You, Me, and IoT: How Internet-connected Consumer Devices Affect Interpersonal Relationships

NOAH APTHORPE, Colgate University
PARDIS EMAMI-NAEINI, University of Washington
ARUNESH MATHUR, Princeton University
MARSHINI CHETTY and NICK FEAMSTER, University of Chicago

Internet-connected consumer devices have rapidly increased in popularity; however, relatively little is known about how these technologies are affecting interpersonal relationships in multi-occupant households. In this study, we conduct 13 semi-structured interviews and survey 508 individuals from a variety of backgrounds to discover and categorize how consumer IoT devices are affecting interpersonal relationships in the United States. We highlight several themes, providing exploratory data about the pervasiveness of interpersonal costs and benefits of consumer IoT devices. These results inform follow-up studies and design priorities for future IoT technologies to amplify positive and reduce negative interpersonal effects.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; *Ubiquitous and mobile devices;*

Additional Key Words and Phrases: Internet of Things, smart home devices, interpersonal relationships, multi-occupant households

ACM Reference format:
Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2022. You, Me, and IoT: How Internet-connected Consumer Devices Affect Interpersonal Relationships. *ACM Trans. Internet Things* 3, 4, Article 25 (September 2022), 29 pages.
https://doi.org/10.1145/3539737

1 INTRODUCTION

Consumer IoT devices have greatly increased in popularity over recent years and are often designed to replace existing non-networked products by introducing new effort-saving features into consumer homes. Like the introduction of refrigerators, televisions, and other domestic technologies in previous decades [46], the growing adoption of consumer IoT devices can dramatically alter the day-to-day interactions between people living in shared spaces. Recent reports have documented that IoT devices are disrupting households in unexpected ways—from replacing a spouse

This work was funded by NSF Award CNS-1953740.
Authors' addresses: N. Apthorpe, Department of Computer Science, Colgate University, 13 Oak Drive, Hamilton, NY, 13346; email: napthorpe@colgate.edu; P. Emami-Naeini, Paul G. Allen School of Computer Science & Engineering, University of Washington, Box 352350, Seattle, WA, 98195; email: pardis@cs.washington.edu; A. Mathur, Department of Computer Science, Princeton University, 35 Olden Street, Princeton, NJ, 08540; email: amathur@cs.princeton.edu; M. Chetty and N. Feamster, University of Chicago Department of Computer Science, John Crerar Library Building, 5730 South Ellis Avenue, Chicago, IL, 60637; emails: {marshini, feamster}@uchicago.edu.

2577-6207/2022/09-ART25 $15.00
https://doi.org/10.1145/3539737

as an attentive conversation partner [12] to being used by domestic abusers to exert control over others in their homes [6, 27].

In this study, we investigate how consumer IoT devices affect interpersonal relationships, including how they improve household dynamics and how they cause or exacerbate interpersonal conflicts. We use the terms "Internet of things" and "IoT devices" in this article to refer to consumer-grade Internet-connected physical products designed predominantly for domestic use, excluding smartphones, tablets, personal computers, and Internet-connected technologies in non-commercial domains (e.g., industrial, commercial, or medical). This aligns with previous definitions of the consumer Internet of Things [8] and encompasses the broad variety of devices considered as such in the literature, including voice assistants [28], game consoles [37], smart TVs [54], WiFi speakers [26], security cameras [2], large appliances [34], activity trackers [30], and other "smart home" automation devices [15]. This inclusive definition allows us to consider a wide range of IoT devices that intersect with many aspects of users' lives. However, we do not assume that the devices owned by our study participants are comprehensive of the consumer IoT space. We use the term "interpersonal relationships" in this article to refer to social interactions, connections, and opinions existing over an extended period among multiple individuals sharing a household or other physical space. We use the terms "interpersonal benefits" and "interpersonal conflicts" to refer to events and actions that strengthen or weaken these relationships, respectively. These definitions align with the vernacular use of these terms and are consistent with ideas expressed in prior research on shared IoT technology use [25, 31, 63].

We first conducted 13 semi-structured one-on-one interviews with individuals living in multi-occupant U.S. households with a variety of IoT devices (Section 3). The interviews involved discussions of how IoT devices have affected household relationships from a variety of perspectives, including spouse/partner/roommate dynamics, parenting decisions, and interactions with guests. Open-coding of interview transcripts revealed several recurring themes that deepen our understanding of IoT devices and interpersonal relationships. We then surveyed an additional 508 individuals living in multi-occupant households with IoT devices to better understand the extent of the effects surfaced in the interviews and to identify additional themes across a larger sample size and wider variety of demographics (Section 4).

The combined interview and survey results indicate that IoT devices often *benefit (B)* interpersonal relationships and cause interpersonal *conflict (C)* by the following mechanisms (Section 5):

- **B1. Strengthening interpersonal connections** through bonding over shared experiences, simplifying remote communication, and inspiring playfulness.
- **B2. Enabling empowerment and independence** by reducing the sense of being a burden and helping individuals with special needs.
- **B3. Easing household management**, resulting in increased free time to spend with household members and improved peace of mind.
- **C1. Facilitating surveillance and causing mistrust** due to potential or actual undesired monitoring and a lack of data collection transparency.
- **C2. Provoking differences in knowledge or preferences** about the functionality, benefits, risks, privacy, or security of IoT devices.
- **C3. Causing tensions about device use, sharing, and technical issues** that arise during day-to-day operation and proximity of the devices.

These results are important, because qualitative research on IoT devices and household relationships remains limited, and large-scale quantitative data about the interpersonal effects of consumer IoT adoption are likewise non-existent in the HCI literature (Section 2). Revealing and categorizing these interpersonal conflicts and benefits allows us to identify common underlying factors

that not only motivate future studies but also inform recommendations for device manufacturers (Section 6). First, insufficient and unclear documentation leads to users having contradictory mental models of device behaviors and conflicting assumptions about data collection practices and appropriate device use. Second, many IoT devices lack customization options with enough flexibility to account for diverse user relationships, especially in households where individuals have different device control responsibilities or data privacy concerns. Manufacturers must be cognizant of these issues while recognizing that IoT devices, when designed well, can actually improve interpersonal relationships. By enhancing device documentation, clarifying data collection practices, and providing more flexible customization options, manufacturers could better support real-world use of their products. Ultimately, this article forms the basis for future investigations of the interpersonal benefits and conflicts we report and serves as a call for manufacturers to consider a broader range of social and household dynamics when designing IoT devices.

This article makes the following contributions:

- Discovers and categorizes common effects of IoT devices on interpersonal relationships through interviews and open-ended survey responses.
- Provides exploratory survey data indicating the pervasiveness of interpersonal conflicts and benefits across multi-occupant U.S. households.
- Discusses common underlying factors, recommendations for device manufacturers, and follow-up studies to improve the effects of IoT devices on interpersonal relationships.

2 RELATED WORK

Most research to date has only tangentially examined how consumer IoT devices affect interpersonal relationships, often in light of related research topics, such as multi-user content sharing or privacy concerns. A few closely related studies conducted in 2019 [25, 31, 63] investigated multi-user interactions and shared control of IoT devices in homes. Other IoT user studies have focused on different research questions, including purchasing decisions [21], privacy concerns regarding entities external to the home (manufacturers, governments, etc.) [64], privacy expectations of devices themselves [3, 19], and how friends and experts influence IoT data collection consent [20]. Our project complements and extends this literature by specifically focusing on the interpersonal benefits provided by IoT devices as well as the household tensions, conflicts, or disagreements caused by these products.

2.1 Benefits of IoT Devices

Previous studies of the benefits of IoT devices have focused predominantly on functionality with fewer studies noting how these devices benefit interpersonal relationships.

2.1.1 Curiosity & Routines. Lazar et al. [33] found that interview participants chose to use IoT devices because "the devices satisfied curiosity and held hope for potential benefit to them," or because the devices had been incorporated into the participants' routines. Our work also indicates that curiosity about home IoT devices can improve interpersonal relationships by inspiring playful behavior and facilitating bonding over shared interests (Section 5.2).

2.1.2 Convenience. Coskun et al. [16] found that improved comfort and performance through automation incentivized the incorporation of IoT appliances into households. Zheng et al. [64] also found that early adopters cited convenience as a primary reason for using IoT devices, a factor that outweighed concerns about privacy vis-a-vis device manufacturers, governments, and other entities external to the home. Strengers et al. [55] similarly noted that productivity benefits were central to experiences with IoT devices for 31 early adopters, including small conveniences

such as energy savings and support for multi-tasking. This article extends these findings by showing that the conveniences afforded by IoT devices can directly benefit interpersonal relationships (Section 5.4).

2.1.3 Connection with Friends and Family. Emami-Naeini et al. [21] found that prospective buyers of IoT devices often turned to friends and family for word-of-mouth recommendations and advice. Woo and Lim [60] conducted an observational study in DIY smart homes and found that home automation could provide emotional comfort as a happy reminder of the person who set up the automation. Takayama et al. [56] found that home automation systems can support family communication, connection to loved ones, and positive household monitoring (e.g., observing a family pet when away from home). Strengers et al. [55] reported that early adopters appreciated IoT device features that allowed them to better protect their households, viewing this protection as a form of care provided to others in their home. These early adopters also cited improvements to home ambiance provided by IoT devices and the ability to showcase new technologies to visitors. Kraemer et al. [31] described the processes used by a household navigating shared IoT devices as "group efficacy," extending Bandura's definition of self-efficacy [4] to communal behavior. Morris [43] provides many examples of individuals using connected technologies to support and enhance social relationships, often in ways not anticipated by the technology designers. While some of these studies, especially Morris [43], prioritize varying *uses* of technology, others (including this article) explore the effects that connected devices have on relationships.

2.1.4 Community Benefit. An ethnographic study by Burrows et al. [11] found that users of IoT health technologies were willing to share anonymized data if they believed it would improve community well-being. This corroborates findings by Zheng et al. [64] that early adopters were willing to share some IoT data with local governments to improve utility expenses and other services for the entire community. While not the focus of this study, these findings indicate how IoT devices could positively affect interpersonal relationships outside of the household.

2.2 Conflicts Involving IoT Devices

Existing research has also examined how IoT devices cause interpersonal conflicts, typically regarding specific use cases or topics of contention (e.g., privacy).

2.2.1 Power Imbalance and Technical Expertise. Geeng and Roesner studied shared control of IoT devices in different living situations [25] and found that multi-user tensions can be categorized by when they occur, namely, during "(1) device selection and installation, (2) regular device usage, (3) when things go wrong, and (4) over the long-term." They also provide examples of tensions arising in specific partnership, roommate, and parent/child relationships and note that many of these tensions are caused by differences in "power, agency, technical skill, and technical interest." Some studies have also found that Internet-connected products may amplify domestic disputes and abuse [6, 22, 27]. Our work is consistent with these results—we find similar concerns over surveillance, for example—and adds further context to past work by exploring the prevalence of these concerns. More generally, we focus on a broader set of interpersonal relationships beyond control and power dynamics. We also provide new examples of interpersonal conflicts involving IoT devices and quantitative data indicating the pervasiveness of these and other causes of tensions (Sections 5.5–5.7).

2.2.2 Incompatible Incentives. Zeng and Roesner [63] conducted an interview study and design exploration to understand how users navigate security and privacy issues in multi-occupant homes with IoT devices. They found that users wanted access controls in place for configuration changes, parental controls, and devices in private rooms—all indicating situations in which

different household members may have differing incentives that could lead to conflict. They also note the importance of social norms, trust, respect, lack of concern, and a desire for convenience as inhibitors of access control use—factors that we find also provide interpersonal benefits in homes with IoT devices.

2.2.3 Differences in Knowledge and Expectations. In 2018, Malkin et al. [36] found that there was a great deal of uncertainty and assumptions about smart TV data collection practices among surveyed users. In 2017, Zeng et al.'s [62] interviews found that differences in security/privacy mental threat models, differences in access and control of IoT devices, and surveillance all led to disagreements or concerns in multi-user homes. In 2014, Ur et al. [57] interviewed parents and children about their opinions of home-entryway surveillance and observed a disconnect between parents' and children's surveillance preferences, which could potentially cause interpersonal conflict.

In 2012, Mennicken and Huang [41] observed variations in roles, including "home technology drivers," "home technology responsibles," and "passive users." Users in these categories had qualitatively different knowledge of and experience with home technologies. Our participants also had a range of knowledge and preferences regarding IoT device behavior, complicating the categories of Mennicken and Huang [41] by demonstrating the diversity of household relationships and roles. These results provide further interpersonal relationship context to Brush et al.'s 2011 results on UI and access control from DIY smart homes [10] and show that some of these issues continue with mass-market IoT products.

2.2.4 Changing Privacy Norms. Issues of privacy in shared spaces often arise in studies of consumer IoT devices, including in many works cited above. Researchers have framed these issues using formal privacy theories, including the application of contextual integrity [44] to understand the landscape of sensitive data and privacy concerns in smart homes and smart buildings [3, 38] and quantified-self health data [48]. The rapidly changing landscape of consumer IoT products is creating new privacy norms and expectations for shared spaces, a topic explored by Zafiroglu et al. in 2016 [61] and raised by several of the participants in this study (Section 5.5).

3 INTERVIEW METHOD

We conducted 13 semi-structured interviews to understand how consumer IoT devices are affecting interpersonal relationships in multi-occupant households. The interviews involved a scripted series of questions interspersed with and followed by open-ended conversation.

The interview study was approved by the Princeton University and Carnegie Mellon University Institutional Review Boards (IRB). All participants provided their informed consent to participate in the screening survey and interviews, to have their voice recorded, and to have the recordings transcribed by a third-party company. We anonymized the transcriptions prior to coding.

3.1 Recruitment

We recruited participants through Craigslist in the Central New Jersey and Pittsburgh, Pennsylvania, regions containing our universities. We also used snowball recruiting, asking interviewees to recruit their friends, family, and acquaintances. The Craigslist advertisements stated that "researchers at Princeton and Carnegie Mellon Universities want to better understand your interactions with smart (Internet-connected) devices" and "researchers at Princeton and Carnegie Mellon Universities want to better understand how smart (Internet-connected) home devices and appliances can cause disagreements, tension, or conflict in interpersonal relationships between people living in the same household." The advertisements specified that participants must be at least

Table 1. Interview Participant Demographics, Household Occupants, IoT Devices, and Interview Durations (mm:ss)

	Gender	Age	Income	Education	Occupants	IoT Devices	Duration
PI1	M	24	<$20K	College	3 Roommates	6 security cameras, smart TV	17:54
PI2	F	42	>$100K	College	Domestic partner	Amazon Echo	28:11
PI3	M	22	<$20K	High School	Domestic partner	Amazon Fire TV, gaming consoles	19:08
PI4	F	41	$50–75K	College	Spouse, 2 Children	Amazon Echo, Amazon Echo Dot, Google Home, Sonos	21:17
PI5	M	50	>$100K	High School	Domestic partner	Amazon Echo	21:46
PI6	F	22	$50–75K	Prof. Deg.	2 Roommates	Google Home	18:57
PI7	M	58	>$100K	Assoc. Deg.	Spouse	Amazon Echo, TVs, Amazon Fire Stick, refrigerator, washer, dryer, doorbell	20:39
PI8	F	53	$50–75K	Prof. Deg.	1 Child	Amazon Echo, security cameras, smart TV	15:43
PI9	F	21	<$20K	College	2 Roommates	Roku TV	20:29
PI10	F	21	>$100K	High School	Domestic partner	Google Home, August Smart Lock	19:39
PI11	F	30	>$100K	Prof. Deg.	Domestic partner	Amazon Echo, Amazon Show, smart TV	16:07
PI12	M	36	>$100K	College	Spouse, 3 Children	Amazon Echo, Roku, wireless doorbell	15:35
PI13	F	34	$50–75K	College	Spouse, 1 Child	Amazon Echo Dot, iRobot Roomba, smart TV, smart plugs	16:40

18 years of age and live in a home or apartment with at least one other person and at least one IoT device.

The advertisements invited individuals to complete a short screening survey. The screening survey asked respondents to list the number and relationships of people living in their household, the number and types of IoT devices in their household, and how they acquired those devices. It also included a series of demographics questions, including age, gender, income, education, occupation, and technology background.

The advertisements were online for five days, after which the screening survey responses were reviewed and qualifying respondents were contacted for interview scheduling. We received 77 responses from Craigslist recruiting. We also received 2 responses from snowball recruiting. We selected all 51 respondents who reported owning at least one IoT device and living with at least one other person. We emailed these respondents with two tentative dates and times for interviews that fit with their reported availability; 26 respondents replied to confirm an interview time. Of these, 13 participants actually joined the video call for the interview at the scheduled time, resulting in 13 total interviews.

These 13 participants had a range of demographic backgrounds, living situations, and IoT devices in their households (Table 1). There were 5 male and 8 female participants ranging from 22 to 58 years old. The participants lived with roommates, spouses, significant others, and children. They owned many popular IoT devices, including voice assistants, smart TVs, IoT locks, WiFi appliances, and others. All participants were compensated with a $25 Amazon gift card for completing the interview.

3.2 Interview Procedure

All interviews were conducted on a one-on-one basis by the first author over video call and were semi-structured in nature. The interviewer used a prepared script (Table 2) and followed up on topics that arose naturally during the conversation, leading to discussions that varied widely, depending on the opinions and experiences of each participant. The interview script included questions about household occupants and devices, device purchasing, setup and account management, device use by home occupants, interpersonal benefits involving the device, interpersonal conflicts involving the device, privacy and in-home surveillance, device use by children, and device design feedback. When discussing interpersonal benefits and conflicts, the interviewer guided the conversation to ensure that the participant reported which devices were involved, how

Table 2. Interview Script

Category	Questions
Household	• Who lives in your household? • What Internet-connected devices do you have in your home?
Device Purchasing	• How long have you had the device? • Who purchased the device and why? • Did you have any concerns about the device before purchase?
Setup & Accounts	• Who set up the device? • Who is in charge of managing the device? • Do you have individual or shared accounts on the device?
Device Use	• How and why do people in your household use the device? • How well do you and others understand how to use the device?
Benefits	• Has the device improved the relationships between people in your household? If so, please describe. • How else has the device benefited people in your household?
Conflicts	• Has the device been involved in any conflicts, tensions, or disagreements in your household? If so, please describe. • Who in your household was involved in these conflicts? • Were these existing conflicts or new ones caused by the device? • Did you take any steps to mediate these conflicts?
Privacy	• Have you discussed or disagreed about the privacy implications of the device with others in your household? • Have you ever used the device to monitor others? • Do you think others have ever used the device to monitor you?
Children (if applicable)	• Do your children use this device? • Have your relationships with your children improved due to the device? • Have you had any conflicts, tensions, or disagreements with your children about their use of the device?
Design Feedback	• What is your opinion about the device? • What would you like to change about the device?

The interviewer asked the device-specific questions about one to three IoT devices in the participants' households as time allowed. The interviewer also asked participants to freely expand on topics when appropriate given the semi-structured nature of the interviews.

household members were affected, whether the device contributed to existing conflicts or created new conflicts, and whether any steps were taken to mediate the conflicts. The interviews only focused on participants' relationships as appropriate. For example, participants without children were not asked about children's interactions with their devices. All interviews lasted between 15–30 minutes.

3.3 Data Analysis

We transcribed the interview audio recordings using NVivo's automated transcription service [45] then manually reviewed the transcriptions, making corrections as necessary to ensure accuracy. We performed open coding [51] on the transcriptions to identify recurring themes. Two authors independently arrived at a set of codes and then consolidated their codes into a codebook[1] with

[1]Interview codebook provided in the Supplementary Material.

6 main parent codes: "Positive experiences," "Benefits to relationship," "Conflicts & concerns," "Conflict mediation," "Involvement," and "Time of benefit/conflict." We also had a total of 40 child codes. For example, the "Time of benefit/conflict," parent code had child codes "purchase time," "installation time," and "use." Each interview transcript was coded by these two authors and disagreements were discussed and resolved in multiple meetings. The entire research team met regularly to identify the main concepts and themes occurring across the coded data. These themes informed the questions in the follow-up survey (Section 4.1.3) and are reported along with additional themes from the survey as the primary results of this study (Section 5). We did not calculate inter-rater reliability (IRR) for our interview analysis, because the coded data was not an end product but a process used to derive concepts as themes, making an IRR measure unnecessary in this case [39].

4 SURVEY METHOD

We conducted a survey to measure the pervasiveness of the interpersonal effects of IoT devices observed in the interviews and to discover additional themes across a wider variety of demographics. The survey was approved by the Princeton University and Carnegie Mellon University Institutional Review Boards. All respondents provided their informed consent to participate in the survey.

4.1 Survey Design

The survey contained five sections[2]:

4.1.1 Consent Form and Home Context. The survey began with a consent form. Respondents were then asked to indicate the number of the people in their household, the relationships of these people to themselves (e.g., "spouse" or "parent"), and the types of IoT devices in their household. Respondents selected their IoT devices from a multiple-choice list of the Internet-connected products in Table 3. This list was provided by the custom prescreening options of the survey deployment platform (Section 4.2). This facilitated survey deployment and provided a broad view of IoT devices consistent with our definition in Section 1. All respondents who did not agree to the consent form, had no IoT devices, or lived alone were not allowed to continue the survey and were not included in the results analysis.

4.1.2 Interpersonal Relationship Questions. The next section of the survey asked respondents whether "Internet-connected products have caused any disagreements (major or minor) between people in your household?" Respondents who answered "yes" were asked to describe the conflict in an open-ended text response question and then to answer multiple choice questions about which device(s) had been involved in the conflict, who in the household had been involved in the conflict, and what steps (if any) they had taken to mitigate the conflict. Respondents who answered "no" were asked to describe whether they "have had any other negative experiences with Internet-connected products."

This structure was then repeated for interpersonal benefits, first asking respondents whether "Internet-connected products have improved your relationships with others in your household?" Respondents who answered "yes" were asked to describe this improvement in an open-ended text response question and then to answer multiple choice questions about which device(s) and household members were involved in the improved relationship. Respondents who answered "no" were asked to describe whether they "have had any other positive experiences with Internet-connected products."

[2]Full survey provided in the Supplementary Material.

Table 3. Self-reported Demographics, Living Situations, and IoT Devices of Survey Respondents

Demographic	Sample	Demographic	Sample	Demographic	Sample
Gender		**Individual Annual Income**		**Household Members**	
Female	53%	<$20,000	9%	Spouse	48%
Male	46%	$20,000–$34,999	13%	Child	36%
Other	2%	$35,000–$49,999	17%	Parent	24%
		$50,000–$74,999	20%	Partner	16%
Age		$75,000–$99,999	18%	Other relative	15%
18–24	19%	>$100,000	20%	Housemate or roommate	9%
25–34	42%	Prefer not to disclose	3%	Other non-relative	2%
35–44	21%				
45–54	11%	**Household Size**		**IoT Devices**	
55–64	6%	2 people	39%	Games console	75%
65–74	1%	3 people	24%	Smart TV	64%
75+	<1%	4 people	23%	Video streaming product	60%
		5 people	8%	Home assistants/smart hub	43%
Education		6+ people	6%	Activity tracker	33%
No high school	1%			Smart watch	21%
High school	34%	**Language at Home**		Connected lights	14%
Associates	11%	Only English	86%	Smart security camera	13%
College	39%	Other language	13%	Smart thermostat	13%
Prof. deg.	14%			Smart plugs	11%
Prefer not to disclose	1%			Other devices	<10%

The less prevalent "other devices" include smart doorlocks/doorbells, baby cameras/monitors, smart water sprinklers/irrigation controllers, smart health monitors, smart smoke monitors and alarms, smart kitchen appliances, and smart Bluetooth trackers.

4.1.3 Likert-scale IoT Questions. The following section contained a matrix of Likert-scale multiple choice questions with the prompt "How much do you agree with the following statements about home technology?" and five answer choices: "Strongly agree," "Somewhat agree," "Neither agree nor disagree," "Somewhat disagree," and "Strongly disagree."

The statements were generated from recurring themes in the interviews to measure their pervasiveness across a larger sample size. Examples include "Internet-connected products have inspired playful behavior in my household" and "I have disagreed with others in my household about whether we should have Internet-connected products in our home." We used the interview participants' own wording about benefits and conflicts (e.g., "disagreed" and "tensions") when creating these survey questions to facilitate interpretability. These questions were not intended to be of balanced valence between positive and negative effects and should not be interpreted as such. Figures 2, 3, and 4 present the full list of statements with response distributions. This section also included an attention check question asking participants to select "Somewhat disagree." After viewing the Likert-scale questions, respondents could not return to modify their answers to the open-ended questions. This prevented priming effects from the Likert question prompts from influencing open-ended responses.

4.1.4 Demographics. The survey concluded with a series of standard demographics questions, including age, gender, education, annual household income, and primary language spoken at home.

4.2 Survey Deployment and Respondent Overview

We tested the length and clarity of the survey by performing seven 10-minute "cognitive interviews" on UserBob [58], a usability testing platform that recruits crowdworkers at a rate of $1/minute to interact with a website while recording their screen and providing audio feedback. We

Table 4. Codebook for Open-ended Responses to Survey Questions About Interpersonal Benefits

Code	Explanation
play	Playfulness and entertainment leading to bonding
convenience	Convenience and improving quality of life
connected	Staying connected with family and friends
do more	Ability to do more or having more choices and features
financial	Saving money together
time	Enabled spending time together (includes conversation, bonding, etc.)
health	Staying fit together
security	Enabling safety and security
special pop.	Helpful for people with disabilities or special needs
interactions	Fewer interactions with each other leading to fewer conflicts
none	None
not clear	Not clear

"Describe how Internet-connected products have improved your relationships with others in your household. Please provide as much detail as you can." and "If you have had any other positive experiences with Internet-connected products, please describe them here."

asked the workers to "go through the survey, pretending you are a participant and letting us know whether the survey makes sense." We adjusted the survey based on their feedback, including reducing the number of questions per page and adding bold font to highlight the Likert-scale questions. The UserBob recordings confirmed that respondents interpreted the questions as expected, avoiding the need for wording changes. The UserBob responses were not included in the final results.

We recruited 536 respondents through Prolific [50], an online survey service founded in 2014 that maintains its own pool of respondents and emphasizes data quality, fair compensation, and significantly fewer bot-like accounts than Amazon Mechanical Turk [7]. We chose Prolific because it allowed us to pre-screen for respondents with multi-occupant households and reported ownership of Internet-connected products. This prevented the need for a separate screening survey as would have been necessary on Amazon Mechanical Turk. All respondents were paid $1.10 for completing the survey, resulting in an average compensation of $13.20/hour across all respondents.

The survey respondents all lived in the United States and had a variety of demographic backgrounds, living situations, and IoT devices (Table 3). The respondents were 53% female, 82% younger than 45, 53% with college degree or higher, 39% with individual annual incomes less than $50,000/year, and 61% living in households with more than two individuals. This higher proportion of young, well-educated respondents compared to the general population reflects well-known biases in Internet use in the United States [49] and other crowdsourcing platforms [29]. The potential effects of these and other representativeness issues on the survey results are discussed in Section 7.

4.3 Response Analysis

We started with 536 survey responses. We removed 16 responses that failed the attention check question and 12 responses from those who took less than two minutes to complete the survey. The remaining 508 responses used for analysis had a median completion time of 5.85 minutes.

We performed open coding [51] on the open-ended text responses. Two authors independently coded these questions, consolidated their codes into interpersonal benefits and conflicts codebooks (Tables 4 and 5), then re-coded the questions, achieving a Kupper-Hafner intercoder reliability score [32] greater than 0.76 on all questions for a sample of 100 respondents. We used these final codebooks to identify several of the interpersonal conflicts and benefits themes presented in Section 5.

Table 5. Codebook for Open-ended Responses to Survey Questions About Interpersonal Conflicts

Code	Explanation
choice	Hard to choose the right device (due to various specifications)
f2f	Negative effects for face-to-face communication
functionality	Functionality and technical challenges of setting up IoT devices
misbehavior	Misbehavior caused using IoT devices
necessity	Lack of need, interest, or perceived benefit in technology or IoT devices
network	Discussions around bandwidth sharing
parenting	Challenges in parenting caused by kids' use of devices
privacy	Privacy and comfort-related concerns (e.g., surveillance, data use, data sharing, discomfort caused by shared privacy settings)
unexpected	Unexpected device behavior
updates	Difficulties caused due to firmware updates and troubleshooting
variance	Different set of users of the same device and their varying use preferences
none	None
not clear	Not clear

"Describe how Internet-connected products have caused disagreements (major or minor) in your household. Please provide as much detail as you can." and "If you have had any other negative experiences with Internet-connected products, please describe them here."

We then analyzed the multiple choice questions to determine the pervasiveness of these themes (Figures 2–5). We compared the relative prevalence of interpersonal benefits versus conflicts by applying the Chi-squared test to compare the distributions of responses to the questions "Have Internet-connected products caused any disagreements (major or minor) between people in your household?" and "Have Internet-connected products improved your relationships with others in your household?" We also compared the responses to selected Likert-scale multiple choice questions across demographic groups, using Mann-Whitney U tests to compare the distribution of agree responses ("strongly agree" or "somewhat agree"), neutral responses, and disagree responses ("strongly disagree" or "somewhat disagree") to each question of interest between all pairwise sets of respondents with different answers to each demographic question.

Given the small interview sample size, we did not compare results between the surveys and the interviews. Rather, we combined the qualitative and quantitative evidence provided by both methods into our results and discussion (Sections 5–6).

5 RESULTS

Our interviews and survey responses indicate the richness of interpersonal benefits (B1–B3) and conflicts (C1–C3) involving consumer IoT devices. This section provides quantitative and qualitative data to support the pervasiveness and influence of these themes and their importance to IoT adoption, design, and research. We refer to interview participants as PI#, survey respondents as PS#, and use the qualitative terminology from Emami-Naeini et al. [21] to report the frequency of qualitative findings from the interviews and the open-ended survey questions (Figure 1). We also present data about conflict mediation and other ways that users are adapting their lives with IoT devices.

5.1 Interpersonal Benefits versus Conflicts

Significantly more survey respondents reported that IoT devices have improved their relationships with others in their household (49%) compared to those who reported that IoT devices have caused disagreements in their household (23%, $p \ll 0.01$). This corroborates the higher frequency of "strongly agree" and "somewhat agree" responses to the corresponding Likert-scale questions about relationship improvements versus conflicts (Figure 2). We did not find any significant

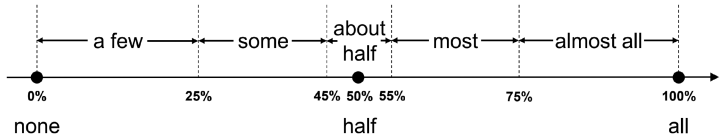

Fig. 1. Qualitative terminology used to report findings of interviews and open-ended survey questions. Figure from Emami-Naeini et al. [21].

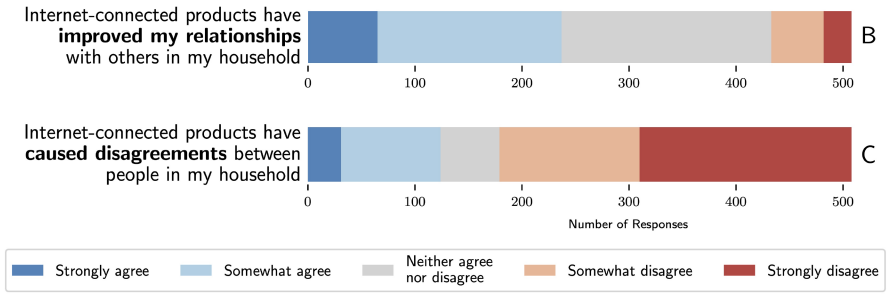

Fig. 2. Survey responses indicating the prevalence of interpersonal benefits (B) and interpersonal conflicts (C) resulting from IoT devices.

differences between the reported frequency of interpersonal benefits or conflicts across demographics, indicating that while such variations may exist, a larger or more representative group of respondents would be necessary to identify them given their effect size.

The interpersonal benefits reported by our participants range from the well-studied, such as simplifying everyday tasks [64], to the less-understood, such as helping support a household member with special needs. Although the reported interpersonal conflicts are less frequent, they are often serious, including the use of devices to surveil household members without their knowledge: 9% (46/508) of survey respondents report active disagreements with others in their household about surveillance, and 15% (78/508) agree that they have used Internet-connected products to monitor someone else's behavior.

5.2 B1. Strengthening Interpersonal Connections

Most participants who reported positive experiences with their IoT devices linked these experiences to improved interpersonal connections with other household members. We found several recurring ways that these devices facilitated such strengthened connections.

5.2.1 Bonding over Shared Experiences. Most of our interview and survey participants said that IoT devices caused family members to bond over shared experiences, often facilitated by the ease of content sharing enabled by the devices. For example, PS97 said,

> Streaming movies helps my relationship with my partner. It gives us bonding time.

PS438 talked about similar positive experiences with an IoT speaker:

> Smart devices made it easier to share music with my siblings, like smart speakers for example. Instead of having to pass someone's phone or rely on one person connected, we can just tell it to play a song and boom.

IoT devices also precipitated inter-generational bonding when a younger generation helped an older relative with technology they found too complicated, as PI2 described:

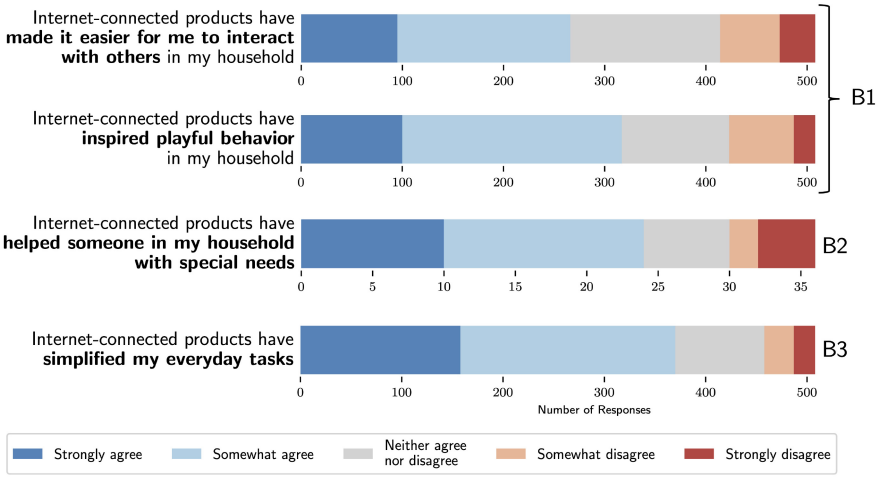

Fig. 3. Survey responses indicating the prevalence of interpersonal benefits from IoT devices related to themes B1–B3. Note the difference in scale for the third question, which was only asked of respondents who reported having special-needs individuals in their households.

> We've got an Apple TV and my father almost cried because he said he was really curious about [the device] and streaming television, but he felt too out of the loop and overwhelmed to try another giant leap in technology. And he was overjoyed...to have my boyfriend help out with setting it up.

PS73 described helping relatives with IoT devices and bonding over this kind of support even more succinctly:

> My parents are not exactly tech savvy, so when I help them in terms of the use of technology, it becomes a kind of bonding moment.

More than 50% (266/508) of survey respondents agreed that Internet-connected products made it easier to interact with others in their household (Figure 3). IoT devices necessitate setup, management, and maintenance, and if these responsibilities are distributed amongst household members or family members in different houses, they can facilitate increased communication and connection.

5.2.2 Simplifying Remote Communication. Some of our participants reported that their IoT devices helped them keep in touch with their remote family members. PS381 described this benefit as provided by Amazon Echo and Google Home voice assistants:

> I am better able to stay connected to my adult children and to my disabled husband when I am at work.

PI5 described a similar situation involving communication with his mother through an Amazon Echo instead of having her try to find and work her phone:

> My mother was sick... and before she passed away, it was tougher and tougher for her to use the phone... So what I did was I got an Alexa and I installed it in the house, and then I could just call her and rather than her having to figure out how to answer the phone, she could just hear my voice in the ether.

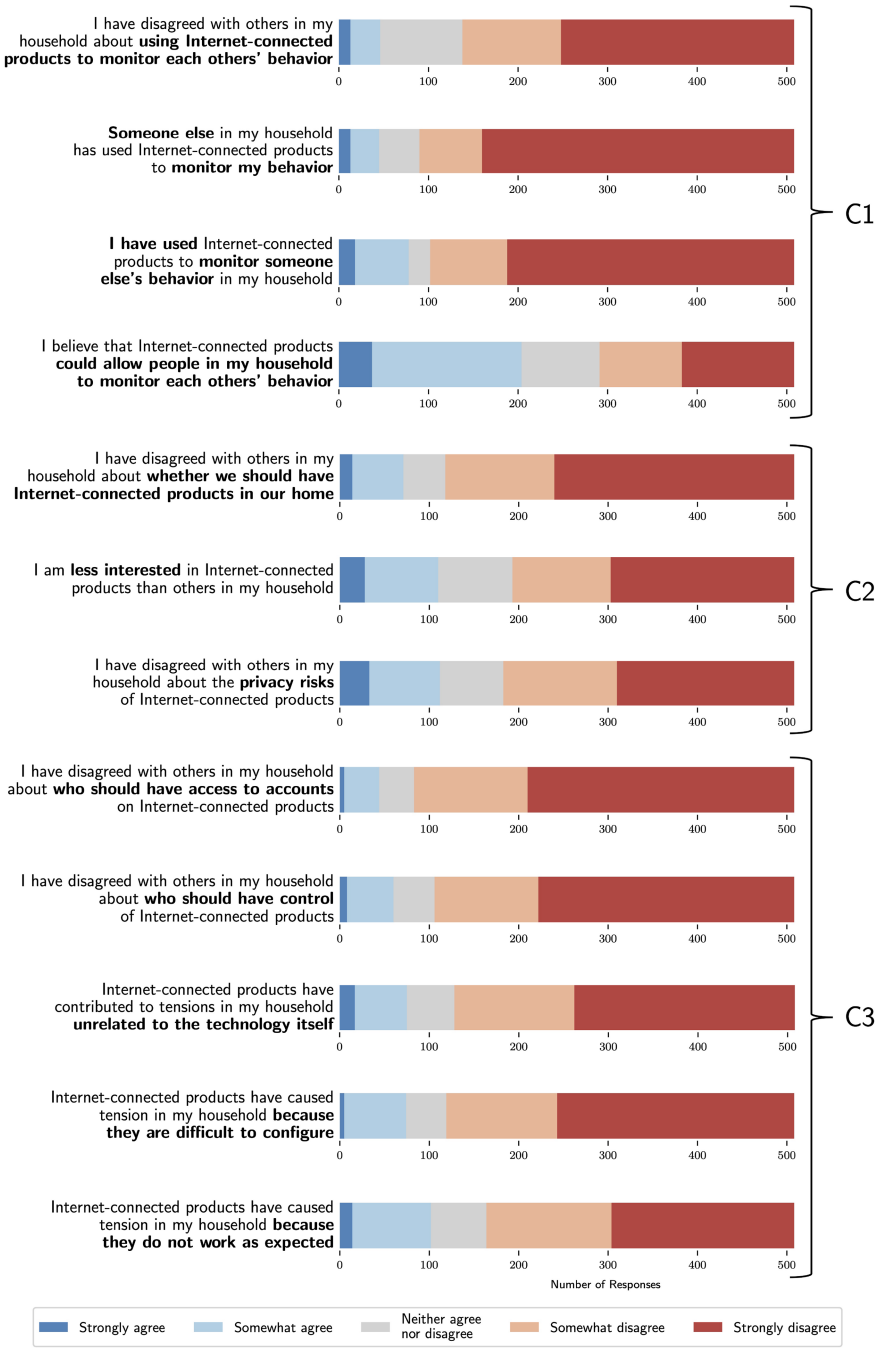

Fig. 4. Survey responses indicating the prevalence of interpersonal conflicts involving IoT devices related to themes C1–C3. The questions are sorted within each theme by the number of "agree" responses.

This quote reveals a benefit provided by a consumer IoT device over a more traditional phone interface. IoT voice assistants also helped a few survey respondents, including PS21, communicate "remotely" with family members inside their home:

> Communicating with my kids is so much easier when we put Echo Dots on each level of our house. We can just drop in on each other and talk instead of yelling.

These findings corroborate past research showing the positive impacts of technology-mediated communications between household members, such as by conveying messages via changing color light bulbs [43]. In this case, IoT devices made interactions between family members in the same or different households easier because they mimicked more natural voice interactions.

5.2.3 Inspiring Playfulness. A few of our interview participants noted that their IoT devices, particularly voice assistants, inspired inquisitive and playful behavior among members of their household. This playfulness was often expressed as asking non-serious questions to the voice assistant to entertain others in the household. For example, PI7 said that their Amazon Echo Dot,

> Lets us sit around and laugh at the different answers…almost like playing a game.

Similarly, PI2 said that hearing their boyfriend talking to their Alexa was amusing:

> The main joy that I get from Alexa is overhearing my boyfriend ask her ridiculous things just to see like if she'll respond, how she'll respond.

These participants shared these anecdotes as some of their favorite experiences with IoT products. The playful feature exploration invited by these voice assistants was related to the perceived novelty of the voice interface. Playfulness was also prevalent factor in positive interpersonal impacts of IoT devices for survey respondents. 62% (317/508) reported that their Internet-connected products have inspired playful behavior in their household (Figure 3).

5.3 B2. Enabling Empowerment and Independence

Most of our participants reported that their IoT devices helped family members seek information and enhance their knowledge without relying on other household members. As PS129 reported,

> My wife can now just ask the Google Home for the weather instead of assuming I know what the weather is.

Strengers et al. [55] described how IoT technologies could help individuals "live independently in their own homes for so many more years." Our results indicate that these benefits are not limited to those living alone, but that improved independence provided by IoT devices can also benefit interpersonal relationships in shared households.

For some of our participants, IoT devices, especially voice assistants, helped family members with special needs when looking for information on their own. PI4 described this benefit for their son who uses Alexa for answering questions:

> My youngest son is actually autistic, but he's very inquisitive in nature and asks me the most intelligent but random questions that we can never really answer. So it's always like "Go ask Alexa"…It's almost like having a teacher or an encyclopedia like right on hand at all times, and for his way of living that's just really helpful for him.

PS445 also described how streaming services accessed through a smart TV helped their child with special needs:

> My kids are special needs, and the ability to find teaching videos through [smart TV] streaming apps has been incredibly valuable to helping teach basics as well as social skills.

The potential benefits of IoT devices for households with special-needs individuals was further corroborated by the multiple-choice survey responses. 66% of the 36 survey respondents who reported an individual with special needs in their household also agreed that their Internet-connected products had helped that individual (Figure 3).

5.4 B3. Easing Household Tasks

Prior work has found that people would like their household chores to be automated, as they perceived them as unwanted tasks [16, 18]. Most of our participants reported that their IoT devices provided convenience in routine tasks and helped them achieve more efficient time management in the household. This was especially predominant in the survey responses: 73% (370/508) of respondents agreed that their Internet-connected products had simplified their everyday tasks (Figure 3). Convenience is a well-studied individual benefit of IoT devices [47, 64]. This study extends these previous findings, demonstrating interpersonal benefits gained from improved convenience.

5.4.1 Increasing Free Time with Household Members. Most of the participants who reported convenience as one of the benefits of IoT devices also said that this convenience allowed them more time to spend with their family members. When asked about the positive experiences of having these devices, PS182 mentioned that their IoT device

> Freed us up to be able to spend more time catching up with each other.

PS50 likewise said that IoT devices make a household easier to manage:

> Having "smart" technology makes it easier to run and manage our household, giving us more time to focus on one another.

5.4.2 Reducing Tensions about Household Management. Some of our participants noted that their IoT devices reduced arguments about chore responsibilities and day-to-day household management. In some cases, these participants were able to entirely offload tasks to their IoT devices. PS325 described how allowing an IoT thermostat and doorbells to automatically manage parts of the home environment reduced household tension:

> With the smart thermostat, we don't argue about the temp of the house because it's automatically set...With the doorbells, we don't have to argue or wonder if it was locked. We can just look on the app...All the small conveniences add up to a happier and healthier lifestyle so we have less tension in the household over stuff.

PS231 described nearly identical benefits of delegating tasks to IoT devices instead of relying on household members to do these tasks:

> We don't have to nag each other to get up and do something. We can ask the device to do it for us. We are not getting into arguments on who forgot what and who didn't set the temperature or lock the door. Everything is programmed.

In other cases, IoT devices helped household members keep track of day-to-day tasks, preventing the need for other members to remind them. This benefit was typically attributed to IoT voice assistants, as described by PS332:

> My partner and I use Amazon Echo to set reminders for each other, which helps with making sure we are both on the same page with groceries and chores.

PS341 also described how automated reminders improved their relationship with their children:

> I have the Amazon Echos in my kids' rooms set to remind them to do daily things like get ready for bed and straighten their rooms. By not having to personally nag them to do these things, we get along better on a daily basis.

By taking care of tasks that an individual might otherwise have to do, IoT devices can reduce cognitive loads on household members who have responsibility for these tasks and other members who want to ensure these tasks are completed in a timely fashion.

5.4.3 Improving Peace of Mind. Some of our participants reported that the convenience provided by IoT devices gave them peace of mind and eased specific worries. According to PS379, who talked about devices for baby monitoring and security,

> Having baby monitors and a smart lock really helps ease our worries, and as worries disappear, there is more room for good feelings.

Peace of mind was also a commonly cited benefit among participants who reported having IoT security systems, including security cameras and door locks. PS8 talked about the feeling of safety provided by their IoT security cameras:

> The smart security cameras provide us with peace of mind, and we feel safe to go out and do things together knowing the house is being watched over.

PS143 reported a similar effect from outdoor cameras and an alarm system easily accessed on a smartphone:

> I have Ring floodlight cameras as well as a smart alarm system connected to my phone, which has given me and my spouse increased peace of mind regarding the security of our home.

By allowing household members to monitor the state of their environment inside and outside the home, IoT devices made our participants feel more at ease.

5.5 C1. Facilitating Undesired Monitoring

While IoT devices facilitated many benefits, they also caused many conflicts. Some of our participants reported that they or other household members were worried about or had experienced surveillance by other household members via their IoT devices. Devices our participants associated with unwanted monitoring all enabled audio or video recording, including security cameras, door bells/locks, and voice assistants. PS433 talked about how one of their housemates became upset by having a Google Home in the house:

> My housemate was very upset when we brought the Google Home in. He is concerned with spying. We appeased him by turning off the microphone, but he has since read that this is not effective.

In another example, PI1 reported the potential for surveillance of household members without their knowledge:

> I was really shocked. I didn't know [the security camera] was working. I thought it was just put in as a design, you know, to threaten someone who's come [to rob the house]. But then when I found out it was tracking everything, I was really concerned.

This led PI1 to address the roommate who had installed the cameras, but this household member "asked me [PI1] not tell anybody." PI1 continued to describe how this monitoring could be of specific concern to roommates in relationships with others outside the house:

> For other people in the house...they have some relation with other people outside the house. Probably someone here wants to know what's going on or when that person comes.

Conflicts over the feeling of being monitored were also common among parents and children. As PI8 mentioned,

> [We have] about six security cameras set up in main areas mostly for security. But as my son has turned into a teenager, he thinks it's an invasion of privacy. So that's always an ongoing conflict even though that's not the intent of it. That's what he thinks.

PI10 also reported conflicts between parents and children over IoT monitoring, but from the opposite perspective:

> My brothers had a party and it was really loud. So nobody heard that people had been ringing the doorbell. And my boyfriend actually was the first one to ring the doorbell for some reason. And you know when you ring the doorbell there's like a video recording, so my parents got a nice snapshot of my boyfriend bringing in like ten pizzas into the house.

Concerns about and instances of household surveillance using IoT devices were common in the survey responses as well. 40% (204/508) of respondents believed that Internet-connected products could allow people in their household to monitor each others' behavior, and 9% (46/508) reported disagreements about the use of these products for monitoring. A further 15% (78/508) agreed that they had actually used these products to monitor others' behaviors, and 9% (45/508) agreed that someone else in their household had used these products to monitor their own behavior (Figure 4). Comparing across demographic groups, we found that respondents in households with four to six people were significantly more likely to report using IoT devices to monitor others' behavior than respondents in two-person households ($p < 0.01$).

Other researchers have also found that being monitored in the household is often perceived as a risk of IoT devices [59], which could also lead to domestic abuse [6]. Given the increasing popularity of IoT products, the prevalence of monitoring found in our survey means that many households are likely facing new interpersonal conflict concerning actual or potential surveillance enabled by these devices.

5.6 C2. Provoking Differences in Knowledge or Preferences about IoT Devices

We found that a common cause of conflict between household members involving IoT devices resulted from differing knowledge, opinions, or preferences about these devices. Related work has shown the effects of such differences on household power dynamics [10, 17, 40, 41, 63]; the rest of this section offers more specifics and data about the prevalence of this cause of conflicts.

5.6.1 Differing Interest in IoT Technology. A few of our participants had disagreements among family members stemming from different levels of interest and perceived necessity of IoT technology. PS481 talked about disagreements over a smart TV:

> My family and I have always had minor disagreements over our smart TV. My mother doesn't really like the features the TV has and complains about technology in general, saying it's over complicated.

PS208 described a similar conflict around the expense and necessity of IoT devices:

> My parents often argue about the cost of all these Internet-connected devices and if we really need them or not.

In a few cases, arguments about IoT devices placed interests in home technologies directly at odds with perceived optimal conditions for others in the household. PS67 gave one such example of making a simple task more complicated unnecessarily:

> My husband added smart bulbs and taped over all the light switches and switched us over to using Alexa to turn on and off the lights. I don't like it because there are times when my young children fall asleep and I want to turn off the lights silently instead of using my voice. My children don't like it because their pronunciation is not clear and Alexa cannot understand them sometimes when they want the lights on or off. We have argued about it a couple of times but it has been made clear that his excitement for a smart home outweighs the desires of me and our two kids, so now I just deal with it and try to help my kids as much as possible.

Prior work has examined how families with children attempt to repair communication breakdowns with Alexa voice assistants [5], due to pronunciation, code-switching, or other linguistic factors. Our findings indicate that such communication breakdowns can lead to interpersonal conflict in addition to or instead of collaborative troubleshooting. Overall, 14% (71/508) of survey respondents reported disagreements between household members about whether they should have Internet-connected products in their homes, while 22% (110/508) of survey respondents said that they were simply less interested in these products than others in their household (Figure 4).

5.6.2 Differing Concerns about Privacy and Security. Our participants also had differing understandings and opinions of the privacy policies and security features of IoT devices. Some reported that different privacy and security attitudes caused conflicts in their household. For instance, PS159 described disagreements about the privacy implications of an Amazon Echo Dot:

> My partner and I had a disagreement over bringing in an Echo Dot into our household for privacy reasons. I understood where he was coming from, but I thought the convenience outweighed the possible concerns for privacy, as it is in a room we don't use very often.

PS403 reported a similar disagreement that resulted in them returning the device for privacy reasons:

> I bought an Amazon Echo so I could play music with it. My wife was very nervous about it listening to our conversations. I decided to return it to make her more comfortable.

PI2 indicated that disagreements about privacy and security issues often arise when different household members have different opinions about the value of new technology in and of itself:

> Beforehand I was like "are you insane...like is this *1984*...we don't need this," but he, like I said, he's a tech guy. He's an early adopter. He likes to play with whatever the newest thing is.

PI2 also cited uncertainty about how to turn off the microphone on an Amazon Echo or how to use other privacy protection features:

> When she [the Amazon Echo] says "I listen when I hear the wake word" does that mean she's off the rest of the time? Is that what that is? [My housemate] also is pretty into privacy so I'm sure whatever actions there were to scale back her monitoring or recording or whatever...I'm sure he chose them. But I don't know what they are.

Overall, 22% (112/508) of survey respondents disagreed with others in their household about the privacy risks of Internet-connected products (Figure 4).

5.7 C3. Causing Tensions about Device Use, Sharing, and Technical Issues

About half of the participants who reported interpersonal conflicts due to their IoT devices attributed this conflict to how these devices were being used and shared in the household.

5.7.1 Disagreements about Sharing. The most common source of tension between household members was due to different family members wanting to use the same IoT device at the same time and disagreeing over who should have access. This was most prevalent among children and between children and parents. PS141 described such a conflict:

> It's basically just the sharing aspect as far as our children share certain devices sometimes and one child wants to use it a little longer than expected and that's where the disagreements come in. So now we are in the process of getting separate devices for our children.

PI8 also said that simultaneous use of devices can affect the Internet connection more generally:

> When [my son] is using all the devices it slows it down…[and when] I'm trying to work it slows down bandwidth…that's tough.

A few of our survey respondents reported device-sharing conflicts specifically involving IoT thermostats. These disagreements typically occurred between spouses and partners as in the following example from PS19:

> My wife and I often disagree on how to program our Nest thermostat. She likes it to be 70 at night but I feel like that's too cold. Also, the Nest is using my wife's phone proximity to set its Eco Mode, so if I am home and she is not, then I have to take it off of Eco Mode and manually set the temperature.

The multiple-choice survey responses also indicate issues with sharing, with 12% (60/508) and 9% (44/508) of respondents agreeing that who should have control of or access to Internet-connected devices, respectively, had caused disagreements in their households (Figure 4).

5.7.2 Frustrations about Technical Issues. Another common source of tension and arguments among household members resulted from frustrations about technical aspects of IoT devices. For example, PS170 described frustration over technical challenges of their IoT devices as a source of conflict with their partner:

> Either me or my partner sometimes get frustrated when we want to use a product and it isn't working correctly. Then we can take it out on each other.

PS361 described a related situation where one individual's greater technical knowledge led to conflict between spouses sharing a device:

> My husband is not as tech savvy as me and gets irritated with me when I can get a device to do something he can't.

In contrast, PS377 reported that their ability to troubleshoot voice assistants and IoT security cameras was appreciated by other household members but sometimes caused additional tension:

> My parents sometimes want things fixed that are beyond my control. We sometimes disagree about what products to purchase and how they would perform on our network.

These individuals are not alone in dealing with conflicts related to technical issues of IoT devices. 20% (102/508) and 15% (74/508) of survey respondents agreed that these devices have caused tension in their households because they do not work as expected or are difficult to configure, respectively (Figure 4).

5.7.3 Antagonistic Use of Devices. A few of our participants talked about how their IoT devices were used to disrupt and annoy other household members in new arguments and pre-existing conflicts. 15% (75/508) of the survey respondents agreed that these devices were contributing to tensions in their households unrelated to the technology itself (Figure 4). For example, PI11 reported the involvement of an Amazon Echo in unrelated arguments:

> Any time that we try to have a conversation about not using our phones or anything like that, the biggest thing is that mostly my fiance, he turns on Alexa and asks her to play a song and at a really high volume so he can't hear me talk anymore…Sometimes it's really frustrating and sometimes it actually diffuses us because he'll play music.

A parent, PS68, described how their Amazon Echo became a source of fights for their children:

> Our young children "fight" over talking to Alexa. They use Alexa to play songs and will cancel the other one's music, or ask her to repeat them and use her to insult one another.

Another type of IoT device misuse was related to children ordering products online without their parents' permission. PI4 reported this behavior when talking about their experience with Amazon Echo and how their son used it without their knowledge:

> My youngest son has ordered toys or put hundreds of dollars of toys in our Amazon cart and we just caught it at the last second.

These examples indicate that conflict connected to consumer IoT devices can originate both from the devices themselves as well as from the use of the devices to perpetuate or escalate other interpersonal tensions.

5.8 Conflict Mediation

Our participants reported several different methods for mediating conflicts involving IoT technologies. Figure 5 presents the frequency of mediation strategies used by survey respondents who also reported disagreements between household members caused by Internet-connected products. Discussing appropriate use was the most common strategy, followed by settings changes and agreeing not to use certain features of the products. For example, PI1 described a conversation about the placement of security cameras to keep household members from feeling uncomfortable:

> When [my roommate] was setting up the cameras, he proposed to have one camera downstairs like around the entrance. But I said, "No, this is not polite at all to have the camera inside, because it would be like tracking someone's motion, or sometimes you might be dressed in a certain way around the house." So I said, "I think we are very close to each other, and we should not do that in the house." So we don't have...as much as I know...there's [no camera] in the house.

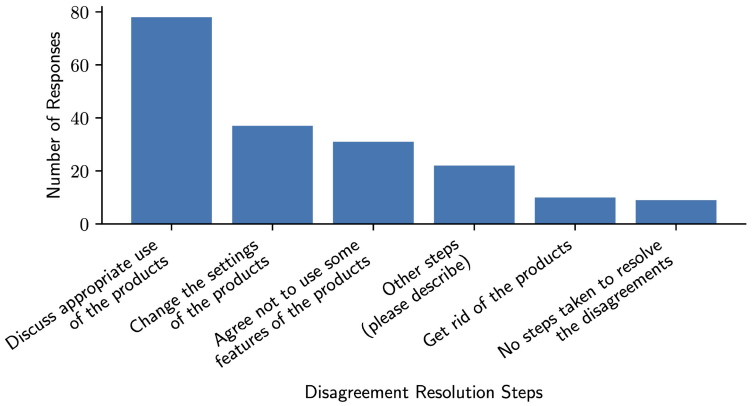

Fig. 5. Prevalence of conflict mediation strategies among survey respondents who reported disagreements with others in their households regarding IoT devices.

Other participants gave other examples of these strategies, including discussing communication issues exacerbated by IoT devices (PI11) and agreeing on schedules for device and bandwidth sharing (PI8). Strategies encapsulated in the "other steps" category (Figure 5) include placing the device in a little-used room (PS233), increasing household Internet speed (PS494), and setting consequences if children misused the devices (PS492).

6 DISCUSSION AND FUTURE WORK

In this section, we explore the implications of our findings concerning interpersonal benefits and conflicts arising from consumer IoT. We first explore possible future research avenues stemming from the benefits that this study has uncovered. We then explore how the conflicts might be mitigated through future research.

6.1 Amplifying Benefits

Our findings suggest that IoT devices can benefit interpersonal relationships by empowering individuals, facilitating certain management tasks, and strengthening interpersonal bonds. Each of these findings offers immediate implications and opportunities for future work.

6.1.1 Design for Strengthened Interpersonal Connections. Previous work has explored the extent to which home automation provides a sense of emotional comfort, as well as how consumer IoT devices can make people feel safer and more secure. Our work builds on these previous results, with nearly half of respondents indicating that IoT devices in the home improved interpersonal relationships through shared experiences, improved communication, and playfulness. Respondents described positive interpersonal experiences involving IoT devices using terms such as "bonding" (PS97, PS73), "laugh" (PI7), "joy" (PI2), "connected" (PS381), and "communicating" (PS21). Devices that reduced the technological complexity or time overhead required for users to engage with others or encouraged playful feature exploration were often involved in these positive experiences. Our study did not, however, dissect which specific design elements are most likely to lead to these positive outcomes or the specific devices that were most likely to cause these positive benefits. Future research could disambiguate these elements and explore how new IoT devices could further enhance the positive benefits we observed, such as by making it easier for users to have shared experiences or by directly encouraging playfulness through interfaces [9] or nudging.

6.1.2 Understanding How Design Affects Empowerment. One of our more surprising findings was that individuals, especially older adults and those with accessibility needs, experienced a sense of increased independence and empowerment (Section 5.3). For example, two participants (PI4, PS445) reported that IoT interfaces were particularly helpful for special-needs children in their households who could independently find media content and other information through the devices. Although this finding emerged as a theme in this study, the benefits of empowerment likely depend on context, as well as the nature of the specific devices that are deployed in a shared household setting. This finding is particularly interesting, because it runs counter to existing work that explores the more pernicious effects of shared IoT devices (e.g., intimate partner violence [22, 25]) and our own result that devices can provide unbalanced utility for different household members (Section 5.6). Future studies could further explore the circumstances under which devices might empower or disempower an individual in a shared household setting. One potential hypothesis to explore is the relationship between an individual's *autonomy* and their sense of empowerment. For example, it is possible that an individual may feel more empowered if they have some control over how a particular device is deployed and used as well as how it collects data about them and others in the household. This hypothesis is supported by the multiple participants who expressed dissatisfaction with the IoT devices in their household related to a perceived loss of control or limited understanding of the devices (Sections 5.5–5.7).

6.1.3 Technology Design for Easier Home Management and Automation. Our findings revealed that consumer IoT technology can provide benefits by making it easier for household members to coordinate management tasks and by increasing free time to spend with one another (Section 5.4). This suggests that designing devices with household management in mind could not only ease the home management responsibilities of individuals but correspondingly benefit interpersonal relationships of users sharing home management tasks. Of particular interest is the result that shared management interfaces can reduce arguments about various management tasks (e.g., locking doors). This suggests that, if certain technologies are deployed more broadly, these effects could be more pervasive across household chores, from cleaning to groceries. Of course, such pervasive deployment also carries associated privacy risks, and thus it is important that future research considers these benefits in light of potential conflicts, as we discuss in the next section.

6.2 Mitigating Conflicts

This study revealed three themes concerning interpersonal conflicts resulting from shared IoT devices: the potential for surveillance and mistrust, unease as a result of differences in knowledge or preferences, and tensions surrounding shared use of devices. We now explore various opportunities for future work concerning each of these findings.

6.2.1 Mitigating Surveillance Risk. Consumer IoT devices unilaterally increase opportunities for surveillance—not only by third parties, but also by other household members. This concern emerged as a significant source of conflict in this study (Section 5.5), which echoes and amplifies a large body of previous work on IoT privacy, tracking, and intimate partner violence [22, 25]. If this surveillance risk is not mitigated, then shared IoT devices could further exacerbate existing power imbalances in domestic settings—particularly in situations where users may have limited autonomy. For example, a roommate may have limited autonomy over what devices another household member deploys in the house, creating a situation of unwanted or unknown surveillance such as that described by participant PI1. A child or teenager may have limited autonomy over audio or visual recording devices installed by their parent or guardian as described by participants PI8 and PI10. A victim of intimate partner violence may not even be aware of the deployment of certain technology, let alone have the capability to control its deployment and use. Such settings may

result in IoT devices either amplifying a lack of trust or a power imbalance that already exists or introducing a new one. Future work must focus not only on understanding these risks but also on allowing users to mitigate them whenever possible. Furthermore, mitigation technology should not be cumbersome or difficult to use. Recent work from Chen et al. [13] on wearable microphone jamming is one such approach for preventing IoT devices from recording audio. More work is needed in this area to provide users with usable technologies to mitigate in-home surveillance.

6.2.2 Improving User Understanding of Device Function. Many household conflicts arise because different members of the household have different understandings of a device's function and may thus reach entirely different conclusions about the benefits and risks of a particular device (Section 5.6). This is supported by our findings, as well as by prior work focusing specifically on IoT voice assistants [23]. Ultimately, even with the same set of facts, different household members may view associated benefits and risks differently, merely as a result of different values or priorities. Nevertheless, our findings suggest that some conflicts could be mitigated if users at least had a common understanding of a device's function, as well as a basic understanding of how to use, reset, and even disable the device if desired. To draw an analogy to the physical world, different household members may have different views on the appropriate thermostat setting, whether to keep the blinds open or closed or whether to turn off the lights when leaving a particular room—such conflicts are inherent, but can be surfaced more directly because all participants know how to operate devices such as blinds and light switches. Similarly, IoT devices could provide "quick start" guides to any user who installs an application on their mobile device to allow all household members to be apprised with the same information about basic function and operations.

A related approach could be to make interaction with IoT devices more tangible. For example, webcams can be equipped with physical covers, and most voice assistants have mute buttons to stop continuous recording. Related research in HCI is already exploring how similar tangible interfaces for consumer IoT devices can make managing privacy with these devices more intuitive [1]. Future work could also explore how these tangible interfaces can be designed to provide "useful intelligibility" [42] specifically to mitigate conflict in interpersonal relationships. We expect that several of the conflicts reported in Section 5.5 could have been avoided by improved notifications indicating to all household occupants when certain monitoring features were active. The exact details of these interfaces would vary by device, but our findings show that they must be accessible and intelligible to all household members, including those not involved in device setup or management.

6.2.3 Designing for Conflict Mediation. We observed conflicts concerning the use of shared devices and resources, from thermostats to Internet connectivity (Section 5.7.1). Past work has demonstrated that making information about resource usage or actions more transparent can help reduce conflicts [14]. Future research could extend this past work into the home IoT setting to better understand whether and how exposing information about device usage and interaction could help mitigate certain sharing conflicts. This research could also reference prior work seeking to provide transparency for mitigating privacy threats in IoT systems [52].

Our study found that individuals sometimes use IoT devices to antagonize other members of their household, such as by using a voice assistant to play a song at high volume (Section 5.7.3). These anecdotes highlight the difference between conflicts caused by devices themselves and unrelated conflicts exacerbated by device use. While household conflict pre-dates consumer IoT, future research could explore interfaces or nudges that discourage the use of these devices to escalate antagonistic behavior towards other household members. This work could draw from prior studies of IoT device use unanticipated by designers [43].

6.3 Designing for Diversity

Households can have many types of relationships, including parents and children of varying levels of independence, intimate partners with individual insecurities and task responsibilities, intergenerational families with different levels of technological familiarity, and many other unique situations. Our results provide further evidence that many IoT devices do not provide settings options with enough flexibility to account for this variety of relationships among household members. In particular, our results suggest that parent/teenager, roommate, and older adult/caregiver relationships are especially poorly served by the default "adult partners with or without young children" model assumed by many device manufacturers. In the case of parents and teenagers, IoT devices can cause conflicts when there is unintended surveillance of teenagers who are in a transitional stage of independence (Section 5.5). When device features do not allow for more complex sharing situations, users must revert to social resolution techniques to negotiate device use, such as agreeing not to use some features or engaging in long-term discussions about appropriate interactions with a device (Section 5.8).

Our findings support existing evidence [31] that IoT device users employ a variety of social and technical approaches to address potential and actual interpersonal conflict arising from these technologies. One potential path forward is to offer additional default settings that cater to common household relationships beyond the nuclear family. For instance, the initial setup for a voice assistant could involve choosing between "roommates," "frequent visitors," "caregiver," "nuclear family," or other such defaults, allowing users in those situations to select these options instead of creating and managing separate accounts for every user—a task that often seems overwhelming due to the technological familiarity required for configuration and the ongoing attention required to use the correct account when many users share devices fluidly. Designing these default settings would force device manufacturers to consider whether their devices are able to gracefully handle a diversity of household scenarios or what additional functionalities might be required. This approach may also inspire further research into what default settings would best cater to specific household situations. As long as these defaults are well-explained during the setup process and provide some flexibility for unique circumstances, they could reduce the prevalence of interpersonal conflicts involving IoT devices.

7 LIMITATIONS

This study has the following limitations, mostly due to the qualitative nature of the interviews, potentially sensitive topic of the research, and representativeness of the participants.

Some interview participants may not have felt comfortable sharing details of their interpersonal relationships with researchers. However, the follow-up survey provided a more anonymous setting for participants, allowing us to uncover additional benefits and harms to interpersonal relationships. Some participants may also have become used to their IoT devices over time and been unable to remember their interpersonal impacts. However, this possibility emphasizes the importance of this research, suggesting that the impact of IoT devices on household relationships may have an even broader scope than we report.

Self-reported demographics indicate that, while diverse, our interview and survey participants were still non-representative in ways that may bias our results. For example, our participants were skewed toward a younger demographic. We chose not to compare our findings across age groups to avoid conflating factors, as our participants often lived households with older or younger members. However, a 2017 survey [35] did observe that 46% of IoT device owners were 26–35 years old, similar to the age range of our participants.

Additional demographic characteristics that we did not collect, such as participant race and elements of socioeconomic status other than income, have also been shown to correlate with

technology use by parents and children. Garg et al. [24] reported these effects for IoT speakers and smartphones, and it follows that they would carry over to other IoT devices as well. Shin et al. [53] point out that the characterization of "the home" in human-computer interaction literature remains narrow and typically does not include alternative domestic configurations, such as collective homes, that are also not represented in this work. These limitations emphasize the exploratory nature of our findings and the need for future research focusing on specific interpersonal effects of IoT technologies in targeted populations.

Our observed prevalence of interpersonal benefits over conflicts may also be due to a participant selection bias. Participants who have decided to purchase and continue using IoT devices may have disproportionately positive sentiments towards these technologies [3]. Future research is needed to understand the experiences of users who choose to avoid or discontinue use of IoT products. Users responsible for the setup and maintenance of the IoT devices in their homes may also have been more likely to respond to our recruitment advertisements. Future research could explicitly recruit participants who live with IoT devices but who were not involved in purchasing or deployment decisions.

8 CONCLUSION

We conducted semi-structured interviews of 13 participants and a followup survey with 508 respondents to understand the impact of consumer IoT devices on interpersonal relationships in multi-occupant households. We identify and categorize the most pervasive positive and negative impacts of consumer IoT devices on participants' relationships with other household members.

On the positive side, we find that IoT devices strengthen interpersonal connections through bonding over shared experiences, simplify remote communication, inspire playfulness, support independence of individuals with special needs, ease household management, improve peace of mind, and increase free time to spend with household members. On the negative side, we find that IoT devices facilitate surveillance and cause mistrust due to potential or actual undesired monitoring and a lack of data collection transparency, provoke differences in knowledge or preferences about the functionality, benefits, risks, privacy, or security of the devices, and cause tensions about device use, sharing, and technical issues that arise during day-to-day operation.

These findings suggest design improvements that would amplify the interpersonal benefits of consumer IoT devices, prevent or mitigate many of the reported conflicts, and support greater diversity of household relationships. For example, devices should more readily support sharing arrangements for multi-generational families and non-familial roommates. Devices should also provide clearer descriptions of data collection behavior to limit conflicts arising from different views of surveillance potential. This article also informs future research, motivating studies of users who have chosen *not* to incorporate IoT devices into their households and closer examinations of IoT devices supporting independence and empowerment.

ACKNOWLEDGMENTS

We thank our study participants.

REFERENCES

[1] 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, CSCW (2020), 116.

[2] Noah Apthorpe, Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan, and Nick Feamster. 2019. Keeping the smart home private with smart(er) IoT traffic shaping. *Proc. Privac. Enhanc. Technol.* 2019, 3 (2019), 128–148.

[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., Wear. Ubiq. Technol.* 2, 2 (2018), 59.

[4] Albert Bandura. 1994. *Self-efficacy. Encyclopedia of Human Behavior (Vol. 4).* Academic Press, New York, 71–81.
[5] Erin Beneteau, Olivia K. Richards, Mingrui Zhang, Julie A. Kientz, Jason Yip, and Alexis Hiniker. 2019. Communication breakdowns between families and Alexa. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–13.
[6] Nellie Bowles. 2018. Thermostats, locks and lights: Digital tools of domestic abuse. *The New York Times* (June 2018). Retrieved from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.
[7] Phelim Bradley. 2018. Bots and data quality on crowdsourcing platforms. *Prolific Blog* (August 2018). Retrieved from https://www.prolific.co/blog/bots-and-data-quality-on-crowdsourcing-platforms.
[8] Broadband Internet Technical Advisory Group. 2016. *Internet of Things (IoT) Security and Privacy Recommendations*. Technical Report.
[9] Barry Brown, Alex S. Taylor, Shahram Izadi, Abigail Sellen, Joseph "Jofish" Kaye, and Rachel Eardley. 2007. Locating family values: A field trial of the whereabouts clock. In *Proceedings of the 9th International Conference on Ubiquitous Computing*. 354–371.
[10] A. J. 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*. 2115–2124.
[11] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. *Health Place* 50 (2018), 112–118.
[12] Caren Chelser. 2018. Alexa? Please ignore my husband. *The New York Times* (May 2018). Retrieved from https://www.nytimes.com/2018/05/04/style/modern-love-alexa-please-ignore-my-husband.html.
[13] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable microphone jamming. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–12.
[14] Marshini Chetty, David Haslem, Andrew Baird, Ugochi Ofoha, Bethany Sumner, and Rebecca Grinter. 2011. Why is my internet slow? Making network speeds visible. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1889–1898.
[15] Bogdan Copos, Karl Levitt, Matt Bishop, and Jeff Rowe. 2016. Is anybody home? Inferring activity from smart home network traffic. In *Proceedings of the IEEE Security and Privacy Workshops*. 245–251.
[16] Aykut Coskun, Gül Kaner, and İdil Bostan. 2018. Is smart home a necessity or a fantasy for the mainstream user? A study on users' expectations of smart household appliances. *Int. J. Des.* 12, 1 (2018), 7–20.
[17] Alexandre Demeure, Sybille Caffiau, Elena Elias, and Camille Roux. 2015. Building and using home automation systems: A field study. In *Proceedings of the International Symposium on End User Development*. 125–140.
[18] Berry Eggen, Gerard Hollemans, and Richard van de Sluis. 2003. Exploring and enhancing the home experience. *Cogn., Technol. Work* 5, 1 (2003), 44–54.
[19] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Proceedings of the 13th Symposium on Usable Privacy and Security*. 399–412.
[20] Pardis Emami-Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The influence of friends and experts on privacy decision making in IoT scenarios. *Proc. ACM Hum.-comput. Interact.* 2, CSCW (2018), 48.
[21] 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 CHI Conference on Human Factors in Computing Systems*. 534.
[22] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proc. ACM Hum.-comput. Interact.* 1, CSCW (2017), 46.
[23] Radhika Garg and Christopher Moreno. 2019. Exploring everyday sharing practices of smart speakers. In *IUI Workshops*.
[24] Radhika Garg and Subhasree Sengupta. 2019. "When you can do it, why can't I?": Racial and socioeconomic differences in family technology use and non-use. *Proc. ACM Hum.-comput. Interact.* 3, CSCW (2019), 1–22.
[25] Christine Geeng and Franziska Roesner. 2019. Who's in control? Interactions in multi-user smart homes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–13.
[26] George Hatzivasilis, Ioannis Askoxylakis, George Alexandris, Darko Anicic, Arne Bröring, Vivek Kulkarni, Konstantinos Fysarakis, and George Spanoudakis. 2018. The interoperability of things: Interoperable solutions as an enabler for IoT and Web 3.0. In *Proceedings of the 23rd International Workshop on Computer-aided Modeling and Design of Communication Links and Networks*. 1–7.
[27] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In *Proceedings of the 28th USENIX Security Symposium*. 105–122.

[28] 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 *Proceedings of the 27th USENIX Security Symposium*. 255–272.
[29] Paul Hitlin. 2016. Turkers in this canvassing: Young, well-educated and frequent users. *Pew Res. Cent.* (July 2016).
[30] Ahmad Jalal, Majid Ali Khan Quaid, and Kibum Kim. 2019. A wrist worn acceleration based human motion analysis and classification for ambient smart home system. *J. Electric. Eng. Technol.* 14, 4 (2019), 1733–1739.
[31] Martin Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring communal technology use in the home. In *Proceedings of the Halfway to the Future Symposium 2019*. 1–8.
[32] Lawrence L. Kupper and Kerry B. Hafner. 1989. On assessing interrater agreement for multiple attribute responses. *Biometrics* 45, 3 (1989), 957–967.
[33] Amanda Lazar, Christian Koehler, Joshua Tanenbaum, and David H. Nguyen. 2015. Why we use and abandon smart devices. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 635–646.
[34] Bojun Li, Piyanuch Hathaipontaluk, and Suhuai Luo. 2009. Intelligent oven in smart home environment. In *Proceedings of the International Conference on Research Challenges in Computer Science*. 247–250.
[35] Shanhong Liu. 2017. *Smart Home Device Ownership Rates in the United States, as of March 2017, by Age Group*. Technical Report. Statista.
[36] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What can't data be used for?" Privacy expectations about smart TVs in the US. In *Proceedings of the European Workshop on Usable Security*.
[37] M. Hammad Mazhar and Zubair Shafiq. 2020. Characterizing smart home IoT traffic in the wild. In *Proceedings of the IEEE/ACM 5th International Conference on Internet-of-Things Design and Implementation*. 203–215.
[38] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The contextual complexity of privacy in smart homes and smart buildings. In *Proceedings of the International Conference on HCI in Business, Government, and Organizations*. 67–78.
[39] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proc. ACM Hum.-comput. Interact.* 3, CSCW (2019), 1–23.
[40] Sarah Mennicken, Jonas Hofer, Anind Dey, and Elaine Huang. 2014. Casalendar: A temporal interface for automated homes. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. 2161–2166.
[41] Sarah Mennicken and Elaine Huang. 2012. Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them. In *Proceedings of the International Conference on Pervasive Computing*. 143–160.
[42] 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 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 105–115.
[43] Margaret E. Morris. 2018. *Left to Our Own Devices: Outsmarting Smart Technology to Reclaim Our Relationships, Health, and Focus*. The MIT Press.
[44] Helen Nissenbaum. 2009. *Privacy in Context*. Stanford University Press.
[45] nVivo Transcription. 2019. Retrieved from https://www.qsrinternational.com/nvivo/nvivo-products/transcription.
[46] Jon O'Brien and Tom Rodden. 1997. Interactive systems in domestic environments. In *Proceedings of the 2nd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*. 247–259.
[47] Xinru Page, Paritosh Bahirat, Muhammad Safi, Bart Knijnenburg, and Pamela Wisniewski. 2018. The internet of what? Understanding differences in perceptions and adoption for the internet of things. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 2, 4 (2018), 1–22.
[48] Heather Patterson. 2013. Contextual expectations of privacy in self-generated health information flows. In *Proceedings of the 41st Research Conference on Communication, Information and Internet Policy*.
[49] Pew Research Center. 2019. Internet/Broadband Fact Sheet. Retrieved from https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.
[50] Prolific. 2019. Retrieved from https://www.prolific.co/.
[51] Irving Seidman. 2013. *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Teachers College Press.
[52] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–14.
[53] Jo Shin, Gabriela Aceves Sepúlveda, and William Odom. 2019. "Collective wisdom" inquiring into collective homes as a site for HCI design. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–14.
[54] Ji-Yeon Son, Jun-Hee Park, Kyeong-Deok Moon, and Young-Hee Lee. 2011. Resource-aware smart home management system by constructing resource relation graph. *IEEE Trans. Consum. Electron.* 57, 3 (2011), 1112–1119.

[55] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–13.
[56] Leila Takayama, Caroline Pantofaru, David Robson, Bianca Soto, and Michael Barry. 2012. Making technology homey: Finding sources of satisfaction and meaning in home automation. In *Proceedings of the ACM Conference on Ubiquitous Computing*. 511–520.
[57] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 129–139.
[58] UserBob. 2019. Retrieved from https://userbob.com/.
[59] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. Benefits and risks of smart home technologies. *Energ. Polic.* 103 (2017), 72–83.
[60] Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourself-style smart homes. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 779–790.
[61] Alexandra Zafiroglu, Heather Patterson, and Faith McCreary. 2016. Living comfortably in glass houses. In *Ethnographic Praxis in Industry Conference Proceedings*, Vol. 2016. Wiley Online Library, 540–540.
[62] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security*. 65–80.
[63] 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 Security Symposium*. 159–176.
[64] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proc. ACM Hum.-comput. Interact.* 2, CSCW (2018), 200.

Received April 2021; revised January 2022; accepted May 2022