NISTIR 8330

Research Report: User Perceptions of Smart Home Privacy and Security

Julie M. Haney
Susanne M. Furman
Yasemin Acar

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8330

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8330

Research Report: User Perceptions of Smart Home Privacy and Security

Julie M. Haney
Susanne M. Furman
Information Access Division
Information Technology Laboratory

Yasemin Acar
Leibniz University Hannover

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8330

November 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8330
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8330, 29 pages (November 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8330

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Smart home technologies may expose adopters to increased risk to network security, information privacy, and physical safety. However, users may lack understanding of the privacy and security implications, while devices fail to provide transparency and configuration options. This results in little meaningful mitigation action to protect users' security and privacy. To better understand users' perceptions of smart home privacy and security, we conducted an in-depth interview study of 40 smart home users. In this document, we report the study findings related to perceptions of data collection/use, privacy and security concerns, and mitigations employed to alleviate concerns. We found that users have varied, and often unclear, understandings of how smart home data are collected and used. In addition, although users may have security and privacy concerns, many participants displayed a willingness to accept risks in favor of smart home benefits, and they feel limited responsibility for mitigating these due to constrained options or lack of knowledge to enact more sophisticated countermeasures. While this report is not meant to be prescriptive, an understanding of user perceptions may be used to inform future smart home security and privacy guidance for manufacturers and users.

Key words

cybersecurity; internet of things; privacy; smart home; usability.

Table of Contents

List of Tables

List of Figures

1. Introduction

The Internet of Things (IoT) market is rapidly expanding, with the number of IoT devices expected to increase from 26 billion in 2019 to 75 billion in 2025 [1]. With this increase, IoT smart home technology is becoming more pervasive, with an annual growth of 31% [2] and 34% of broadband households forecasted to have smart home systems by 2025 [3]. While early adopters of smart home technology have typically been more technically savvy, smart home devices are increasingly being purchased by users who may not understand the technology's privacy and security implications [2]. Within the current dynamic threat and technology environment, the uptick of smart home technology adoption may expose users to increased risks to their network security, privacy of their information, and quite possibly their physical safety [4, 5]. As such, it is imperative that smart home consumers be able to protect the security and privacy of their devices while still being able to enjoy the benefits of the technology.

However, smart home devices may fail to provide transparency of privacy and security protections and configuration options, perhaps because some manufacturers view security as secondary to functionality [6]. Also, privacy may directly conflict with manufacturers' business models of data monetization, so it may be in their interest to obfuscate existing controls while protecting themselves from legal repercussions. In combination with users' lack of in-depth understanding of smart home device technology, functionalities, and privacy and security, there may be little meaningful mitigation actions being taken to protect consumer security and privacy [7–10].

To improve this situation, manufacturers and third parties with influence in the smart home space can follow a user-centered approach [11]. This approach requires empirical evidence of end users' perceptions, needs, wants, and challenges in order to create meaningful and effective privacy and security controls, interfaces, guidelines, and other resources to support users. It is also important to understand what actions users are willing and able to take on their own versus which functions they feel are the duty of or would be better suited to others.

Between February and June 2019, a research team led by the Visualization and Usability Group within the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) conducted an exploratory, semi-structured interview study of 40 smart home users to understand their experiences with smart home devices and their perceptions of smart home privacy and security. We previously published research papers focused on smart home privacy and security mitigations [12], updates [13], and perceptions of responsibility [14]. Therefore, we do not go into detail about these topics in this report. Rather, we describe a subset of study results that address the following research questions (RQs):

RQ1: What are users' perceptions concerning the collection and use of data captured by their smart home devices?

RQ2: What are smart home users' privacy and security concerns, if any?

RQ3: What mitigation actions, if any, do smart home users take to address their privacy and security concerns?

The results revealed perceptions of data collection and use, privacy and security concerns, and mitigations employed to alleviate concerns. We found that users have varied, and often unclear, understandings of how smart home data are collected and used. In addition, although users may have security and privacy concerns, many participants displayed a willingness to accept risks in favor of smart home benefits, and they feel limited responsibility for mitigating these due to constrained options or lack of knowledge to enact more sophisticated countermeasures. This NISTIR is meant to report user-centric research findings that may help to inform smart home security and privacy guidance for manufacturers and users. However, we do not explicitly prescribe guidance or recommendations in this document.

The target audience of this report consists of researchers, designers/manufacturers, administrators, policy makers, decision makers, and creators of privacy and security guidance who perform work related to smart home devices. Users of smart home devices may also be interested in the study results. Readers who are less interested in the research methodology may wish to proceed directly to section 3: Results.

2. Methodology

Between February and June of 2019, we conducted a semi-structured interview study of 40 smart home users to understand their perceptions of and experiences with the devices. Semi-structured interviews follow an established interview protocol while allowing the interviewer to ask unanticipated follow-up questions to clarify or expand upon participant responses.

The National Institute of Standards and Technology Research Protections Office reviewed the protocol for this project (ITL-2018-0118) and determined it meets the criteria for "exempt human subjects research" as defined in 15 CFR 27, the Common Rule for the Protection of Human Subjects. Prior to data collection, participants were informed of the study purpose and how their data would be protected. Data were recorded without personal identifiers (instead using generic identifiers such as P10_A) and not linked back to individuals.

2.1 Participant Recruitment

Eligible participants were adult users (18+ years of age) of smart home devices. A consumer research company did most of the recruitment (33 general public participants), while we identified an additional seven government employees to interview. General public participants were compensated with a $75 prepaid card. All participants lived in the Maryland-Virginia-District of Columbia region of the U.S.

To determine eligibility for the study, prospective participants first completed an online screening survey about their smart home devices, their role with the devices (decision

maker, purchaser, installer, administrator, troubleshooter, user), professional background, basic demographic information (age, gender), and number of household members. After reviewing the screening information, to ensure we found information-rich cases that covered the spectrum of smart home device users, we purposively selected participants for interviews if they had multiple smart home devices for which they were an active user. Despite a review of the screening questionnaire, one interviewed participant (P5) was found not to have any smart home devices (only a smartphone), so was excluded from study analysis.

For the purposes of the study, we defined smart home devices as being networked devices in the following categories:

Smart security: e.g., security cameras, motion detectors, door locks

Smart entertainment: e.g., smart televisions, speakers, streaming devices, other connected media systems

Home environment: e.g., smart plugs, energy consumption monitors, lighting, thermostats, smoke and air quality sensors

Smart appliances: e.g., refrigerators, coffee pots, robot vacuums, washers

Virtual assistants: e.g., voice-controlled devices such as Amazon Echo (colloquially called Amazon Alexa) and Google Home.

Participant demographics are shown in Table 1. Of the 40 participants, 32 had installed and administered the devices (indicated with an A after the participant ID), and eight were non-administrative users of the devices (indicated with a U). Twenty-two (55%) were male and 18 (45%) were female. The majority (70%) were between the ages of 30 and 49 (see Figure 1). Participants were highly educated with 18 (45%) having a master's degree or above and another 20 (50%) with a BS/BA. Thirty-four participants lived in multi-person households, with four couples among the participants (interviewed individually).

Figure 5 shows the general categories of smart home devices in participants' homes. All but one participant had three or more individual smart home devices, with 34 (85%) having three or more different types of devices.

2.2 Data Collection

In addition to the screening survey, we collected data via 40 in-person interviews. Interviews lasted between 22 and 80 minutes, averaging 41 minutes. All interviews were audio recorded and transcribed.

Prior to the interviews, the interview protocol was reviewed by an IoT domain expert to ensure the usage of correct terminology and consideration of reasonable aspects of smart home use. We also piloted the protocol with four individuals to determine face validity of the questions, appropriate use of language, and timing. The protocol was refined based on these inputs.

ID	Gen	Age	Ed	Degree	Occupation
P1_A	F	50-59	M	French, Education	Liaison
P2_A	M	30-39	M	Engineering	Lead engineer
P3_A	F	40-49	M	Law	Professor
P4_A	M	60+	M	Math, Governmental Admin	Retired
P6_U	F	30-39	B	Business	Events manager
P7_A	M	30-39	B	Computer Engineering	Software engineer
P8_A	M	30-39	B	Finance	Federal employee
P9_A	F	30-39	M	Environmental Science	Educationist
P10_A	M	30-39	B	Computer Science	Computer scientist
P11_A	M	50-59	M	Electrical Engineering	Electrical engineer
P12_U	F	30-39	M	Human Resources	Administrative assistant
P13_A	M	50-59	M	Psychology	Manager, Cognitive scientist
P14_U	F	40-49	H	N/A	Information specialist
P15_A	M	30-39	B	Computer Science	Computer scientist
P16_A	M	40-49	M	Computer Science, Biochemistry	Research chief
P17_A	F	30-39	M	Economics, Commerce	Systems engineer
P18_A	M	30-39	B	Social Science	Business consultant
P19_A	M	50-59	B	Business Administration	Retail services specialist
P20_A	F	30-39	B	Business Administration	Administrator
P21_U	F	18-29	B	I/O Psychology	Human resources manager
P22_A	M	30-39	B	Political Science	Executive admin assistant
P23_A	F	40-49	M	Fine Arts, Education	Community arts specialist
P24_A	M	40-49	B	Language, International Affairs	Operational safety analyst
P25_A	M	30-39	B	Finance	Program management analyst
P26_A	M	30-39	B	Finance	Analyst
P27_A	F	40-49	M	Law	Program coordinator
P28_A	F	50-59	B	Philosophy	Consultant
P29_A	M	18-29	M	Anthropology, Museum Studies	Events coordinator
P30_U	F	18-29	B	Theater Production	Event planner
P31_A	F	30-39	M	Policy, English	Lobbyist
P32_A	M	30-39	B	English	Health educator
P33_A	M	18-29	B	Information Systems	Senior technology analyst
P34_A	M	40-49	B	Economics	Financial analyst
P35_A	M	40-49	M	Accounting	Accountant
P36_A	F	30-39	B	Business Management	Project manager
P37_A	F	40-49	M	Business, Education	Assistant principal
P38_U	F	60+	M	Education	Special educator
P39_U	M	60+	M	American Studies	Retired
P40_U	F	30-39	C	Social Science	Customer service rep
P41_A	M	40-49	B	Security	Security

Table 1. Participant demographics
ID: A - smart home administrators/installers, U - smart home users; Gen (Gender); Ed (Education): M - Master's degree, B - Bachelor's degree, C - some college, H - High school.

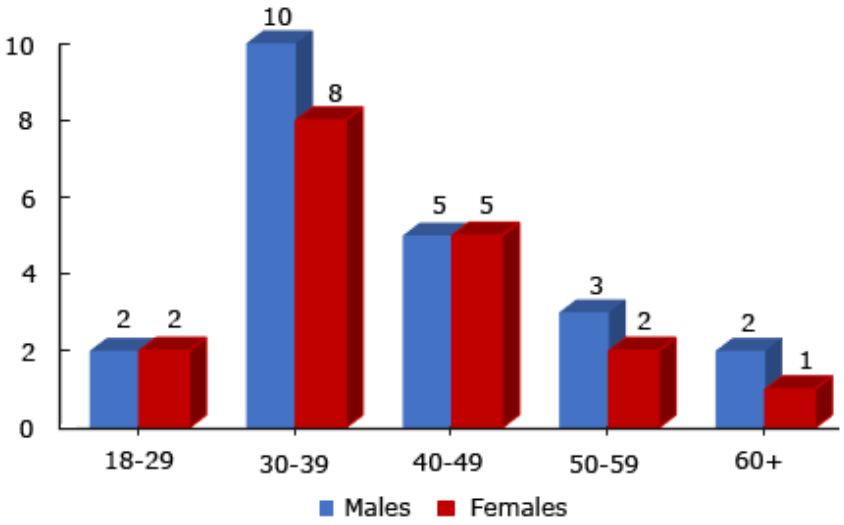

Fig. 1. Participant age categories by gender

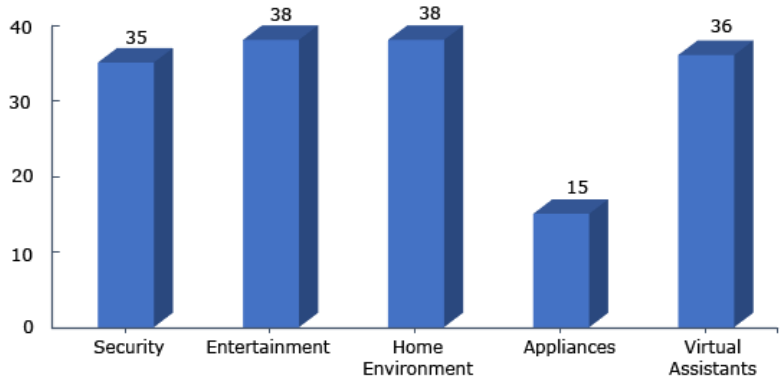

Fig. 2. Types of smart home devices owned by participants

Interview questions addressed several areas in the following order: understanding of smart home terminology; purchase decision process; general use; general concerns, likes, and dislikes; installation and troubleshooting; privacy and data collection/use; security; and safety. In this paper, we focus only on collected data pertaining to privacy and security.

Note that participants may have mentioned privacy and security concepts throughout the interview (for example, when asked if they had any hesitations prior to device purchase), not just during the designated privacy and security portions. Prior to each of the designated privacy and security sections, we provided participants with a short description of each term (privacy and security) in non-technical language to focus their responses. This differentiation ultimately helped us contrast and compare participants' perceptions of each concept as well as where they conflated the two.

2.3 Data Analysis

Data analysis started with coding, which involves categorization of data. In the case of interview data, units of text are labeled based on their topic, with these labels being called "codes." Units may consist of a phrase, sentence, or multiple sentences. For example, the unit of text "the companies that have the information, you know data breaches happen. . . So that was a concern as well" was assigned the code "Data Breach Concerns." We employed both deductive and inductive coding practices, which allowed for an emergence of themes. Deductive coding involves starting with pre-defined codes that the researchers believe will appear in the data. With inductive coding, codes emerge from the data itself.

Analysis of the interview transcripts began with the development of an *a priori* code list based on the research questions. Using the initial code list, each of the three research team members individually coded a subset of four interviews, then met as a group to discuss code application. Related codes were grouped into higher-level categories, called axial codes. For example, the codes "Data Breach Concerns," "Audio/video access," and "Financial loss" were combined into an axial code called "Security Concerns." As part of the final codebook (a list of codes to be used in analysis), all codes were "operationalized," which involves formally defining each code to ensure understanding among all coders.

Using the codebook, we then coded the remaining interviews independently, with each transcript coded by two researchers. Each pair of coders then examined and resolved differences in code application. Throughout the analysis phase, during regular group meetings, we discussed relationships among the codes and our interpretations.

2.4 Limitations

As with any interview study, participant responses are subject to recall, self-report, and social desirability biases. In addition, the participants, who were generally highly educated professionals in a high-income metropolitan area, may not be fully representative of the overall smart home user population in the U.S. However, our study population appears to mirror smart home adopters characterized in prior industry surveys [15]. We also acknowledge that U.S. smart home users may have different privacy and security attitudes from

those in other countries, for example, due to political or cultural factors related to privacy expectations and tolerance. In addition, our study only captures perceptions of smart home adopters of multiple devices, so does not adequately capture those of limited adopters or non-adopters. These limitations could be addressed with replication of this study in other countries or a global quantitative survey informed by the results of our study. However, even with its limitations, the study serves as an exploratory investigation that can inform subsequent surveys of broader populations.

3. Results

In this section, we report results from a subset of the interview data specific to privacy and security. Note that these results often describe participant perceptions, which may or may not reflect reality.

Example quotes from participants are provided throughout. Counts of participants mentioning specific topics are provided in some cases, not as an attempt to distill our qualitative data to quantitative measures, but rather to illustrate weight or unique cases.

3.1 Smart Home Data

We asked study participants several questions related to their perceptions of smart home data collection and usage. We summarize their responses in this section.

3.1.1 Collection

Participants were asked what data, if any, they thought their smart home devices were collecting. Most were aware that data were being collected but provided different levels of specificity as to the kinds of data. Types of data mentioned during the interviews included home environment readings, energy usage, issued commands, audio, video, entertainment viewing, and account and service subscription information, among others. One participant described his perceptions of collected data:

> *"I'm sure that the [smart thermostat] is collecting, I know it's collecting how hot I'm heating the room, how long it's being heated, time periods which it's being heated... The plugs, I'm sure they collect how long they're on for, how frequently they get turned on and off, how much power it's providing to the external outlet" (P10_A).*

A technically-savvy, do-it-yourselfer created a separate segment on his home network that only contained smart home devices. He regularly monitored the traffic leaving the network, observing as much as possible the kinds and volume of smart home data sent out of the network even though much of it was encrypted:

> *"I know they are collecting environmental data. I know they are collecting certain event data, and, unfortunately, I know they're also collecting voice*

> *data inside the premises. I also know they are collecting our energy usage profiles…There's packets attempting to leave every day. Yesterday I ran a profile. There was six megabytes of data that was trying to leave the network" (P16_A).*

Participants with virtual assistants or smart cameras discussed the "always on" mode of these devices and how audio and video are collected and stored. A smart security camera owner said, *"I know it's always recording. So it's recording all your conversations around it, pretty much just recording everything you do and uploading it to the cloud" (P22_A).* A participant with a virtual assistant commented, *"I know it records and stores every command that you give it, because you can retrieve them in the app, and you can actually play the recording of you saying whatever you said" (P24_A).*

Participants also mentioned data collected when setting up an account, for example via companion apps on their smart phones:

> *"All these devices require an account, so you're giving them your email and you're probably opting in, whether you know it or not, on them sending your information to third parties. So they now have your name, in a lot of cases your address, phone number, maybe even a cell phone number, your email address, and whatever password you associate with that email address" (P11_A).*

Another participant spoke about payment information being collected by smart entertainment subscription services: *"If you're doing it through the TV itself, you're going to have to set up an account and then put in your credit card information" (P20_A).*

Others were less specific about the kinds of data they thought were being collected. One participant thought that his devices were collecting *"everything it sees, everything it hears, everything you input into it, all the data you provide. I think it collects all of it somewhere" (P26_A).* Another talked in broad terms about information being collected from his smart entertainment devices: *"I'm sure they're collecting what you're watching, kind of your habits. I'm sure they're collecting a lot of stuff that I don't even know about" (P18_A).*

3.1.2 Destination

We asked participants where they thought collected data go. Twenty-three participants thought that data are sent to the smart home manufacturer. Eight of these made specific mention of the manufacturer's cloud or cloud service as a destination. For example, one participant said, *"Devices that are collecting sensor information, all that sensor information leaves your house and is stored in a cloud service" (P11_A).* Others referred to manufacturer servers or databases: *"it goes to the companies, I guess their servers, a database" (P28_A).*

Some participants expressed uncertainty about whether manufacturers send the data elsewhere after receiving it, as demonstrated by one participant who commented, *"hopefully they're not selling it. We don't know" (P28_A).* Another remarked:

> *"I know for a fact, the way the [virtual assistant] and the other voice-based smart devices work is every audio segment that it records gets sent back to a server to be analyzed. And what they do with it after it's received is a little bit of a question mark" (P15_A).*

Thirteen participants believed that manufacturers transferred or sold smart home data to third parties, most often advertisers. One participant commented, *"I'm pretty sure they're selling that information to different advertisers... because the best way to make money is through ads that are specifically targeted to exactly what the person needs" (P22_A).* A user believed *"companies get this data and send it over to marketing firms" (P21_U).*

Still others thought that the government was directly collecting smart home data (6 participants). P14_U thought that data go *"to Big Brother pretty much. CIA"* Another participant went into more detail:

> *"I assume it's compiled somewhere in a research lab of the government... And I can only imagine there is some like poor sap somewhere in the government who has to weed through like thousands and thousands of data... to maybe find something. But I assume it's just some basement in the government" (P30_U).*

Finally, several participants provided vague answers to the question about data destination. Five talked about the data going out to the internet in general, e.g., *"Up in internet world" (P12_U).* Four others were not sure. For example, one said, *"I kind of think that it goes nowhere... Who knows?" (P23_A).* Another expressed apathy: *"Who knows?... I guess, who cares, is my answer" (P8_A).*

3.1.3 Use

Participants were asked how they think the data collected by smart home devices are used. Several believed that data are analyzed by manufacturers for product improvement purposes. From a functionality perspective, one participant commented that his smart vacuum cleaner *"was sending back maps of the area that it's cleaning and scoping out, so it can improve and build better maps" (P13_A).* Another remarked, *"I'm sure they're also collecting information about the device, if it's faulty or if you know maybe how quickly their customer support team reaches out to us" (P28_A).* Data analysis was also viewed as a way to improve future versions of the product or inform the design of completely new products. A participant believed that, through data collection, manufacturers *"study consumers' habits, the behavior, so that will help them to come up with better products to solve their needs" (P36_A).* An owner of a smart thermostat viewed the data as contributing to a larger effort to save energy: *"it definitely goes into a database where they collect and analyze that information which actually, I'm okay with. If it's going to save the environment, sure" (P6_U).*

As also reflected in participant responses related to data destination, many of the interviewed smart home users thought that data are used by the manufacturer or third parties for

targeted advertising. One participant said that manufacturers are *"doing data mining... It's not malicious I don't think. I mean everything about it is to sell you a product, everything about the internet is to sell you a product" (P40_A)*. Another thought that manufacturers or third parties *"take that information and potentially target emails with advertisements to you, because they know where you live, they might know what type of devices you have in your house" (P11_A)*. A user talked about data being sold *"to agencies that do these surveys to kind of figure out what's popular out there in the market" (P21_U)*.

A few participants saw a use of smart home data by law enforcement agencies when needed. One remarked, *"If there's a microphone in your house and they have a warrant to collect information, they'll use it" (P2_A)*. Another talked about the value of law enforcement having access to audio logs: *"For criminal cases or if something really happens that's scary or bad, it would be really good to have a way to play that information back"* (P23_A).

Finally, several participants personally made use of the data to monitor what is going on in their homes. For example, one discussed how she uses data from her smart door lock to monitor entry to the home: *"We have a maid that comes in on Wednesdays. We know exactly when she comes in the house, when she leaves" (P14_U)*. Another talked about benefits of looking at the data collected by his smart thermostat:

> *"If there's something I notice in that data that's actionable, I'll try to take action... With the HVAC system, if I'm noticing that it's running a lot more than I would like it to or expect it to or it's not affecting the temperature change as quickly as it should, then that might tip me off that it's time to change a filter. Or maybe I want to check if any windows are cracked or if there are any leaks, any areas that I want to insulate, things like that. I mean, it has tipped me off to the furnace having problems running and starting, things like that" (P15_A).*

3.1.4 Policies

Multiple interviewees discussed how device and manufacturer privacy policies and user level agreements are meant to provide information on data collection and use, but few found that information to be satisfactory or easily understood. One participant talked about manufacturers providing privacy-related information: *"Sometimes I think, by law, they might have to update, or at least send out, their information on privacy, what data are collected, et cetera... It's laborious, it's in lawyer speak" (P31_A)*. Another commented:

> *"There's the end user licensing agreement for everything that's 100 pages long, no one ever reads. But everything is disclosed in there if you care to read it, which nobody ever does. I don't think I've read one my entire life" (P40_A).*

Several participants expressed a general lack of trust related to manufacturer's reported data collection policies. For example, one smart home administrator commented:

"I don't have much trust in what companies say they collect and don't collect. I think they collect what they can and use it. Even if they say they're not collecting it, I think it's being used somehow" (P10_A).

Another participant reflected, *"I don't trust the information that's provided, so I don't really believe that when they say they're transparent, that they really are" (P22_A).* A smart home owner discussed how he believes control options for data collection are set to the advantage of manufacturers: *"I feel like the default is always full access, so you have to really look for and pursue stricter settings" (P18_A).*

3.1.5 Control

Interviewees were asked in what ways, if any, their device or the device manufacturer provides a means to control or manage what information is collected and how it is shared. Several said that they did not think there was a way to control the information (7 participants) or that they did not know (11 participants).

A few mentioned specific control options. A smart home administrator who owned a number of devices answered:

"Depends on the device. Like the light bulbs and the plugs give you nothing. The [smart entertainment device] gives you a couple of choices between usage statistics and problem, like if there's a failure or something... It gives you the choice to automatically report like a crash. But it also gives you the choice like if you just want usage statistics to be sent to [manufacturer], which I don't. So the thermostat's like that too, you have the choice send them extra information for their diagnostic, whatever that means, purposes" (P13_A).

Another participant spoke about settings she remembered seeing on her devices:

"They have choices where you can say send your data, or don't send your data, or like I said the [virtual assistant] has a 'delete your history daily,' or store it for whatever. I forgot what the other options were, but I just automatically chose delete it daily" (P27_A).

Several participants were vaguely familiar with some data collection settings, but not sure about all options available to them. For example, one participant commented:

"I think I've read that [virtual assistant] has the option to delete some information. I know that there's a physical mute button on the side of them that you can flip... It turns everything off. I don't know about anything beyond that. I don't know enough about whether or not there's a way to control what specifically it deletes, or if I can be like, delete everything" (P29_A).

Several remarked that opting out of certain data collection practices can be difficult. Two participants were aware that a letter had to be sent to the manufacturer in order to opt out, with one of those saying, *"There's an opt-out thing that no one's ever going to do... I saw the address, a mailing address, and I, out of curiosity, was like, 'What is this mailing address for?' It was the opt-out" (P3_A)*. Another smart home owner was resigned to the fact that she did not have much of choice with respect to opting in or out of data collection: *"at the end it's like, okay, if I want to use this device, I have to opt in" (P17_A)*. P41_U was also resigned: *"No one reads the agreements. We just want to use our device, so we just agree to it, I guess."*

3.2 Concerns

In the first half of interviews, participants were asked if they had any hesitations prior to device purchase, if they had any general concerns about their smart home devices, and what other members of the household thought about the devices. Two-thirds of participants mentioned privacy-related concerns and half acknowledged security concerns in the context of these questions. These unprompted mentions offer interesting insight into whether privacy and security concerns are in the forefront of users' minds.

Participants were later explicitly asked about their privacy and security concerns. In some cases, participants were personally concerned about privacy or security but to varying degrees. Other participants mentioned concerns that were expressed by others (e.g., family members, friends, media) but not personally held. For example, one participant mentioned a disparity in privacy concerns between him and his partner: *"The [virtual assistant], I didn't have any hesitations. My fiancé did because she doesn't like being listened to all the time" (P10_A)*.

The most frequently mentioned concerns for both privacy and security are summarized in this section. For each category of concern, we indicate whether the concern was mentioned only in the privacy context, only in the security context, or both. Fig. 3, 4, and 5 show the number of participants expressing each type of concern. Note that some participant concerns fell into multiple categories. For example, a concern about the government eavesdropping by accessing audio collected by virtual assistants falls under both the "audio/video access" and "government access" categories.

3.2.1 Audio and Video Access

The most frequently mentioned concern from both a privacy and security perspective was access to audio and video recorded within the home. Some were uneasy about manufacturers collecting this data. For example, one smart home user talked about her husband's concerns when he is teleworking: *"My husband's paranoid [virtual assistant] is listening to him about conversations about work" (P12_U)*.

Others were concerned about unauthorized people gaining access to the device. A participant spoke about his wife's hesitancy about the smart cameras in the home: *"I think she's concerned about someone hacking into the cameras and watching us" (P2_A)*.

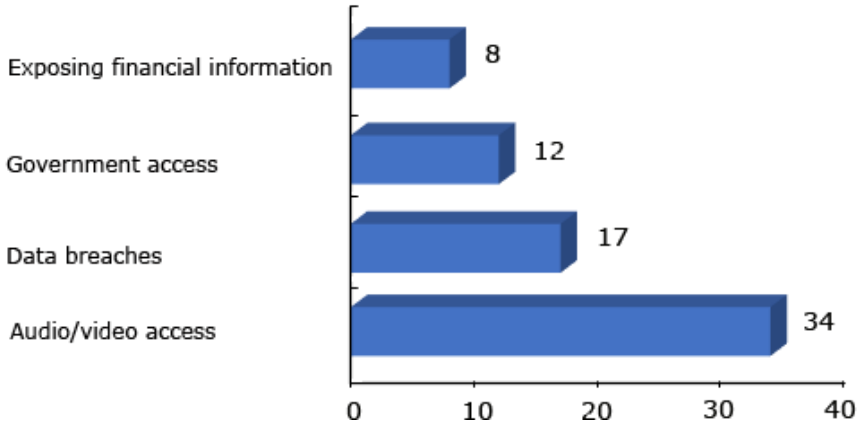

Fig. 3. Concerns mentioned in both the privacy and security contexts

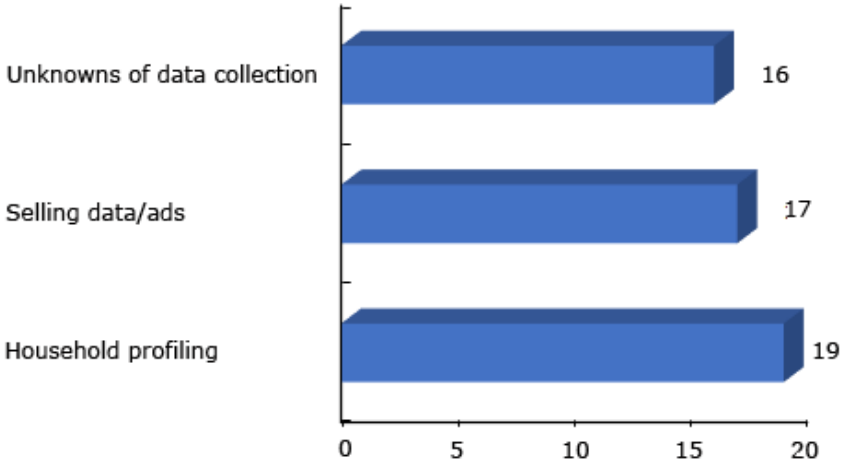

Fig. 4. Concerns mentioned in the privacy context

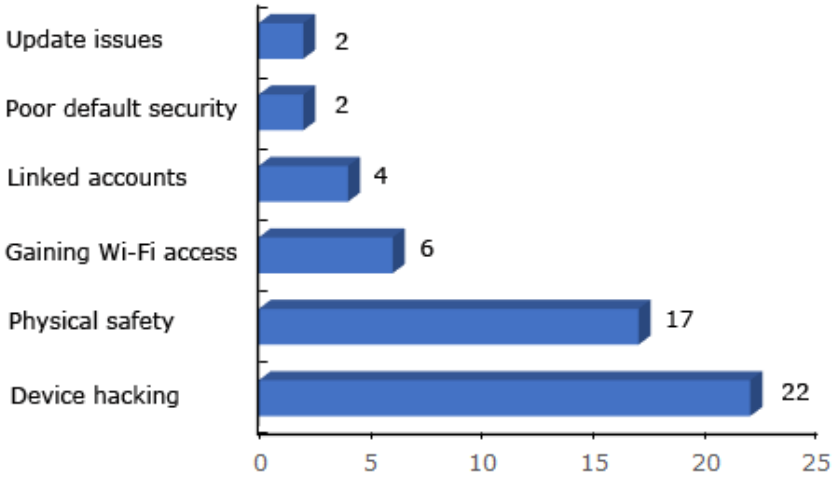

Fig. 5. Concerns mentioned in the security context

Two participants expressed concern about there being recording mechanisms in the devices without their knowledge. One said, *"I recall a couple of years ago, [manufacturer's] smart TVs, I think it was, had a built-in camera that the users weren't aware of. So having stuff like that that I'm not aware of is a bit concerning" (P22_A).*

In some cases, participants made a conscious decision not to purchase or use devices that record audio or video because of their concerns. One participant, although owning many other smart home devices, did not own a virtual assistant, saying:

> *"I'm too concerned about the privacy with a device in my home recording audio constantly. So that's one I purposely stay away from despite being very interested in lots of the other smart devices. That one crosses the privacy line for me" (P15_A).*

P28_A received a virtual assistant as a gift but had not yet decided whether to install it because of news reports she had seen:

> *"We've heard some really weird things. You know, like [the virtual assistant] talking back and laughing. Isn't that crazy? I don't know. Somebody is manipulating it somewhere to spook people out, or just pranksters. But I'm just debating on whether or not I want to use it" (P28_A).*

3.2.2 Data Breaches

The possibility of unauthorized individuals accessing smart home data stored by manufacturers was frequently mentioned in both the privacy and security contexts. One participant described his concern:

> *"With most of these systems, the information's going back to a central server that's operated by the company that provides the device. And with that said, I know that's a potential area where someone else could gain access to that information. So I'm very conscious about do I even want that information out there" (P15_A).*

A user was concerned about potential data leaks because she was not sure about *"the security around, if any, the information that's being stored" (P21_U).*

Multiple participants mentioned high visibility data breaches during the interview as a point of reference. Although not directly involving smart home device manufacturers, these breaches eroded overall trust in companies' abilities to protect consumer information. One participant talked about these breaches as he believed smart home device manufacturers may also be susceptible: *"You hear people's data has been compromised, which seems to be happening fairly frequently, where you're signed up as part of some kind of database. It's being hacked" (P4_A).* Another expressed his lack of trust:

> *"These big corporations can say they're going to protect your data but it's almost like they can say what you want but they really can't protect it... I think if you put your information out there you have to be ready for it to get hacked" (P33_A).*

3.2.3 Government Access

Several participants were concerned about national governments gaining access to smart home data, especially audio and video. This concern was discussed in the privacy context with respect to surveillance and the security context related to governments possibly hacking into smart home devices.

Among those concerned about the U.S. government obtaining the data, one participant opined, *"Just from a general big brother perspective, I think you're naive to think that we're not being watched and the government is overreaching" (P26_A).* Others were worried about foreign government espionage. A user said, *"we have so many other countries that are trying to hack into our accounts" (P12_U).* Another participant was concerned about supply chain issues with smart home devices: *"there's chips in there to where even the manufacturer may not even be entirely sure that the [foreign government] is monitoring what they're doing with the device" (P3_A).*

3.2.4 Exposure of financial information

Several participants expressed concerns that their personal financial information could be obtained should their smart home devices be hacked (security context) or if their information be divulged (privacy). Some of this concern stemmed from payment and contact information stored as part of an account for a smart home app or service. For example,

one participant commented, *"while I don't care what people see on my [smart entertainment device], I would care if they see my credit card information" (P37_A)*. A smart home device administrator put financial concerns above other types of privacy:

> *"I don't really care about my privacy more so that I care about money... If they just watch my [streaming service], no big deal. But if... someone got in my bank account or even my email... they could... figure out how to get to my money" (P2_A).*

Another said that her biggest concerns were financial: *"bank account because, in that case, you could lose money and they actually wouldn't bring it back. Identity purposes, I don't want my credit being affected because then they can get a whole host of other issues going on" (P17_A).*

3.2.5 Household Profiling

One of the concerns mentioned in the privacy context was the profiling of household members, including their pattern of life, what kinds of things they like, approximate ages of household members, and *"the literal movements of our family,... the times that we're there and the times that we're not, and who's there" (P1_A)*. Profiling could be accomplished by looking at individual pieces of data collected by smart home devices but most often when examined in aggregate, as discussed by one participant:

> *"Any information they record is typically about how the device is being used and certainly indirectly you could infer some things. And certainly having access to the data from all of my devices together you can probably build a picture about my daily habits" (P15_A).*

3.2.6 Selling of Data and Targeted Ads

Also within the privacy context, many consumers suspect that the data collected by their smart home devices is being used for targeted ads, either by the manufacturer or by other companies that buy the data. As one participant remarked, *"All these companies, they're mining our data. They're trying to see what they can eventually sell us, or sell our information to somebody" (P28_A)*. While some participants were not bothered by this, others were. One smart home owner commented, *"I hate targeted ads. I hate them with a passion" (P17_A)*. Another expressed his discomfort with a perceived correlation about commands his family gives to their virtual assistant and ads they see on other online platforms:

> *"The amount of times we've said a word and all of a sudden seen ads for things is way too high to be not a thing, so that kind of weirds me out... I think most of these companies are a little too hungry for ad info, and so they just take anything and everything, regardless of how creepy it can be. Sometimes it's a little too personal"* (P29_A).

3.2.7 Unknowns of Data Collection

About 40% of participants were concerned that they did not have a good grasp on smart home device data collection and usage, which led to privacy concerns. One participant commented, *"You have no idea when it's communicating to the manufacturer or what it's communicating to the manufacturer. And I think the privacy aspects of that are underappreciated" (P13_A)*. A smart home do-it-yourselfer discussed challenges finding ground truth about data collection:

> *"Unless you really monitor what's going out of your network, you really don't know what the devices are broadcasting. There's really no firewall that is looking at whether the devices are broadcasting what they're supposed to. For instance, is your [virtual assistant] device, is that actually listening to more than what you would expect it to? Is it relaying information out? Same with a video camera,... doorbell, whatever type of device. Is it doing more than you think? Are there functions inside of these devices that are not advertised, but capable of doing things?" (P11_A).*

One smart home device owner lamented that privacy policies and user level agreements are typically not transparent about data collection: *"You don't really know what they're collecting because they can use language to mislead you. It's legal, but misleading" (P31_A).*

3.2.8 Device Hacking

Within the security context, participants mentioned that they were concerned about their devices being hacked by unauthorized or malicious actors, as expressed by one participant who worried that hackers would be able to *"shut off, or dismantle, or mess with the system that I have in place" (P37_A)*. In fact, the threat of device exploitation underpinned many of the privacy and security concerns discovered in our study. For example, exploitation could lead to unauthorized individuals gaining access to audio and video feeds. Governments could hack into devices or their companion apps for surveillance purposes.

Several discussed the potential ease and perceived inevitability of their smart home devices being hacked. One remarked:

> *"It's as simple as username and passwords... All these apps also have a back end where you can go and pull it up on the Internet. For example, I go to [website] to pull up my cameras... If you just stole my username and password, again, you have the same access" (P8_A).*

Another was pessimistic about having any sense of security:

> *"I would not entrust my security in any way to any of these devices to be honest. It may not be the fault of the device itself. Any type of connectivity that you have to the internet is hackable, and if it's not, tomorrow it will be. If they haven't figured how to break through some firewall, somebody will (P40_A).*

One participant was concerned about smart home vulnerabilities in certain types of devices based on conversations he had with colleagues in which he learned *"each manufacturer is actually just borrowing security APIs instead of creating their own, and the APIs specifically have holes in them. So the same vulnerability is being propagated across vendors" (P13_A)*. Others were concerned based on their exposure to news stories about smart home devices being compromised. For P34_A, one such story prompted him to be more suspicious of his devices:

> *"There was just an article I read about all the smart devices and now how they stole people's information. And, I'm a little hesitant. So with my security camera,... sometimes I feel, you know it takes pictures without my consent. And I feel some information is going somewhere that I have no control over" (P34_A).*

3.2.9 Physical Safety

Participants believed that security vulnerabilities and device hacking could also result in safety consequences since smart home devices often have the ability to make changes to the physical environment. For example, since many of the participants owned smart thermostats, there were concerns about hackers being able to control the heating and air in the house, which could impact the physical well-being of household members. One smart home user wondered, *"what if someone hacks into our phones and... with the [smart thermostat] they try to change the temperature if we've already set it and they go in and they try to reconfigure it on their own?"* (P12_U).

Others were concerned that malfunctioning or hacked devices could allow intruders easier access to the home should smart alarm systems or security cameras be disabled. A user with a smart door lock said, *"If somebody could hack our system, they could easily open our front door" (P14_U)*. P31_A commented, *"If criminals were wise enough, they'd just knock out the wireless and enter these homes."* Another participant talked about potential dangers if his smart garage door opener was exploited:

> *"I would say that it actually could be detrimental to my safety because who knows if it's hackable and they can get into my house. I just gave you the entryway. So, you don't need to pick a lock at all. You just got to get into my Wi-Fi" (P8_A).*

Related to the household profiling concern, information collected by smart home devices, if accessed by unauthorized individuals, could provide insight into when a home is or is not occupied, thus facilitating the timing of home invasions. One participant remarked, *"If somebody is... actually able to associate when you're home and when you're not home based on the sensors and other things you have in your house, they could potentially target you" (P11_A)*. Another said:

"I specifically did not get a smart thermostat because I thought that it would be an easy way for somebody to hack in and figure out when you're home and when you're not home. So, you know, if you can get into the system and say, it's set to 78 [degrees Fahrenheit] until 5:00, and then it goes down to 72" (P18_A).

3.2.10 Other Security Concerns

Three other security-specific concerns were revealed during the interviews. Several participants were concerned about unauthorized individuals gaining access to the Wi-Fi network and other devices on that network through smart home devices, as noted by a participant: *"I use my phone for everything, and it's connected to my Wi-Fi. My Wi-Fi's connected to my smart home. So I'm not a hacker, but I'm sure they find ways" (P41_U).*

Four people were worried that access to other linked accounts, e.g., email and social media accounts, could be gained by exploiting smart home device apps, especially if passwords were common across accounts. For example, one participant said, *"Our [app] account is associated with an email. So if you were to hack into it, you have my email and then from my email you can get anything else" (P30_U).*

Two participants mentioned a concern with devices having poor default security settings. One commented, *"One of the areas of concern with these would be if they have default passwords out of the box that are easily looked up, easily found on the internet" (P15_A).*

Finally, two expressed hesitations with smart home device updates from a security perspective. As one smart home owner said about manufacturers, *"They're able to change your stuff in your house... So there's some kind of access from the outside" (P26_A).*

3.2.11 Lack of Concern

We also found examples of various levels of lack of concern, with seven participants having neither privacy nor security concerns. In 24 cases, participants did not value the information collected by smart home devices, believing they would not be a worthwhile target. For example, one participant remarked, *"I feel like you've got people who are pretty talented with computers and can get this stuff... I'm of the mindset, have at it. We don't do anything cool in my house, anyways" (P8_A).*

We also identified evidence of privacy resignation [9] in which users believe that their data are already publicly available via other means (e.g., social media, prior data breaches, etc.), and that there is nothing they can do about it (8 participants). A participant expressed this resignation when she said, *"If you don't think people have all of your information already, you're crazy" (P17_A).*

Finally, five participants viewed hacking as a nebulous concept with a low probability of occurrence, especially among those who did not think they would be interesting enough to target. For example, a participant commented, *"Some people are concerned about hacking,*

but that seems to be kind of a remote thing that people would be interested in doing" (P3_A).

3.2.12 Risk Acceptance

Although some participants had concerns, they ultimately made a conscious choice, described as *"willful ignorance"* by P1_A, to accept privacy and security risks in exchange for perceived benefits. One participant expressed this as *"Does the good outweigh the bad? I made the decision that, yes" (P8_8).* Purchase decision and continued use signaled that risks did not cross users' privacy/security threshold [16]. For example, one participant believed that the government was monitoring his smart home information but felt *"This is the risk you take by getting a smart home... You don't like it, go off the grid" (P26_A).* Another discussed the trade-offs of owning smart home devices: *"I know that it's collecting personal data,... and I know there's the potential of a security leak, but yet, I like having the convenience of having those things" (P1_A).*

3.3 Mitigations

During the privacy and security portions of the interviews, participants were asked if they performed any mitigations to alleviate their concerns. Although we summarize mitigations in this paper, a more in-depth discussion of protective measures identified in the study is included in another paper [12].

Mitigations, along with examples given by participants, are shown in Table 2. We observed that all the identified mitigations were discussed at least once within both the privacy and security contexts as participants often conflated the two concepts or mitigations were viewed as being effective for both. We also noticed that most mitigations mentioned in the interviews were rather simplistic, for instance, setting a device app or Wi-Fi password.

We explored reasons why some participants do not take mitigative actions. Obviously, some were simply not concerned enough to put forth the effort to take any action. Others were not aware of available options or were not given options. For example, one smart home user commented, *"I've been given very little methods to alleviate the concerns. Usually the description of the controls aren't specific enough for me to alleviate my concerns" (P13_A).* Another said, *"I can only image what you can and can't turn off. There's probably some things. Whether or not that actually happens or the user just thinks that it's turned off, I don't know" (P2_A).*

Some lacked the knowledge to choose effective mitigations, especially within the security context. For example, P34_A commented, *"I'm not really like an IT guy, or like tech savvy... There's just so little I can tell about that."* Another participant said, *"I know it is password protected. That's as far as my knowledge. I don't know more than that. I'm not certified with cybersecurity" (P41_U).*

As with concerns, we also observed the influence of privacy resignation as well as loss of control and fatalism, which are characteristics of security fatigue [17]. One participant

Mitigation	#	Examples
Authentication	17	setting or changing passwords on device apps, using facial recognition/biometrics
Limiting audio and video exposure	16	not locating devices in certain rooms, restricting conversations when near devices, unplugging devices in certain situations
Home network configuration	14	network segmentation, setting a Wi-Fi password, using virtual private networks (VPNs)
Configuring device options	12	disabling automatic ordering, history, and error reporting
Limiting information in apps	8	using fake information or infrequently-used email addresses
Device selection	7	choosing devices with strong security/privacy features, buying products from trusted vendors
Limiting access	5	limiting access to codes/passwords, placing orders from computer instead of from virtual assistant
Updates	3	applying app and firmware updates, upgrading products

Table 2. Privacy and security mitigations
- number of participants mentioning the concern

exhibited this resignation when he said, *"I just kind of assume if it exists, there's a way to hack into it" (P18_A).*

4. Conclusion

Via in-depth, semi-structured interviews, we investigated users' perceptions of smart home privacy and security. Our results suggest that users often have incomplete knowledge of what smart home data are collected and how they are being used. Despite having privacy and security concerns, users often accept risks as a tradeoff for perceived benefits. We also found that concerns do not always result in taking mitigative action for a number of reasons, most centered on lack of available options, transparency, or knowledge.

The examination of users' perceptions of smart home privacy and security can begin to inform possible ways in which a diverse range of users can be more empowered to take protective actions for their smart home devices and feel more comfortable when introducing these devices into their homes. These might include improvements in the usability of privacy and security mechanisms or options that manufacturers could provide in their products.

Acknowledgments

The authors would like to thank Mary Theofanos and Brian Stanton for their contributions to the initial study design and Michael Fagan and Kevin Mangold for their reviews and comments.

References

[1] Statista (2019) Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Available at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[2] GutCheck (2018) Smart home device adoption. Available at https://resource.gutcheckit.com/smart-home-device-adoption-au-ty.

[3] Ablondi B (2019) Connected consumer: Chairperson's opening remarks at the Internet of Things World Conference.

[4] Duffy TF (2018) Security and privacy in the connected home. *Center for Internet Security Newsletter* Available at https://www.cisecurity.org/newsletter/security-and-privacy-in-the-connected-home/.

[5] Fu K, Kohno T, Lopresti D, Mynatt E, Nahrstedt K, Patel S, Richardson D, Zorn B (2017) Safety, security, and privacy threats posed by accelerating trends in the internet of things (Computing Community Consortium Report 29, no. 3), Available at http://ecl.cc.gatech.edu/sites/default/files/publications/2619facd570a34becd8e3fa41d5f99da10e2.pdf.

[6] Fagan M, Megas KN, Scarfone K, Smith M (2020) NISTIR 8259 Foundational activities for IoT device manufacturers. Available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

[7] Abdi N, Ramokapane KM, Such JM (2019) More than smart speakers: Security and privacy perceptions of smart home personal assistants. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* SOUPS '19 (USENIX), pp 451–466.

[8] Zeng E, Mare S, Roesner F (2017) End user security and privacy concerns with smart homes. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security* SOUPS '17 (USENIX), pp 65–80.

[9] Lau J, Zimmerman B, Schaub F (2018) Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* CSCW '18 (ACM), pp 102:1–31.

[10] PwC (2017) Smart home, seamless life. Available at https://www.pwc.fr/fr/assets/files/pdf/2017/01/pwc-consumer-intelligence-series-iot-connected-home.pdf.

[11] Norman DA, Draper SW (1986) *User centered system design: New perspectives on human-computer interaction* (CRC Press), 1st Ed.

[12] Haney JM, Furman SM, Acar Y (2020) Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. *Proceedings of the 22nd International Conference on Human-Computer Interaction* HCII '20, pp 1–19.

[13] Haney JM, Furman SM (2020) Work in progress: Towards usable updates for smart home devices. *Proceedings of the 10th Workshop on Socio-technical Aspects of Security* STAST '20, pp 1–15.

[14] Haney JM, Acar Y, Furman SM (2021) "It's the Company, the Government, You and I": User perceptions of responsibility for smart home privacy and security. *Proceedings of the 30th USENIX Security Symposium (to appear)* USENIX '21, pp 1–18.

[15] GfK (2016) Future of smart home study global report. Available at https://www.gfk.com/fileadmin/user_upload/dyna_content/GB/documents/Innovation_event/GfK_Future_of_Smart_Home__Global_.pdf.

[16] Fruchter N, Liccardi I (2018) Consumer attitudes towards privacy and security in home assistants. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* CHI '18 (ACM), pp 1–6.

[17] Stanton B, Theofanos MF, Prettyman SS, Furman S (2016) Security fatigue. *IT Professional* 18(5):26–32.