Who's In Control?: Interactions In Multi-User Smart Homes

Christine Geeng and Franziska Roesner
Paul G. Allen School of Computer Science & Engineering
University of Washington
cgeeng@cs.washington.edu,franzi@cs.washington.edu

ABSTRACT

Adoption of commercial smart home devices is rapidly increasing, allowing in-situ research in people's homes. As these technologies are deployed in shared spaces, we seek to understand interactions among multiple people and devices in a smart home. We conducted a mixed-methods study with 18 participants (primarily people who drive smart device adoption in their homes) living in multi-user smart homes, combining semi-structured interviews and experience sampling. Our findings surface tensions and cooperation among users in several phases of smart device use: device selection and installation, ordinary use, when the smart home does not work as expected, and over longer term use. We observe an outsized role of the person who installs devices in terms of selecting, controlling, and fixing them; negotiations between parents and children; and minimally voiced privacy concerns among co-occupants, possibly due to participant sampling. We make design recommendations for supporting long-term smart homes and non-expert household members.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**; **Empirical studies in ubiquitous and mobile computing**.

KEYWORDS

smart home; privacy; multi-user; user experience; qualitative study; experience sampling

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300498

ACM Reference Format:
Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3290605.3300498

1 INTRODUCTION

Smart home devices and platforms—including the Amazon Echo, Google Home, Samsung SmartThings, Philips Hue lights, Nest thermostats and cameras, and more—are becoming increasingly ubiquitous in the homes of end users. Unlike the popular personal technologies of recent decades, like laptops and smartphones, smart home devices, when placed in a shared environment, become *shared* devices used by and affecting multiple people.

However, today's commercial smart home platforms often provide only limited multi-user support. For instance, in the case of SmartThings, end users can provision multiple accounts but cannot currently give them different levels of access to information [1]. Prior research has surfaced the need to study multi-user issues in smart homes in more depth (e.g., [37, 59]); taking advantage of the fact that smart homes are now deployed beyond early adopters, we study multi-user device sharing *in situ* among a variety of households.

In this work, we systematically study the interactions between multiple people in contemporary, deployed smart homes, asking: What tensions and challenges arise between multiple people? How do existing smart device and platform designs exacerbate and mitigate these issues? And how should smart device and platform designers best take into account these complex relationships and interactions? We investigate these questions using a mixed methods approach, combining qualitative interviews with experience sampling over a three week period with people living in smart homes. These participants were largely "smart home drivers", who make key decisions about device installation and use.

Our findings (Section 4) reveal tensions that arise among a variety of stakeholders—including parents and children, roommates, partners, and non-occupants—and across several phases of smart device selection, installation, and use. For example, we often observe a concentration of expertise, access, and control with the person who selects and installs smart

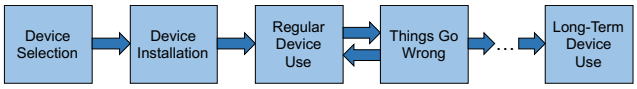

Figure 1: Smart Home Usage Timeline: Our study reveals multi-user tensions and interactions at several points during device installation and use.

devices in a home, which extends and reinforces prior work (e.g., [37, 59]). At the same time, we were surprised to find limited reports of concern about privacy between people in the home. This limited concern may be due to selection bias: our participants, mostly smart home drivers, may have been unaware of other or more serious concerns held by more passive users.

Our interviews also surfaced challenges that arise during the long-term use of smart devices: for example, what happens—or what should happen—when children grow up or house occupants change? From these and other findings, we distill lessons and recommendations for smart home designers, as well as identify opportunities for future research.

2 BACKGROUND AND RELATED WORK

We use the term "smart home" to refer to a home that contains computing devices that assist with automation, remote usage, and/or sensing for domestic use. This term can and often does overlap with the Internet of Things (IoT), which broadly refers to Internet-connected devices (though some smart home devices can function on a local network).

A variety of smart home technologies are becoming commercially available and are on the cusp of widespread deployment [45]. Common smart devices in today's homes include thermostats (e.g., Nest [41]), light bulbs (e.g, Philips Hue [30]), outlets, door locks, motion sensors, TV streaming devices, smart assistants, and indoor/outdoor security cameras. Smart assistants such as Google Home [24] and Amazon Echo [2] include functionalities such as music playing, web search, reminders and timers, and voice command controls for devices connected to it, such as lights. Also commercially available are smart home hubs, such as Samsung SmartThings [48], which provide centralized control for devices that may come from different manufacturers.

Living in Smart Homes

Early "in the wild" user studies with smart home devices focused on understanding technical barriers to adoption (e.g., [8]). With improvements to smart home technology, user studies have moved towards exploring and evaluating how device designs do or could fit into domestic routines and home life, e.g., [31, 32, 37–39, 56–58], as well as other shared physical environments [49].

A particular recurring issue in prior work, reinforced and expanded by our study, is the different levels of access and ability among different people in the home [11]. For example, Bell et al. (2007) called for the study of how ubiquitous computing could reproduce existing power concentrations in relationships [5]. Specific to smart homes, both Mennicken et al. (2012) [37] and Zeng et al. (2017) [59] recognized the need to support household members who did not initiate smart home installation and do not have the same expertise and agency as installers. Our work aims to explore and study these and other tensions that arise in multi-user smart homes *in situ* and in more depth.

Privacy in the Home

User privacy, defined as maintaining "control over personal information" [50], is often a concern in the design of ubiquitous computing environments more generally [6, 28, 29, 43], as well for smart homes in particular.

Prior work has explored in-home privacy from third parties such as device manufacturers, advertisers, and the government [4, 12, 59, 60], as well as the effects of home surveillance by researchers [42]. Choe et al. (2011) surveyed what moments in a home that people would not want recorded [17], but did not make explicit who might have access to recordings. In our work, we explicitly study interpersonal privacy between household members in a smart home, rather than from external parties.

Personal data monitoring within households raised concerns even before contemporary smart home devices [16]. Choe et al. (2012) studied when and why people would want motion, electrical, and video sensing in the home, and surfaced tensions between couples, between parents and children, and between households and visitors [18]; they found that couples were concerned about recordings in case of divorce, and that parents had internal conflicts over telling their children about recording and wanting to be able to watch them. This study used functionless probes and dates to when smart home devices were not yet mainstream; our work updates our understanding of contemporary smart devices deployed organically (i.e., not for research purposes).

Privacy concerns beget access control questions: how should data and device access be controlled among household members? Earlier work on personal data sharing and access control in homes studied digital devices meant not for controlling physical space, but for file storage (such as computers, mobile phones, and music players) [35, 36], whereas more recent work has considered access control for users of smart home devices (e.g. [54]). He et al. (2018) found that multi-user smart home consumers would prefer control at function-level granularity rather than per-device access control [25]. Smart home devices differ significantly from earlier digital devices shared among household members: they sense

and control physical space but often lack screens, making it difficult to rely on traditional interactions for indicating privacy [33] or to use visualizations for supporting awareness [32].

The tension of parents wanting to monitor their children while also respecting their privacy appears in parenting technology research more generally (e.g., [21, 55]); prior work has also studied the privacy and other concerns around home technologies for older adults (e.g., [23, 53]). Smart home devices in shared physical spaces will further press on these issues for both populations. Finally, Hoyle et al. (2014) also considered privacy for incidental users who pass through a device's physical space, rather than device owners, in the context of life-logging cameras [29]; similar issues may arise for people in smart homes.

3 METHODS

Our study consisted of three components. First, we conducted a semi-structured interview that lasted between 15 and 60 minutes (varying based on how many devices the participant owned); second, if participants chose to continue the study, we collected three weeks of experience sampling data; third, we conducted a semi-structured exit interview. Interviews were conducted in-person on our university campus or by video call. The study protocol was approved by our institution's human subjects review board (IRB).

Procedures

During the initial semi-structured interview, we asked questions about which smart devices our participants had, how they used them, who installed the devices, and whether any tensions had arisen between them and other people who lived or came into the home. We also asked if participants had ever learned anything surprising about their co-occupants through the smart devices or vice versa. To avoid priming participants, we avoided using the word "privacy" explicitly unless a participant brought it up first.

We then collected three weeks of experience sampling data via a smartphone application that we developed for Android and iOS based on an open source template [52]. We asked participants to use the app to log any experiences that they considered a "tension" in their house with another person related to a smart device. These incident logs were submitted to the research team. The app reminded participants about the study every three days. We used experience sampling, rather than asking participants only to recall past incidents during the interviews, in the hopes that participants would provide more logs and more accurate details logging the events as they occurred [19].

At the end of the three-week experience sampling period, we conducted an exit interview with participants to ask follow-up questions about incidents that were logged. Participants were initially paid $20 for the initial interview, $7 per week of logging (regardless of the number of logs submitted), and $20 for the exit interview. After calibrating during the first several participants based on how much time the interviews and logging activities actually took, we adjusted compensation to $20, $3 per week, and $10 respectively for each study component, in consultation with our IRB.

Recruitment

We recruited subjects by sending recruitment flyers electronically through online communities interested in smart homes, through personal networks on social media, and through local high schools. We also posted physical flyers around a university. Interested participants were directed to fill out an online survey, which we used to collect information about which smart home devices they use or want to use, as well as their comfort level with technology.

Participants

Table 1 summarizes our 18 participants (4 female, 14 male), who range in age from 17-44 and all live in a home with smart devices and share the home with at least one other person. P15 lives in Australia; everyone else lives in the United States from various states. All participants come from different households. All 18 participants completed the initial interview, 14 participants completed the experience sampling section (Table 1 lists how many logs each person submitted), and 11 participants completed all three sections. In our results, we will use the term "smart home driver" to refer to participants who instigate using smart home technology (primarily through installation) and the term "passive user" to refer to people less involved in smart home decision making. These terms are adapted from the smart home roles introduced in previous studies; they are not meant as value judgments, but as a categorical convenience [37, 44].

Our participants represent a variety of co-habiting situations (with a partner or spouse, with roommates, with children, with parents). Specifically, three participants were college students who lived with roommates; 14 participants lived with their partner and/or other family members; one participant is an adolescent. We aimed for variety in household relationships, but found it difficult to recruit a larger number of households with adolescents or roommates. We also found it difficult to recruit more passive users (perhaps in part due to recruiting from smart home enthusiast forums). We were unsuccessful at recruiting other (passive) household members of our smart home driver participants.

Data Analysis

From the 14 participants who completed the three weeks of experience sampling, we received 46 logs, at an average of 3.3

	Gender	Age	House Members	# of Logs	Smart Home Role	# Device Types
P1	Male	26	Girlfriend	3	Driver	19
P2	Male	37	Mother	2	Driver	3
P3	Female	24	Boyfriend	0	Driver	1
P4	Male	34	Girlfriend	9	Driver	15
P5	Male	23	3 Roommates	3	Passive User	3
P6	Male	38	Wife, daughter, son	9	Driver	13
P7	Female	38	Husband, 2 daughters	1	Driver	11
P8	Male	29	Wife, daughter	N/A	Driver	6
P9	Male	33	Wife, daughter	3	Driver	10
P10	Male	17	Mother, father, sister	N/A	Driver	1
P11	Female	24	2 Roommates	N/A	Driver	2
P12	Male	43	Wife, son, daughter	3	Driver	6
P13	Female	20	7 Roommates	1	Passive User	1
P14	Male	30	Wife	1	Driver	6
P15	Male	44	Girlfriend stays over part-time	4	Driver	6
P16	Male	34	Wife, 2 children	3	Driver	6
P17	Male	37	Wife, daughter	4	Driver	6
P18	Male	29	Wife	N/A	Driver	8

Table 1: Study Participants: We detail participant demographics, how many experience logs they submitted during our study, their role in the smart home, how many types of devices they reported having. "Type" here refers to the kind and brand of device, not an individual unit (e.g., owning two same-brand smart bulbs is classified as "one type").

logs per person. The number of logs per person ranged from 0 to 9. Most logs pertained to issues that arose involving a device and more than one person, and we used these entries as discussion points during exit interviews. Some logs described technical issues that only affected the logger. People who owned more smart devices tended to submit more logs.

We transcribed the audio recordings of the interviews, and we took an inductive approach to coding the transcripts and logs. Two researchers read several interviews, developed codes, compared them, and then iterated again with more interviews until we had developed a consistent codebook. The final codebook consisted of 35 codes in total. Then each researcher coded half of the interviews, frequently checking in with each other whether any codes needed to be added or changed. After all interviews had been coded, both researchers spot-checked the others' coded transcripts and did not note any inconsistencies. Finally, we further organized and taxonomized our codes into higher-level categories.

4 RESULTS

From our interview and experience sampling data, we identified several chronological points during smart home implementation and usage when significant multi-user interactions or tensions arose (Figure 1): (1) device selection and installation, (2) regular device usage, (3) when things go wrong, and (4) over the long-term, as changes occur in the home. We organize our results according to this timeline.

Device Selection and Installation

We begin by considering how participants and their co-occupants select and install new smart devices in their homes. 15 of the 18 participants had personally installed at least one device in the home. 14 of these participants were the *only* occupants in the home who had installed these devices.

Device Installation Decisions. Some smart home driver participants explicitly consulted with their co-occupants over which smart devices to get: P8, P18 and P7 all consulted with their partners, reporting that their partners were also interested in the devices. P7 qualified this, reporting that the main reason to consult each other was if the device was expensive.

Other participants selected devices independently but anticipated co-occupant's concerns. For example, P16 lives with his wife and children, and he is aware of his wife's concerns. Initially, "I didn't really ask, I started installing them, but then my wife [said] some of them are kind of ugly and unsightly so you have to find different ways to place them." After learning about her preferences for aesthetics as well as functionality, he was better able to decide what to purchase.

Finally, many participants explicitly did not consult with co-occupants about the decision to install smart devices. Participants who did not consult their co-occupants often discussed the other person's disinterest or passivity with respect to smart devices. For example, P1, P6, P9, P14, and P17 all said they were interested in devices while their partners

were not. P1, when asked about whether he would be the only person making changes or additions to the smart home, said, "[My partner is] a passive person, she doesn't care that much about it, it's definitely me all the way."

Sometimes the passivity of co-occupants changed after the first devices were installed. For example, when P6 was asked if there were disagreements with his partner upon installation he said, "No. She...wasn't too interested. Now that she's seen usefulness, she likes it better." P9's partner had a different experience: "[My wife] was sort of indifferent to [the smart home] when it first started, and then I started expanding it...I think she doesn't necessarily like having all these gadgets...[but] I don't think it's that big of a deal to her." P9's wife does not whole-heartedly like the smart home.

In other cases, smart home drivers did not consult co-occupants because they did not consider them equal decision-makers in the home. P2, whose mother lives with him, said he did not consult her because it is his house, and if he shared the house with an equal partner, he would consult them first (though his mother eventually grew accustomed to the smart devices). P15's partner spends several nights a week at his place but does not live there, and P15 did not consult her about installing Hue lights with a timer and motion sensors.

Account Management. The process of installing smart home devices or platforms often involves creating new accounts, or linking devices to existing accounts. Several participants created separate accounts for people in their home because the service in question made it easy to do. P9, who owns a Google Home and Nest products, set up separate accounts for himself, his wife, and his daughter, as they are all using Google accounts. Once the separate accounts were set up, P9 appreciated the privacy it provided: "I like to just have the stuff separate. So, [my wife] can sign out of it and have sort of her own privacy with it."

In other cases, service providers did not make it easy to create multiple accounts. P12 mentioned that Ecobee (thermostat) did not have an option to allow his wife to set up her own account. By contrast, he was able to do so with Ring (doorbell): "It was a lot easier for her to set up an account [with Ring], so I prefer to do it that way."

Frequently, the use of a single account reflected the disproportionate control or interest of the device's installer. For example, P17's wife uses his account for their Apple Home, and his wife "thinks it's cool and all that, but she's not as motivated to do it." For P5, P11, and P13 who live with roommates, the account for the device was solely the account of the person who bought the device. For most other participants, they had installed the device and so they had their co-occupants share their account.

Some participants shared accounts for other reasons. For instance, P3 described a relationship dynamic in which many things are shared: "My boyfriend and I have each other on Google Maps so we track each other anyway. You can do location sharing permanently. We share everything, [including an] Amazon Prime account. So it makes sense to share the Alexa. Our fingerprints open up each other phones. We're pretty transparent."

Regular Device Usage

After devices are selected and installed, they are integrated into home life. Our data revealed a number of multi-user issues that arise during ordinary use of installed devices.

Agency of Installer. First, we observed the smart home driver having outsized control over smart device data and functionality, as compared to other home occupants. This situation often arose by *default*, as an extension of the installer's agency around device selection and installation in the first place (described above). Other occupants sometimes have less interest in the devices, limited technical ability to control them, or both. For example, P4 says about his girlfriend, who moved in after he started setting up his smart home: "[She says] 'I don't know what I'm doing [with smart devices],' and I try to teach her, but I don't think she wants to know."

When only the device installer has access to the device's account, functionality is limited to this user by default. For example, P10, who lives with his parents and sister, owns a Microsoft Invoke, which is connected to his Microsoft account. Only he has access to the history of voice command searches made with the device.

In other instances, the device installer *purposely* limited access to certain functions. For example, P6 added his 8-year old daughter as a secondary user in the Apple Home app, which centralized control of smart devices. By adding her as a secondary user, P6 prevented her from taking administrative actions like deleting a device.

Information Sharing and Privacy. Unlike traditional homes, smart homes collect significant amounts of data about their occupants, including voice recordings, browsing history, door opening, and other usage data [20, 26, 51], as well as access to potentially sensitive data such as emails [20]. This data is often surfaced to the users of the smart devices; for example, devices like the Amazon Echo allow users to see a history of commands and replay the voice recordings. Going into our study, we asked: Are people who regularly use these devices aware that this data is collected and accessible to co-occupants? Are they concerned or bothered by this?

We found that several installers, including P9, P12, and P16, were aware of the information that their smart devices collected from the whole house. P9 was neither surprised nor particularly concerned: "I can track everything that the Google Home hears through their app...The only thing I do [think] that is a little weird is that the Google Home will,

every now and then, just turn on 'cause I think it thinks that somebody's saying the hot word....but it doesn't really tell anybody any of my information that I'm worried about getting out."

P12 was also not surprised, but his wife "was surprised at how much...[Google Home] actually kept. And that you could go back and see...what you requested..." Despite this, his wife was not concerned: "You know, now she's just aware that...because she's the parent she has access to the kids' [record, which she likes], but unless you know she has access to another person's account, you know she won't be able to see it. It's private between you and Google." His wife trusts him and, by transitivity of his trust, trusts Google with the information collected by the device, and appreciates the access it provides to her children's information. P17 also liked the increase in available information afforded by the installed devices. He said, "The weird thing now is we know whenever somebody comes or leaves, because you get a door open notification... I sort of like it. [My partner] hasn't commented on it, but usually it's just the two of us, so it's just nice to know the other person is home."

By contrast, P5 was surprised when his roommate, who owns the Google Home, replayed the history of voice commands to all of their roommates. Afterwards P5 stated that "we got to know that [device owner] records our voices." In this instance, P5 was also ultimately not concerned: "It's super hilarious. We wanted to hear our voices being played."

One exception to lack of concern came from P6, who anticipated the concerns of another family member, his now 8-year-old daughter. When asked when he removed the internet-connected baby camera, P6 said they "stopped using it by default.... when she was two. But not because, we would have used it longer, but because of [moving to a different city and moving it to our son's room]. She deserves some privacy too. So we probably would have stopped maybe around [age] 5ish?" His child's personal privacy was a concern for him, although it was not the explicit reason why he removed the camera in this case.

Instead of concerns about interpersonal privacy, we heard more concerns about privacy with respect to the companies collecting the data. P14 and P15 both run their smart devices on a local server so that their data doesn't go to a third-party server owned by the device company. P16 stated, "I think for a while we turned Alexa off, because it was just listening all the time and so if we're not getting enough value from home automation, we'll probably turn her off."

Preferences for Analog Devices. Even after smart home integration, we found that people often used or set up analog controls of devices as a backup. For example, P4 mentioned that his girlfriend "likes light switches. The way [the smart home is] set up, you have to leave the light switches off. So I taped over the light switches. Infuriated her." P4 stated that his girlfriend adjusted to it after about a year, after she learned she could control the fan as well as the lights using voice commands.

P9 and P15 both installed analog controls as an alternate control system in addition to motion sensor lights and voice command lights. P9 states, "My wife's a little old school, which is why I installed the light switches and not the bulbs, because she's still very manual, and so she just likes to turn the lights on and off." Analog controls worked except in the case of P6's 3 year old son: he is too short to reach the lights switches, but he also doesn't know the correct wake word to get the Amazon Echo to change the lights.

Playful Behavior. Our data contains a number of cases where smart device use was a source for fun, joking, or accidental laughs among co-occupants. For example, P2 logged that he "laughed when my mom gave her command before I did," when they were both trying to get his Amazon Echo to do something. The two of them have had several light-hearted standoffs attempting to gain control of the Echo, which were resolved by whoever stayed in the room the longest ultimately gaining control. In addition, one of P5's roommates has a Philips Hue Light Strip installed in his room, which is connected to the Google Home. P5 reported that he and his other roommates would sometimes turn off that roommate's lights for fun. In response, "he either comes down, or doesn't care." As a final example, P12's 10-year old daughter will, if he's not at home, "ring the [smart] doorbell and try to get me to answer it [remotely on my phone]."

A few additional instances were still lighthearted but began to hint at sources of possible conflict. When P14 had guests over, they tried to use Amazon Echo voice commands to place orders from Amazon. P14 was annoyed about that, but had the ordering functionality disabled. And when P15's installation of proximity-sensing lights didn't work for his girlfriend's phone, he said she reacted, "'Haha told you it wouldn't work.' It's a little bit annoying but nothing serious." Trust likely plays a factor in the ability of people sharing devices to playfully interact; in this case his girlfriend trusts him to get the device to work eventually.

Though these instances of playful behavior were just that—playful—they suggest potential ways in which co-occupants can come into conflict over smart devices.

When Things Go Wrong

We now turn to what happens when "things go wrong"—when conflicts or tensions arise between people in a smart home, or how people interact when devices do not work as expected or intended.

Tensions and Conflicts Between People. We begin by considering conflicts and tensions that occur when devices work

correctly (i.e., as intended by the manufacturer, designer, and/or device installer) but come up against mismatches in expectations or desires between different people in the home.

Partners. An example of tension between partners occurred when P4 and his girlfriend had disagreements about their cleaning lady's access to the house. P4 stated, "I didn't want to give out our [door lock] code... One of the times she gave the cleaning person her code. I said I really don't like that because I've kind of set up these codes so that we have access to it, but we can take it away. This is like having a key, the way you get your key back is just delete the code. We had a discussion about in the future don't give out the code... 'Cause this is my whole grand idea of the smart house." Part of the source of this tension may have been the fact that P4 is also the only one in the house with the knowledge for adjusting the smart devices, so his girlfriend may not have been able to create a new access code without his help.

P1 is also the sole smart home driver in his home with device knowledge, leading to tension with his partner who cannot change device controls. P1 logged that his girlfriend was annoyed she could not use the voice command "turn off TV" to turn off the TV, since P1 has Apple, Chromecast, and Fire TV, each requiring a specific command, e.g., "turn off Fire TV". In response, P1 set the general command to default to controlling Chromecast.

Roommates. We also observed tensions between roommates, who have a different type of relationship. Between roommates, there is often one person to whom the device belongs, and there is less of an assumption of shared access and control rights as there may be between partners.

For example, P11, a college student, has a Nest Thermostat installed by her landlord in her apartment, where she lives with another student and a young professional. P11 took over use of the thermostat from the previous tenants and is the only one in the house who has the Nest app on her phone. P11 prefers a warmer temperature, while her roommate does not like when the air gets too dry. P11 says, "So sometimes [my roommate] will turn off the thermostat before she goes to bed and then I will pull up [the Nest app on] my phone [and] turn it back on. She knows that though." As to why her roommate does not also get the Nest app, P11 posits that the thermostat is physically close to her roommate's room and she can just change it manually. "We're not like super strict about how the temperature should be, so we never fight or feel uncomfortable with this temperature thing."

P13 is another college student who lives with roommates. One of her roommates owns an Amazon Dot, which the roommates use to play music, ask questions, and other functions. While P13 would say that everyone has equal access to the Dot, "we also know that this device belongs to one person, so if for some reason she's using it, obviously she has priority over everyone else [using it] because she's the one that paid for it." These roommates resolve conflicts by deferring to the default control and agency of the device's installer or owner, a recurring theme in our findings.

P10, a teenager living with his parents and 13-year old sister, has also experienced tension: his sister sometimes uses physical control of a smart device as leverage in a conflict. For example, P10 reports: "I was like five minutes late to pick her up from school or something, and she gets a little bit mad about that. Then, she'll try to take away the smart device so it's hers." However, she cannot use it because P10 will remotely lock the device, since it is connected to his account. "She gives it back, of course." In this case, control of the device requires more than just physical control.

Parents and Children. As conflicts naturally arise in parent-child relationships, conflicts also arise around the use of smart devices in the home. For example, we heard about parents and children competing for control over the Amazon Echo. In addition to the playful competition between P2 and his mother (discussed above), P16 has also vied with his 5-year old and 3-year old child for control of the music selection via the Echo at the dinner table. "Their favorite songs now are like the Pokemon theme song and 'What Did The Fox Say?'...so they'll just yell at Alexa and be like, turn it up to volume ten and let's go for it.... sometimes we would turn it back... I guess if we got really frustrated we would actually mute Alexa, so she wouldn't take any more commands during dinner."

Some parents explicitly used smart devices as parenting tools for setting limits or managing schedules, a recurring theme in smart home literature [57]. P10's father uses the Microsoft Invoke to add chores to P10's calendar, which the Invoke will verbally remind him to do. "He just sets reminders for us, which is kind of annoying, but what are you going to do?" Also, P9 installed an LED smart light and a Google Home Mini in his 4-year old daughter's room because she didn't like her room too dark, and P9 automated it to gradually turn off to signal to his daughter when it is time for bed. However, this scared her because, "she feels she has no control over how it behaves... She doesn't like it in her room. She won't talk to it ever." This incident led his daughter to be uncomfortable with smart devices, as she is afraid of their behavior she cannot predict; she refused to keep a Google Mini in her room because of its blinking lights.

Guests and Non-Occupants. Participants reported a number of cases in which guests or other people entered their homes and interacted with the smart devices, sometimes leading to conflicts or tensions. For example, P5's roommate owns the house's Google Home. This roommate was annoyed when P5's sister stayed over and used the Spotify account he had connected to his Google Home to play music that he did

not like, since it changed future Spotify recommendations for him. In this case, guests having equal access to functionality led to consequences for the device owner.

When Devices Malfunction. Conflicts or tensions also arose when devices malfunctioned, either through a technical failure or by not working as the installer intended (e.g., because a smart home automation was improperly programmed). For example, a timer for a heater wouldn't go off, or a smart lock wouldn't register that someone's phone was in the vicinity. In this section, we consider how co-occupants interact in these cases.

First, we often observed that other home occupants were reliant on the smart home driver to fix the issue (in the meantime manually controlling the device by analog means, if possible). For example, P15 tried to set his heater to turn on automatically when he or his girlfriend were at his home. When it did not work, it fell on P15 to fix the issue, while they used manual controls in the meantime. Since smart devices may represent critical home infrastructure—including lights, temperature, locks, heaters, and other appliances that use electricity—relying on the smart home driver to fix these devices when there are no backup analog controls may put other home occupants in adverse situations. This is particularly the case with DIY smart homes, which may be less reliable than traditional homes where the critical infrastructure is set up and wired by external experts (e.g., electricians).

We also heard frequent complaints about smart device voice commands not working as intended, particularly for less experienced or savvy users. For example, P6's 8-year old daughter "asked Alexa to turn on 'bedroom' light. Being that there are multiple 'bedrooms' set up in my home automation system, if there is a general request as in 'turn on bedroom light', Alexa should ask for clarification as to what bedroom the user is referring to." P6's suggestion hints at a way that smart devices could be redesigned to help guide less experienced people to use them more independently without relying on intervention from the smart home driver.

In other cases, even the smart home driver could not fix a fundamental issue. For example, P6's smart light setup relies on the smart home knowing someone is home. Because P6's children didn't have their own phone at the time, the house failed to recognize they were around: "My wife and I were out...[our phones] outside the geofence, but my kids and the babysitter were still at home. So [the lights] thought we were away... And for whatever reason, the motion didn't pick up that they were there." Asked when he would get his children their own smart phones, P6 said: "Probably around maybe 14 to 15, somewhere around there." Until then, the smart home may not be fully functional for P6's children, putting the intended functionality of the smart home at odds with P6's parenting choices around smart phone ownership.

Long-Term Use: Changes in the Home

Finally, our results surface how relationships between people and with smart devices may change over time.

Children Grow Up. Several participants mentioned changing their smart device interactions as their children grow older. For example, P6 has a Ring doorbell which sends a notification to his and to his wife's phone when someone is at the door. When his children are older, he plans to buy an additional smart door lock so he can give his child a unique access code which will open the door and also notify P6 who opened the door. Recall also P6, discussed above, who noted that while his daughter's baby monitor camera was removed when they moved, he would have still removed it "maybe around [age] 5ish" because "she deserves some privacy too."

Occupants Change. Occupants of a home may change over time, though the smart devices installed in that physical space may stay behind. What does this mean for the configurations of these devices, as well as the potentially private data they store and make accessible? For example, when P11 moved into her apartment, she noticed that the landlord had installed a Nest Thermostat, and the previous tenant had not deleted their old account from the device; P11 deleted the account to connect the Thermostat to her own account.

In another case, a participant discussed theoretically what he would do if he moved out of his home in the future: he planned to leave his smart devices behind, viewing them as intentionally integrated with the specific physical space rather than personal devices he would take with him: "[all these devices] I'd think I'd leave, 'cause hopefully they'd be useful to other people."

5 DISCUSSION

We now step back to consider the broader issues raised by our findings for multi-user smart homes, and we make recommendations for smart home designs and future research.

Differing Agency For Smart Device Access

A major theme throughout our results are the differences in power, agency, technical skill, and technical interest among different people living in a smart home. There is often a smart home driver who takes initiative to learn about and use devices, and passive users who adapt to devices and/or rely on smart home drivers to make changes. Practically speaking, this means smart home drivers often have access to vastly more functionality (including the ability to set permissions for functions co-occupants can use) and more information (such as knowing when someone opens and closes a smart-locked door) than passive users. Our findings reinforce and expand upon those from prior work [8, 37, 59], and we observe that this dynamic is becoming increasingly concerning

for technology-enabled abuse [7] as commonly deployed smart home devices expand from thermostats and lights to more security- and privacy-sensitive devices like digital assistants, smart locks, and smart door bells.

In some cases, this power difference simply reflects existing power dynamics in co-occupant relationships (such as parent and child). In other cases, the inclusion of technology can exacerbate these dynamics or allow for increased control or abuse by the smart home driver. For example, smart homes allow remote access to important household resources such as lights, heating, and door locks, breaking the assumption in a "dumb" home that physical access to a device allows—and is necessary—for controlling it. Likewise, managing a smart home requires some technical ability, which may widen the gap between people in the home when something goes wrong (e.g., a device malfunctions or the network goes down).

Limited Concern in Our Sample. In our study, we found that none of our participants expressed particular concern over these power differences, nor about issues related to interpersonal privacy. We see several possible reasons for this lack of concern. First, we interviewed people who reported being in stable, generally trusting relationships; other work has highlighted the importance of considering the role of smart home technology in cases of domestic abuse and intimate partner violence [7, 13, 34]. Second, our participants may have incorrect or incomplete mental models about the data collected by or accessible via smart devices and what private information is implied by this data [27, 59]. Finally, most of our participants are smart home drivers; other passive users may have different thoughts on this dynamic.

Gender Differences. We observe that the majority of smart home drivers that we interviewed were men. These drivers frequently had female partners who were (claimed to be) passive users. A similar gender dynamic was reported in an older paper by Mennicken et al. (2012) [37]. Though we cannot generalize this dynamic to the entire smart home user population, in light of gender differences in other technology domains (e.g. software usage [9, 10, 47], ambient belonging [14, 40], and domestic technology [15, 46]), we suggest that future work (1) explicitly study the role of gender in smart homes, (2) situate these findings in the broader study of gender, domesticity, and technology, and (3) develop designs to make smart devices more accessible to a diverse population.

Design Recommendations

Design to Minimize Power Differences. Smart home technology designs can and should take a role in minimizing the power differences among users in the home.

Analog Control. While automation and remote control are great benefits of smart devices, this functionality is often not available to co-occupants who do not have phones, who prefer analog control, or who are dealing with an Internet or other failure. When a device stops working (as in Section 4), passive users who do not know how to troubleshoot the issue have to rely on either the smart home driver or analog controls (if available). Smart device manufacturers should thus recognize the important of backwards compatibility and design for it as much as possible. For example, smart devices should include easy-to-use mechanical switches and controls, at least for basic features (e.g., turning lights on and off). Smart outlets could perhaps alert users (via sound or light) attempting to manually control devices plugged into it when the smart outlet is off (and thus power is, perhaps unexpectedly, not flowing to the device).

Account Creation. Smart home designers should support users in considering the entire household in the account creation process. For example, when on-boarding a new installer, smart home related applications should ask if there are other people in the home and streamline the process for their device access as well. The Nest app already does so, and we recommend that other companies follow. At the same time, developers should aim to require the minimum possible prerequisites for users to engage with their smart devices and applications. For example, we note that Apple Home requires users to have iCloud accounts and iOS 11.2 or later (i.e., iPhone 5 or later) [3], which may be a barrier for users with older devices.

Consider Different Relationship Types. More generally, designers should consider the variety of relationships that may exist between smart home installers or driver and other occupants, or in non-traditional home units, including partners, roommates, children and parents, older adults, landlords and tenants, people in potentially abusive relationships, etc.

For example, consider a landlord who installs smart devices in a renter's apartment. What kind of control should tenants have over whether and what data is collected via these devices, the remote access by the landlord, and whether smart devices are installed at all? Some of these questions may be legal questions, but smart home device designers should consider them as well—e.g., considering how a "tenant mode" might differ from an "owner mode".

Smart homes also affect *non*-occupants of the home, including household employees (e.g., childcare providers, cleaners, and tradespeople) and guests. Designers should consider possible interactions with these people, who may need temporary access to devices or have privacy concerns, or from whom occupants may wish to protect their own privacy. For example, with devices that collect information for future use, such as Spotify through a voice assistant, a visitor mode

could allow guests to use the device but not record their command and music history, supporting both owner music recommendations and non-occupant privacy.

Designing for Long-Term Changes. As smart home devices become more widely adopted, we may expect that they become long-term fixtures in people's homes , and we urge smart home designers to consider the long-term use of their devices and platforms.

Occupants Changing. Some smart home fixtures may remain physically with a home when people move, such as smart outlets or thermostats. Since many people move, these devices should have built in functionality that allows old accounts and data to be easily deleted or migrated.

Some devices, such as the Nest and Ecobee thermostats, already have this functionality, and we recommend that other devices follow their lead. However, we note that one of our participants reported finding a previous tenant's account still connected to the Nest thermostat, suggesting that the usability or discoverability of this function could still be improved. For example, a possible solution with improved usability might involve smart devices automatically detecting changes that suggest a new tenant and prompting them locally—or the previous user remotely, e.g., via email—to reset the device and delete old data and accounts.

Handling occupant or other relationship changes correctly in general may be challenging, and designers should consider the full range of possible circumstances. For example, consider the August smart lock. To reset it, one must submit proof of purchase and the lock serial number to the company, who will contact the old owner to validate that the reset was intended. While this design choice prevents an attacker from resetting a lock to gain access to the home, it can also raise security concerns when the former owner *is* an adversary who may wish to prevent the lock from being reset (e.g., a former spouse in an abusive relationship).

Relationships Changing. Even if the occupants of a smart home do not change, the relationships between the people living there might change over time. For example, as children grow up, the changes in parent-child relationships can significantly impact smart home interactions and may require fundamental changes to how the smart home is setup and managed. While some prior work brings up the importance of designing devices for seasonal changes in a child's life [22], we want to call attention to how the change in trust and power between a parent and child might affect smart device usage as people grow older.

6 LIMITATIONS AND FUTURE WORK

A major limitation of our study is that all except two of our participants were smart home drivers. Thus, while we can report on the perspectives of smart home drivers, our results do not fully reflect the experiences of passive users, who may have additional or more serious concerns than those raised in our interviews. For example, the lack of passive users in our sample may explain the limited concern about privacy or power imbalances in our findings. We advocate that future work study (1) passive users in significantly more depth to understand their perspectives, and (2) how to better engage and provide information to passive users, should they need or want to use smart devices.

Future work should also consider the concerns of children in smart homes, as well as how interactions with smart homes change over a longer period of time than a few weeks. For example, at what age do children gain the agency to have a say on smart devices in their personal spaces? What will be the longer-term privacy perceptions of children who grow up in smart homes surrounded by devices like cameras and digital assistants?

We also recommend that future work focus on designing and evaluating the technologies themselves: for example, evaluating the usability and discoverability of important device functions, such as account and data deletion and resetting (e.g., for when a new tenant moves in).

7 CONCLUSION

As smart devices move beyond early adopters and become integrated into the longer-term infrastructure of users' homes, we must critically consider how these technologies interact with complex and changing human relationships. We conducted a mixed-method qualitative study of interactions and tensions that occur between people sharing a smart home.

Our results paint a picture of households where smart home use reflects existing relationship dynamics and power structures in homes (e.g. parent and child), and use that creates power imbalances; smart home drivers tend to have more access to functionality and data than passive users. We make recommendations for designers and researchers to help minimize these differences between co-occupants, to consider different relationship types, and to design for long-term use as children grow up and people move.

ACKNOWLEDGEMENTS

We are grateful to Tal August, Audrey Desjardins, Lucy Simko, and Eric Zeng, as well as to our anonymous reviewers, for their feedback on earlier versions of this paper.. This work was supported in part by the National Science Foundation under Award CNS-1513584.

REFERENCES

[1] 2017. Multiple users - can they all see each other? Retrieved 2018-08-20 from https://community.smartthings.com/t/multiple-users-can-they-all-see-each-other/102723

[2] Amazon. 2018. Echo & Alexa Devices. Retrieved 2018-08-31 from https://www.amazon.com/b?&node=9818047011&ref=ODS_v2_FS_AUCC_category

[3] Apple. 2018. Use the Home app on your iPhone, iPad, and iPod touch. Retrieved 2018-08-30 from https://support.apple.com/en-us/HT204893

[4] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2, Article 59 (July 2018), 23 pages. https://doi.org/10.1145/3214262

[5] Genevieve Bell and Paul Dourish. 2007. Yesterday's Tomorrows: Notes on Ubiquitous Computing's Dominant Vision. *Personal Ubiquitous Computing* 11, 2 (Jan. 2007), 133–143. https://doi.org/10.1007/s00779-006-0071-x

[6] Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third Conference on European Conference on Computer-Supported Cooperative Work (ECSCW'93)*. Kluwer Academic Publishers, Norwell, MA, USA, 77–92. http://dl.acm.org/citation.cfm?id=1241934.1241940

[7] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. Retrieved 2018-08-23 from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

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

[9] Margaret Burnett, Anicia Peters, Charles Hill, and Noha Elarief. 2016. Finding Gender-Inclusiveness Software Issues with GenderMag: A Field Investigation. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2586–2598. https://doi.org/10.1145/2858036.2858274

[10] Margaret M. Burnett, Laura Beckwith, Susan Wiedenbeck, Scott D. Fleming, Jill Cao, Thomas H. Park, Valentina Grigoreanu, and Kyle Rector. 2011. Gender Pluralism in Problem-solving Software. *Interact. Comput.* 23, 5 (Sept. 2011), 450–460. https://doi.org/10.1016/j.intcom.2011.06.004

[11] Marta E. Cecchinato and Daniel Harrison. 2017. Degrees of Agency in Owners & Users of Home IoT devices. *Making Home: Asserting Agency in the Age of IoT workshop in CHI '17* (2017).

[12] Pew Research Center. 2016. Privacy and Information Sharing Report. Retrieved 2018-08-22 from http://www.pewinternet.org/2016/01/14/scenario-home-activities-comfort-and-data-capture/

[13] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. *Proceedings of the IEEE Symposium on Security and Privacy* (2018), 441–458.

[14] Sapna Cheryan, Andrew N. Meltzoff, and Saenam Kim. 2011. Classrooms matter: The design of virtual classrooms influences gender disparities in computer science classes. *Computers & Education* 57, 2 (2011), 1825 – 1835. https://doi.org/10.1016/j.compedu.2011.02.004

[15] Noelle Chesley. 2006. Families in a High-Tech Age: Technology Usage Patterns, Work and Family Correlates, and Gender. *Journal of Family Issues* 27, 5 (2006), 587–608. https://doi.org/10.1177/0192513X05285187 arXiv:https://doi.org/10.1177/0192513X05285187

[16] Marshini Chetty, Richard Banks, Richard Harper, Tim Regan, Abigail Sellen, Christos Gkantsidis, Thomas Karagiannis, and Peter Key. 2010. Who's Hogging the Bandwidth: The Consequences of Revealing the Invisible in the Home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 659–668. https://doi.org/10.1145/1753326.1753423

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

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

[19] Sunny Consolvo and Miriam Walker. 2003. Using the Experience Sampling Method to Evaluate Ubicomp Applications. *IEEE Pervasive Computing* 2, 2 (April 2003), 24–31. https://doi.org/10.1109/MPRV.2003.1203750

[20] M. Courtney. 2017. Careless talk costs privacy [Censorship Digital Assistants]. *Engineering Technology* 12, 10 (November 2017), 50–53. https://doi.org/10.1049/et.2017.1005

[21] Alexei Czeskis, Ivayla Dermendjieva, Hussein Yapit, Alan Borning, Batya Friedman, Brian Gill, and Tadayoshi Kohno. 2010. Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-teen Mobile Safety. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 15, 15 pages. https://doi.org/10.1145/1837110.1837130

[22] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K. Dey. 2006. Principles of Smart Home Control. In *Proceedings of the 8th International Conference on Ubiquitous Computing (UbiComp'06)*. Springer-Verlag, Berlin, Heidelberg, 19–34. https://doi.org/10.1007/11853565_2

[23] George Demiris and Brian K. Hensel. 2008. Technologies for an aging society: A systematic review of "smart home" applications. *Yearbook of Medical Informatics* (2008), 33–40.

[24] Google. 2018. Google Home - Smart Speaker & Home Assistant. Retrieved 2018-08-31 from https://store.google.com/us/product/google_home

[25] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[26] Kashmir Hill and Surya Mattu. 2018. The House That Spied on Me. Retrieved 2018-08-22 from https://gizmodo.com/the-house-that-spied-on-me-1822429852

[27] Jason Hong. 2016. Toward a Safe and Secure Internet of Things. June (2016). Retrieved 2018-08-31 from https://www.newamerica.org/cybersecurity-initiative/policy-papers/toward-a-safe-and-secure-internet-of-things/

[28] Jason I. Hong and James A. Landay. 2004. An Architecture for Privacy-sensitive Ubiquitous Computing. In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys '04)*. ACM, New York, NY, USA, 177–189. https://doi.org/10.1145/990064.990087

[29] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 571–582. https://doi.org/10.1145/2632048.2632079

[30] Philips Hue. 2018. Light your home smarter. Retrieved 2018-08-30 from https://www2.meethue.com/en-us

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

[32] 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 (CHI '17)*. ACM, New York, NY, USA, 1620–1633. https://doi.org/10.1145/3025453.3025799

[33] Meg Leta Jones. 2015. Privacy Without Screens & the Internet of Other People's Things. *Idaho Law Review* (2015). https://ssrn.com/abstract=2614066

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

[35] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. 2010. Access Control for Home Data Sharing: Attitudes, Needs and Practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 645–654. https://doi.org/10.1145/1753326.1753421

[36] Michelle L. Mazurek, Peter F. Klemperer, Richard Shay, Hassan Takabi, Lujo Bauer, and Lorrie Faith Cranor. 2011. Exploring Reactive Access Control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2085–2094. https://doi.org/10.1145/1978942.1979245

[37] Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them. In *Pervasive Computing*, Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 143–160.

[38] Sarah Mennicken, Amy Hwang, Rayoung Yang, Jesse Hoey, Alex Mihailidis, and Elaine M. Huang. 2015. Smart for Life: Designing Smart Home Technologies That Evolve with Users. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 2377–2380. https://doi.org/10.1145/2702613.2702631

[39] Sarah Mennicken, Jo Vermeulen, and Elaine M. Huang. 2014. From Today's Augmented Houses to Tomorrow's Smart Homes: New Directions for Home Automation Research. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 105–115. https://doi.org/10.1145/2632048.2636076

[40] Danaë Metaxa-Kakavouli, Kelly Wang, James A. Landay, and Jeff Hancock. 2018. Gender-Inclusive Design: Sense of Belonging and Bias in Web Interfaces. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 614, 6 pages. https://doi.org/10.1145/3173574.3174188

[41] Nest. 2018. Nest Thermostats | Keep You Comfortable and Help Save Energy. Retrieved 2018-08-31 from https://nest.com/thermostats/

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

[43] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. ACM, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[44] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. 2008. More than meets the eye: Transforming the user experience of home network management. *Proceedings of the 7th ACM conference on Designing interactive systems* (2008), 455–464. https://doi.org/10.1145/1394445.1394494

[45] Juniper Research. 2017. AMAZON ECHO & GOOGLE HOME TO RESIDE IN OVER 50US HOUSEHOLDS BY 2022, AS MULTI-ASSISTANT DEVICES TAKE OFF. Retrieved 2018-08-06 from https://www.juniperresearch.com/press/press-releases/amazon-echo-google-home-to-reside

[46] Jennifer A. Rode and Erika Shehan Poole. 2018. Putting the Gender Back in Digital Housekeeping. In *Proceedings of the 4th Conference on Gender & IT (GenderIT '18)*. ACM, New York, NY, USA, 79–90. https://doi.org/10.1145/3196839.3196845

[47] Mary Beth Rosson, Hansa Sinha, and Tisha Edor. 2010. Design planning in end-user web development: Gender, feature exploration and feelings of success. In *Proceedings - 2010 IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC 2010*. 141–148. https://doi.org/10.1109/VLHCC.2010.28

[48] Samsung SmartThings. 2018. Add a little smartness to your things. Retrieved 2018-08-30 from https://www.smartthings.com/

[49] Stephen Snow, Frederik Auffenberg, and m. c. schraefel. 2017. Log It While It's Hot: Designing Human Interaction with Smart Thermostats for Shared Work Environments. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 1595–1606. https://doi.org/10.1145/3025453.3025578

[50] D.J. Solove. 2008. *Understanding Privacy*. Number v. 10 in Understanding privacy. Harvard University Press. https://books.google.com/books?id=XU5-AAAAMAAJ

[51] J. Sturgess, J. R. C. Nurse, and J. Zhao. 2018. A capability-oriented approach to assessing privacy risk in smart home ecosystems. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. 1–8. https://doi.org/10.1049/cp.2018.0037

[52] Sabrina Thai and Elizabeth Page-Gould. 2017. ExperienceSampler: An Open-Source Scaffold for Building Smartphone Apps for Experience Sampling. In *Psychological Methods*. http://dx.doi.org/10.1037/met0000151

[53] D. Townsend, F. Knoefel, and R. 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

[54] 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)*.

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

[56] Jong-bum Woo and Youn-kyung Lim. 2015. User Experience in Do-it-yourself-style Smart Homes. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 779–790. https://doi.org/10.1145/2750858.2806063

[57] Allison Woodruff, Sally Augustin, and Brooke Foucault. 2007. Sabbath Day Home Automation: "It's Like Mixing Technology and Religion". In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. ACM, New York, NY, USA, 527–536. https://doi.org/10.1145/1240624.1240710

[58] Rayoung Yang and Mark W. Newman. 2013. Learning from a Learning Thermostat: Lessons for Intelligent Systems for the Home. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. ACM, New York, NY, USA, 93–102. https://doi.org/10.1145/2493432.2493489

[59] 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

[60] Serena Zheng, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. In *ACM Conference on Computer Supported Cooperative Work (CSCW)*.