much can tell you like, 'Oh, this will connect to this device' or 'it'll connect to this device.'" *(P2, 22, Man - Week 3)*

This convenience is indicative of why users prefer to purchase devices which have a wide range of compatibility. They would prefer devices which they can integrate with their *existing* smart home devices, over a system which might have been more usable if purchased first and certainly is more privacy-preserving, as having already learned to engage with one device creates a barrier to adopting another mode of interaction. In terms of privacy the result is a preference for devices that easily connect with other devices, as compatibility is easiest if devices connect without authentication and share information widely in the local network.

This was in contrast with Castelli et al.'s findings, perhaps due to the nature of the smart home devices [8]. In their study, it was found that visualization gave participants a better sense of the data being collected by the various sensors. In our case, the dashboard visualization of the connected smart devices was informed by and similar to *open.DASH* developed by Castelli et al. However, participants indicated that while the dashboard was easy to use, greater compatibility with smart home assistants (like Amazon's Alexa or Google Home) made them more likely to use those devices. In our study, some of the devices had easily accessible mobile applications that did not show data flow from the participants' home. In later weeks, as we asked participants to evaluate their experiences with the dashboard as their familiarity increased, the perceived utility and usability of the dashboard increased.

4.9 Familiarity Drives Setup and Usage

Familiarity was a primary reason why participants found it easier to setup some of the devices compared to others. Those with prior experience with a specific smart home device or platform, like

Raspberry Pi (on which the Safe Router was installed), found it easier to setup and use some of the included devices:

> "... the Raspberry Pi, that's not something that I've ever worked with before. I'd never really seen one in person, so I would not have known otherwise what it was." *(P7, 26, Woman - Week 1)*

Familiarity also contributed to why participants chose not to use some of the privacy-preserving services provided. For instance, by the end of the third week, none of the participants used the service integrated with the Safe Router that allowed isolated guest access to the the home Wi-Fi. The Safe Router provided network isolation and connection tracking to mitigate the risk of installing IoT devices and to limit access of others' personal devices so that guests could access Wi-Fi but not control IoT devices. Participants perceived the Safe Router as an unused device, when in fact every connection used network characteristics to evaluate the security state of the IoT devices and prevent suspicious incoming connections.

Similarly, they did not use the Yubikey as a second factor authentication system that would be used to control their network allowing new connections or not regardless of how much previous access was granted.

4.10 Automation Constrained Customization

The argument against automation was summed up nicely by P4:

> "So this is the other thing that I've found with things that are automatic... (they) are great when they do what you want. But they're really irritating when they don't and they don't provide you with like a switch to say I'd like a set of options thing. I'd like you to do this or this or this." *(P4, 59, Man - Week 3)*

About half the participants did not actively dislike automation with smart devices, but would like options that allowed them to customize based on their needs. For example, P3 liked home automation which was energy-saving, but would not like that for a smart device he did not want turned off - like a smart fridge.

Although the participants voiced rejection of any but basic automation (some participants mentioned they liked smart lights that dim automatically), some participants preferred customized automation. There were two participants who already had experience using smart devices in their home that they controlled via their smart assistants. One of them automated the Hue lights to turn on or off based on their sleep routine (P7). Another participant liked home automation devices because they were energy-saving (P3). Two other participants who had more experience with networking and working with Raspberry Pis were annoyed that they could not customize the whole network of devices. Few of them mentioned that they could not customize enough through the dashboard. They instead downloaded the application (for the Hue smart lights) to do routine customization beyond basic on/off/dim functions, which was limited through the dashboard. One participant also mentioned that they would like to control and move the camera, but since it was not possible to do so through the dashboard, they used the application for the camera on the tablet to make it turn and move. In fact, as opposed to Jakobi et al. [24], where participants mentioned that they wanted information and awareness about what is going in the house, particularly historical data (e.g., utility usage) in a central dashboard, the lack of customization caused them to use additional apps outside the provided dashboard.

5 DISCUSSION & RECOMMENDATIONS

During the interviews participants described their own decision-making with respect to privacy and security, and their management decisions addressing those concerns. In this section we move beyond the observed and reported behavior and describe the motivation and reasoning as reported by participants.

In addition to building on the recommendations from previous studies, our work provides feedback from a test-bed setup of smart home devices and how users manage them. We also report on the effectiveness of some well-known security mechanisms, specifically two-factor authentication when applied in the context of a smart home ecosystem and its adoption.

5.1 Two-Factor Authentication Acceptability in Smart Homes

As we saw in our usage map, Figure 2, the Yubikey meant to secure the SafeRouter was never used by any participant. While one of the possible reasons could be limited guests in the home due to the research taking place during the summer of 2021 and COVID-19 being a concern in the region, participants did not use it for their own household security. One participant was still left to setup the SafeRouter at the end of Week 1. This could indicate that even with setting up multiple devices, when participants chose to not have additional network protection, a likely reason could be due to perceived usability. Thus, more usable two-factor authentication, perhaps automated even, could be helpful if integrated in a home-based smart device network.

5.2 Customization for Individuals in Shared Spaces

Geeng and Roesner argue for customization of controls in multi-user systems [21]. We add to their recommendation, and suggest customization. Different participants have different needs, as they have indicated in our interviews, specific to *their* personal usage scenario. This also supports the Contextual Inquiry privacy norm framework developed by Apthorpe et al. [3] as context *does* seem to matter. Customization for a single user - even just "basic" versus "advanced" settings - where users can choose to manipulate the functionality of their smart home device was desired. Furthermore, customization might be especially necessary to address practical boundary problems in individual devices for specific usage scenarios. For example, custom sounds settings in devices like the Ring alarm would allow people with neighbors to install and use them without disturbing neighbors.

5.3 At Home versus Away Data

While participants' desired smart devices for home security, they also wanted to distinguish between data collected in their absence and presence, similar to Yao et al. [44]. For example, they wanted smart cameras for watching their pets or property while they were away. They did not want them to capture video of them or of people around them when they were present at home. Some participants

also enforced information boundaries by turning off notifications when they were at home. Accordingly, smart devices, especially those for home security, must be mindful of users being in the residence and adjust their functionality accordingly. Furthermore, more customization for notifications should be added to benefit specific use cases.

5.4 Types of Data can Invade Personal Boundaries

Participants expressed that they were more concerned about their privacy when it came to video capture over collection of metadata, even knowing the researchers were only collecting daily reports of device states being connected to the network or not. This is consistent with previous examinations of the sensitivity of video [5].

One example of a participant who expressed and acted on a privacy concern regarding a device was P5, who disconnected the camera upon discovering that it could also capture audio. This was especially true for inside the boundary of homes where audio or video collection was unwanted, which is why none of the participants installed the smart camera in their sleeping or bathing areas. Thus, to protect user privacy against video surveillance, smart devices should be transparent about the data they are collecting and have an opt-out mechanism (hard disconnect) or mute [7] without device disconnection. For example, multi-functional smart home devices like Echo Show [1] could have different modes where the video calling function could be muted - this would turn off the camera without turning off other device functionality.

5.5 Familiarity Increases Comfort

Participants chose to use devices that were more familiar to them. Familiarity also contributed to why participants chose not to use some of the privacy-preserving devices that were *separate* from the other smart devices, for example, the Safe Router. Thus, a recommendation would be to integrate privacy-preserving systems like the Safe Router into a system that participants are familiar with. A network segregation mode in existing devices that integrate two factor authentication would be more preferable than a stand-alone system that is an add-on to an existing smart home ecosystem.

6 LIMITATIONS AND FUTURE WORK

While the study was designed before the COVID-19 pandemic, we were required to make certain changes to the design due to restrictions on human subject studies needing to be conducted remotely. The small population size of our project is a limitation to the generalizability of our findings. Additionally, participants had to setup the devices themselves with no technical help except remote check-ins. Thus, all of participants interactions are self-reported in their interview and not real time think-aloud data. Our interviewers made sure to cross-check responses so that participants had all smart devices provided to them setup properly. Furthermore, we report on installation and use for three weeks of an in-home IoT systems study. An extended study with high level of habituation may have yielded different results.

[1] https://www.amazon.com/b/?node=23660877011

In future work, as participants could be in person again, having them complete specific scenario based tasks weekly with similar device setups in lab to ensure their use while incorporating small surveys may be a method to better help us understand what privacy considerations users have in specific usage scenarios while also collecting technical data of their use without violating their personal privacy boundaries of their home.

7 CONCLUSION

Our two research questions were (1) What privacy trade-offs did users make when given a network of multiple new smart devices and (2) How did they manage their privacy in a connected home? Due to the onset of COVID-19, participants had to install all of the devices themselves and setup their home network. After the three weeks of our study, we found that convenience, familiarity, and respect for participant sharing preferences were key to adoption. We also found that in addition to many of the findings from previous research, practical concerns like living situation also affected the usage of smart devices. Furthermore, unexpected media type and unnecessary automation were often seen to be intrusive in these homes.

One goal in this study was to understand if some of the concerns echoed by participants in other smart home device studies would be echoed in a situation with a network of devices. We also examined how expressed desires differed from actions. We offer initial insight around two-factor authentication in devices and if it would be reasonable to expect participants to embrace at home. However, our findings indicated that over even three weeks, the inconvenience of an external hardware token was found to be seen as greater than the benefit. Perhaps there might be a way to integrate these into an alternative house key or some other individual device in a future study.

In future, we would like to extend this analysis for multiple weeks to understand how participants would interact with these devices in different usage scenarios. One particular question of interest would be if during extended use participants reflect the same concerns expressed as those found in previous work exploring a contextual integrity framework for smart devices [3].

Since smart home devices are increasingly operating as components in networks within smart homes, this study contributes to an understanding of privacy around these devices when experienced collectively. By investigating the privacy concerns of participants in regards to integrated smart home networks we can build a more nuanced understanding of privacy concerns identified in previous studies of discrete device usage.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 451–466.

[2] 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, Article 116 (oct 2020), 28 pages. https://doi.org/10.1145/3415187

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

[4] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. In *International conference on financial cryptography and data security*. Springer, Springer Berlin Heidelberg, Berlin, Heidelberg, 367–377.

[5] Michael Boyle and Saul Greenberg. 2005. The Language of Privacy: Learning from Video Media Space Analysis and Design. *ACM Transactions on Computer-Human Interaction (TOCHI)* 12, 2 (2005), 328–370.

[6] 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* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2115–2124. https://doi.org/10.1145/1978942.1979249

[7] Kelly E. Caine, Celine Y. Zimmerman, Zachary Schall-Zimmerman, William R. Hazlewood, Alexander C. Sulgrove, L. Jean Camp, Katherine H. Connelly, Lesa L. Huber, and Kalpana Shankar. 2010. DigiSwitch: Design and Evaluation of a Device for Older Adults to Preserve Privacy While Monitoring Health at Home. In *Proceedings of the 1st ACM International Health Informatics Symposium* (Arlington, Virginia, USA) *(IHI '10)*. Association for Computing Machinery, New York, NY, USA, 153–162. https://doi.org/10.1145/1882992.1883016

[8] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens, and Volker Wulf. 2017. What Happened in My Home? An End-User Development Approach for Smart Home Data Visualization. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 853–866. https://doi.org/10.1145/3025453.3025485

[9] Pew Research Center. 2020. Implications of The Internet of Things Connectivity Binge. https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications [Online; Accessed 9. Feb. 2022].

[10] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I Would Have to Evaluate their Objections": Privacy Tensions between Smart Home Device Owners and Incidental Users. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 54–75.

[11] Giselle Corbie-Smith, Alice S Ammerman, Mira L Katz, Diane Marie M St. George, Connie Blumenthal, Chanetta Washington, Benita Weathers, Thomas C Keyserling, and Boyd Switzer. 2003. Trust, Benefit, Satisfaction, and Burden: A Randomized Controlled Trial to Reduce Cancer Risk through African-American Churches. *Journal of General Internal Medicine* 18, 7 (2003), 531–541.

[12] Nils Dahlbäck, Arne Jönsson, and Lars Ahrenberg. 1993. Wizard of Oz Studies — Why and How. *Knowledge-based Systems* 6, 4 (1993), 258–266.

[13] Soteris Demetriou, Nan Zhang, Yeonjoon Lee, XiaoFeng Wang, Carl A. Gunter, Xiaoyong Zhou, and Michael Grace. 2017. HanGuard: SDN-Driven Protection of Smart Home WiFi Devices from Malicious Mobile Apps. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Boston, Massachusetts) *(WiSec '17)*. Association for Computing Machinery, New York, NY, USA, 122–133. https://doi.org/10.1145/3098243.3098251

[14] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[15] Steven Dow, Blair MacIntyre, Jaemin Lee, Christopher Oezbek, Jay David Bolter, and Maribeth Gandy. 2005. Wizard of Oz Support Throughout an Iterative Design Process. *IEEE Pervasive Computing* 4, 4 (2005), 18–26.

[16] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[17] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security Analysis of Emerging Smart Home Applications. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 636–654. https://doi.org/10.1109/SP.2016.44

[18] Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, and Atul Prakash. 2017. Security Implications of Permission Models in Smart-Home Application Frameworks. *IEEE Security and Privacy* 15, 2 (apr 2017), 24–30. https://doi.org/10.1109/MSP.2017.43

[19] Geoffrey A. Fowler. 2019. The Doorbells have Eyes: The Privacy Battle Brewing over Home Security Cameras. *Washington Post* (Jan 2019). https://www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras

[20] Radhika Garg and Jenna Kim. 2018. An Exploratory Study for Understanding Reasons of (Not-)Using Internet of Things. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3170427.3188466

[21] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[22] Shakthidhar Gopavaram, Jayati Dev, Sanchari Das, and L Jean Camp. 2021. Iot Marketplace: Willingness-to-Pay vs. Willingness-to-Accept. In *Proceedings of the 20th Annual Workshop on the Economics of Information Security (WEIS 2021)*.

[23] Paul Grassi, Ray Perlner, James Fento, William Burr, Justin Richer, Naomi Leftovitz, James Danker, Yee-Fin Choong, Kristen Green, and May Therofanos. 2017. *Digital Identity Guidelines Authentication and Lifecycle Management: Section 10 - Usability*. Technical Report NIST Special Publication 800-63B. National Institute of Standards and Technology, Gaithersburg, MD.

[24] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799

[25] Amanda Lazar, Christian Koehler, Theresa Jean Tanenbaum, and David H Nguyen. 2015. Why We Use and Abandon Smart Devices. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 635–646.

[26] Anil N Makam, Holly J Lanham, Kim Batchelor, Brett Moran, Temple Howell-Stampley, Lynne Kirk, Manjula Cherukuri, Lipika Samal, Noel Santini, Luci K Leykum, et al. 2014. The Good, the Bad and the Early Adopters: Providers' Attitudes about a Common, Commercial EHR. *Journal of Evaluation in Clinical Practice* 20, 1 (2014), 36–42.

[27] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.

[28] Chandrakana Nandi and Michael D. Ernst. 2016. Automatic Trigger Generation for Rule-Based Smart Homes. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security* (Vienna, Austria) *(PLAS '16)*. Association for Computing Machinery, New York, NY, USA, 97–102. https://doi.org/10.1145/2993600.2993601

[29] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Wash. L. Rev.* 79 (2004), 119.

[30] Sukhvir Notra, Muhammad Siddiqi, Hassan Habibi Gharakheili, Vijay Sivaraman, and Roksana Boreli. 2014. An Experimental Study of Security and Privacy Risks with Emerging Household Appliances. In *2014 IEEE Conference on Communications and Network Security*. 79–84. https://doi.org/10.1109/CNS.2014.6997469

[31] Temitope Oluwafemi, Tadayoshi Kohno, Sidhant Gupta, and Shwetak Patel. 2013. Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security. In *LASER 2013 (LASER 2013)*. 13–24.

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

[33] Blaine Reeder, Haley Molchan, Eric Gutierrez, Ewelina Pena, Kelly Caine, George Demiris, Katie A Siek, and Kay Connelly. 2019. HomeSHARE: Implementing Multi-Site Smart Technology Infrastructure.. In *AMIA*.

[34] Kalpana Shankar, L Jean Camp, Kay Connelly, and Lesa Huber. 2011. Aging, Privacy, and Home-based Computing: Developing a Design Framework. *IEEE Pervasive Computing* 11, 4 (2011), 46–54.

[35] Anna Kornfeld Simpson, Franziska Roesner, and Tadayoshi Kohno. 2017. Securing Vulnerable Home IoT devices with an in-hub Security Manager. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 551–556. https://doi.org/10.1109/PERCOMW.2017.7917622

[36] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. 2015. Network-level Security and Privacy Control for Smart-Home IoT Devices. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 163–167. https://doi.org/10.1109/WiMOB.2015.7347956

[37] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 243–255.

[38] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I Don't Own the Data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 435–450.

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

[40] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The Current State of Access Control for Smart Devices in Homes. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2014, 209–218.

[41] Kami Vaniea, Emilee Rader, and Rick Wash. 2014. Mental models of software updates. *International Communication Association* (2014).

[42] Hal R Varian. 2002. Economic Aspects of Personal Privacy. In *Cyber Policy and Economics in an Internet Age*. Springer, 127–137.

[43] Melanie Volkamer and Karen Renaud. 2013. Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*. Springer, 255–280.

[44] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428

[45] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[46] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and in-Home User Study. In *Proceedings of the 28th USENIX Conference on Security Symposium* (Santa Clara, CA, USA) *(SEC'19)*. USENIX Association, USA, 159–176.

[47] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (nov 2018), 20 pages. https://doi.org/10.1145/3274469

[48] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, smart home'–exploring End users' mental models of smart homes. *Mensch und Computer 2018-Workshopband* (2018).

A INTERVIEW QUESTIONS

First Week Questions: Set-up
How did you set up smart devices? What challenges did you face?
How comfortable are you understanding the information provided by the dashboard?
Did it help you identify your devices? Does it help you identify foreign devices?

Check-in interviews (weekly)
Are you using this device? How often do you use it?
Is your device connected to other systems in your residence?
If yes - Which? / If no – Why not?
Has owning your device impacted your life? How? Why not?
Can you think of a good experience you have had with your device?
Can you think of a negative or unexpected experience/ experience that was frustrating with your device?
Did you have to change your behavior from using the device? If yes, how?
Do you ever turn your device off? Why? Why not?
Do you believe your system is safe for you while using it? Why/ why not?
Where have you placed your smart devices in your residence? Why?
Are there any smart home devices, including health devices that you wish to own? Why? Please elaborate.
Is there anything else you would like to tell us?

Trust Benefit Satisfaction Burden (Please select True or False for the following statements)

(1) In general, I trust the smart home devices provided
(2) As a result of using these smart home devices, I feel more comfortable about participating in research
(3) As a result of using these smart home devices, I feel more confident that users and smart home device manufacturers can form trustworthy relationships
(4) I trust that the devices would not do me any harm
(5) By participating in this research, I feel like I have contributed to a greater understanding of how researchers understand how people use smart home devices
(6) I like the idea of contributing to a better understanding of how people use smart home devices
(7) My technology skills have improved from participating in this research
(8) I like the idea that I have learned useful things about smart home technology from this research
(9) If I had the opportunity to participate in the smart home research again, I would do it
(10) I would encourage other people to participate in this research
(11) The study was clearly explained to me
(12) The researchers were helpful in encouraging me to complete the study
(13) Being a part of this study takes too much effort
(14) Answering all the surveys and interviews takes too much time
(15) Participating in this research is worth the time and effort
(16) Having sensors and internet-connected technology installed in my home, participating in interviews and surveys is worth the time and effort