Kids, Cats, and Control: Designing Privacy and Security Dashboards for IoT Home Devices

Jacob Abbott*, Jayati Dev*, DongInn Kim*, Shakthidhar Reddy Gopavaram*, Meera Iyer*,
Shivani Sadam*, Shirang Mare†, Tatiana Ringenberg‡, Vafa Andalibi*, and L. Jean Camp*
* Indiana University
Bloomington, Indiana, USA
Emails: jaeabbot@indiana.edu, jdev@iu.edu, dikim@indiana.edu, sgopavar@iu.edu,
meeriyer@iu.edu, ssadam@iu.edu, vafandal@iu.edu, ljcamp@indaina.edu
†Western Washington University
Bellingham, Washington, USA
Email: shri.mare@wwu.edu
‡Purdue University
West Lafayette, Indiana, USA
Email: tringenb@purdue.edu

***Abstract*—In the last decade integration of Internet of Things (IoT) ecosystems has increased exponentially, and it is necessary that our understanding of human behavior when interacting with multiple smart devices in an IoT ecosystem keep pace. To better understand users' perceptions and use of in-home IoT ecosystem over time, we implemented an ecosystem in homes of participants so that we could both test previous findings about individual devices and identify differences that arise in the content of a home with multiple IoT devices. Specifically, we recruited eight participants from separate households who installed identical IoT configurations, and interviewed each participant for five weeks. We included an Android dashboard to provide device control and data transparency. We detail the semi-structured interviews to compare user perceptions of what devices are classified as IoT, the perceived sustainability of IoT devices, interactions with and desires of dashboard information, and exploration of current notification preferences and mitigation strategies. We discuss the factors which participants identified as being relevant to their personal experiences with IoT devices and contribute recommendations for dashboard designs and control mechanisms for IoT devices. We note that the participants uniformly had a more expansive definition of IoT than that found in much of the previous literature, implying that our understanding of perceptions of in-home IoT may be informed by previous research on security systems, wearables, watches, and phones. We identify where our results reify findings of studies of those devices.**

I. Introduction

The use of Internet of Things (IoT) devices research has addressed fields of application [22], motivators of adoptions [14], and barriers to entry for multiple populations [41], [11]. Recent literature on IoT devices has not only addressed how to better create technical interventions, but also incorporates usability and consideration of users' mental models into the device. For example, Zeng et al. explored the privacy concerns participants had around IoT devices [59], while Garg and Kim looked at if purchasing and adoption of IoT devices was impacted by security and privacy factors [23]. Other examples have tested devices with users in their home to gather feedback from the participants themselves on what they thought [29], [30]. In this study, we created a field deployment with a network of IoT devices, so we might see how participants manage multiple devices, and their own boundaries within an interconnected environment. Our design of the dashboard builds upon prior work [15], [60], and an evaluation of the use and acceptability of the IoT dashboard visualization is part of our experimental ecosystem. There are two specific questions we address in this experiment:

RQ1 What experiences did participants have with IoT devices and how do they define the IoT? We report on how users expressed their background with various IoT devices and were challenged with previous devices breaking and mitigation strategies for handling difficulties. We observed that participants were very inclusive and expansive in what they considered to be IoT devices including: smart watches, fitness trackers, streaming devices, thermostats, etc. Additionally, many expressed having no prior experience with IoT devices breaking, but high degrees of uncertainty of what to do with a broken device and a desire to not just throw it into a landfill.

RQ2 How did participants engage with the devices and the IoT ecosystem? We report on how users were challenged with practical constraints not just in terms of privacy, but also sometimes also due to the nature of their living situation, ability to manage their information, or existing device capabilities. We observed the reduced usage of two-factor authentication for network segregation. We identify how our results reify or differ from

Symposium on Usable Security and Privacy (USEC) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-91-6
https://dx.doi.org/10.14722/usec.2023.236290
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

previous privacy studies for each of our components when the devices are part of a larger ecosystem.

RQ3 How did users interact with information on the IoT dashboard and what were their preferences? We report on interviews over five weeks to show that users continued using the IoT dashboard as an access point to view all their devices in a convenient location with minor control mechanisms, though they did desire further customization and potential notifications for issues of errors within the IoT ecosystem. We observed reduced dashboard (which consolidates devices in use) usage over time.

To this effect, we recruited eight participants and provided instructions to install a smart home devices kit in their homes. In the following we report results from the installation phase and five weeks of interviews specific to our research questions. Our contributions include (1) First, we report on the user perceptions of what devices are classified as IoT. (2) Second, the perceived sustainability of IoT devices and the mitigation strategies of participants encountering non-functioning technology. (3) Third, we discuss the interactions with the IoT dashboard and collected design feedback. (4) Fourth, we expand on the current notification preferences of participants and mitigation strategies. (5) Finally, we make actionable recommendations on how researchers and designers working on IoT dashboards and control mechanisms can compliment each other in an ecosystem to provide improved utility to users.

II. Related Work

In the section below, we discuss key findings in recent regarding smart home device perceptions and trends in data presentation to situate the contribution of our work.

A. Perceptions of Smart Home Devices

The factors influencing what motivates adoption of IoT devices has been explored for the home environment [11], medical [40], [27], industrial [14], and infrastructural areas [17], [53]. Atzori et al. highlighted IoT's integration of multiple technologies and communication methods as a desirable benefit [7] which has been echoed in other works [14], [27]. Yet, while Carcary et al. found similar motivators towards adoption, research has also expressed multiple constraints to adoption of IoT such as concerns regarding scalability, privacy, and security [14], [41], [11].

Privacy and data security are recognized as potential hazards in the IoT [13], [55], [39]. Privacy concerns result in decreased use [37], lack of satisfaction [16], as well as decreases in trust [9] and comfort [58] when cameras are not visible in shared spaces. The balance between privacy and convenience for consideration as a motivating factor in deciding which devices to adopt was found to have a higher weight towards privacy by Alghamdi et al. [3].

A classification of mental models of sixteen participants about their perceptions of security and privacy resulted in two categories of users: advanced and service-oriented. Advanced users of IoT had more accurate perceptions of dataflows outside the home; while service-oriented users had a baseline assumption that only data used for services was compiled [1]. The lack of transparency of data flows and lack of accessible privacy policies have been identified as problematic since the earliest days of the web (e.g., [32]); solving these challenges has new urgency with in-home IoT as trust is an important factor in adoption [31], [4].

Addressing the lack of information at time of purchase, as opposed to use, individuals may choose to adopt a device based on the perceived benefit and value gained by its use [35]. Perceptions and attitudes of IoT devices varied across the types of devices and forms, whether as a wearable band or an environmental object [47], and the factors that play into deciding upon acquiring a device include technological, organizational, and environmental factors [46]. The control of IoT devices also strongly plays a role into their perception [44] and tensions can arise when desires to collect contrast with desires not to share data [43].

B. Presenting IoT Data

Balancing the agency between the IoT devices and the people controlling them depends heavily upon what information is presented from the sensors of IoT devices and the data they collect [33]. Previous work has looked into methods of evaluating User Interfaces (UI) in IoT [48] and the challenges in visualizing IoT data in a meaningful way to users with different experience levels [25], [50]. Explorations into how users previously expressed interest in dashboard information from IoT devices, Ammari et al. found that participants wanted to see all connected devices [5]. Additional work found that participants expressed a desire to have a central point for accessing their smart devices in their homes [29], but that preferences for alerts and updates of information vary and are context dependent [30], [19], [38]. The device used to access the IoT data changes how people interact with it and suggests for adaptive scenarios and UI as methods for optimizing the experience [51], [8].

Along with having mechanisms to control devices in homes, there has been previous work investigating methods for notifying users about events that may be detected by sensors throughout an IoT ecosystem. Kubitza et al. created a hub device that allowed users to select whether notifications for specific applications on their phone would be forwarded via notification or text to other devices on the network connected to the hub they were currently using, such as a tablet or smart TV [36]. A preference for notifications to be sent to smartphones has been noted in multiple contexts such as with two-factor authentication [2], activity nudges [56], and those who own multiple types of devices [57].

III. Study Design

A. Description of System and Dashboard

Due to COVID-19, the researchers were unable to visit participants' homes in person and complete the installation. Thus, we created detailed setup notes and a router configuration file for participants to be able to easily setup the different smart

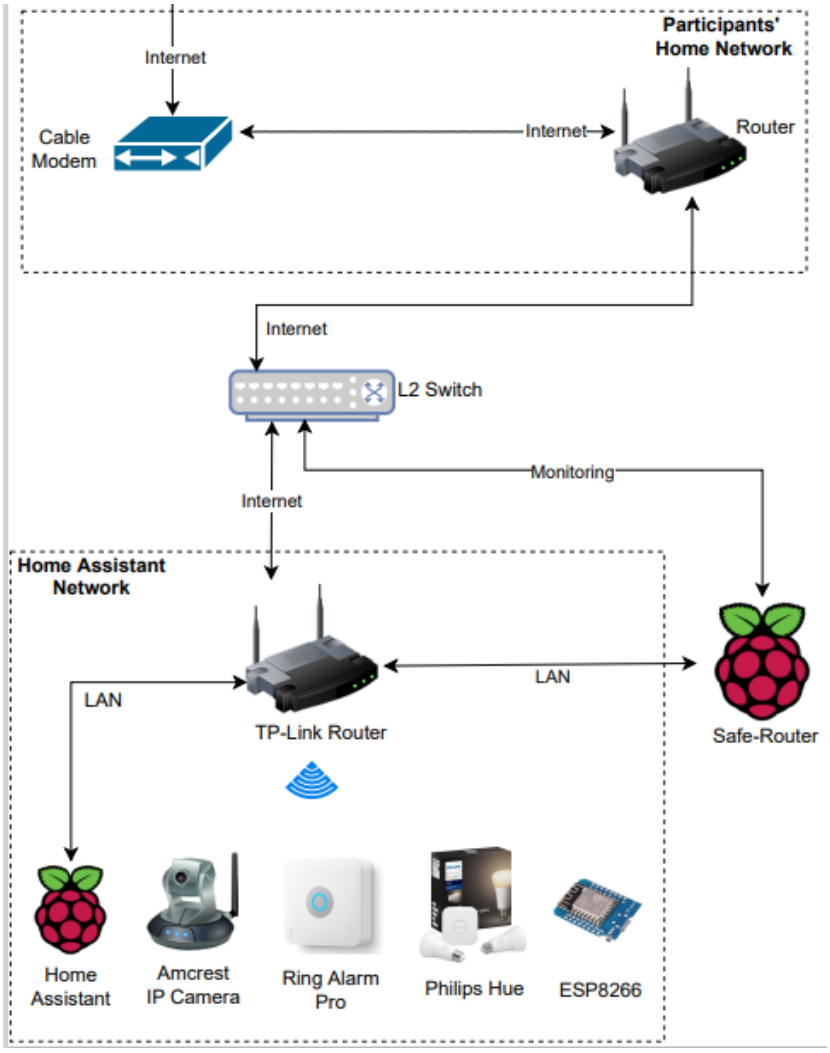

Fig. 1: Diagram of IoT Devices and Home Network.

home devices. This setup and instructions were tested by one of the researchers and another person external to the study. Our system is designed to replicate the home automation system so that we can proceed with the experiments of home IoT securities for each participant. It consisted of the following devices and they were connected as shown in Figure 1. These are a) One TP-Link Router; b) Two Raspberry Pis - Home Assistant and Safe Router; c) One extensible Philips Hue lighting system consisting of the controller and two smart bulbs; d) One Amcrest IP Camera; e) Components of a Ring Alarm system consisting of an Alarm Base, Key Pad, Z-Wave extender, Z-wave motion sensor, and 4 Z-wave contact sensors; f) Two ESP8266 boards with motion, humidity, and temperature sensors; g) One TP-Link network switch (L2); h) a single Yubikey; and i) a USB-3 to RJ45 adapter. Necessary cables for installation and a power strip were also provided.

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

Two Raspberry Pis were used, one to support the Home Assistant and one as a Safe Router system. The Safe Router implemented the functionality of the Home Assistant by enabling participants to disable devices (or the entire system) after installation. The decision to use the Safe Router in addition to the Home Assistant delayed the experiment and made installation more difficult. We were able to ensure that participants' could disable devices or block dataflows through our implementation of the Safe Router rather than using a Wizard of Oz approach, which is a common method for evaluating participants' preferences in interactions by showing people something that appears to function as intended but is inherently not [20], [21]. The widespread sharing of data, including when an app is uninstalled, required a local intervention to ensure the devices did not access the Internet after participants disabled

them.

Participants were also provided with an Android tablet which was able to connect to the provided router's wireless network. The tablet was configured to interact with the Home Assistant software[28] and provide an overview of the different systems as a dashboard for participants. Participants had to login to the tablet and enter a specific URL to see the dashboard visualization. The initial settings for each participants' dashboard were standardized by the research team to appear the same with status information from all included devices to appear on screen. An example mock-up of a participant's dashboard is shown in Figure 2, as a screenshot of a participant's dashboard would reveal significant personal information. The dashboard's goal to have information from all devices accessible on one screen without navigating to other applications or screens, though some adjustments or changes to settings could only be done by changing screens.

B. Recruitment and Participants

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

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

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

C. Interview Protocol

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

To pilot our interview study we recruited four older adult participants from a large-scale IoT-in-the-home study who were already living in a setting similar to ours. Our initial interview pool was participants in the HomeSHARE project [52]. HomeSHARE is a test-bed of adult homeowners who have agreed to engage with researchers for the evaluation of in-home technologies. Any researcher or research group working on a smart home project is able to contact HomeSHARE researchers and request to conduct a study with the participants as long as there is IRB approval. As it was founded in 2015, this is a population that is particularly aware of issues that may emerge when using in-home technologies, and comfortable with interactions with researchers.

We interviewed them during the week of November 17-20, 2020 and asked questions for our pilot interview. Specifically, we sought individuals who were planning to purchase IoT devices or had some experience in IoT devices in order not to create a risk of data exposure. This is a potential limitation of this study, as early adopters may be more positive about technology [42]. Given current market penetration we chose this as a reasonable basis for exclusion with a recognition of the potential limiting effect.

Based on pilot interview responses, we modified the interview protocol slightly by adjusting the structure of weekly interviews to be semi-structured and all questions were open ended, excluding those directly pertaining to the Trust, Benefit, Satisfaction, Burden questions which were requested as true/false responses [18].

In the five weeks immediately following installation, participants were interviewed for approximately 30 minutes each week. The first week of interviews focused on the process of setting up the IoT devices and system along with the Trust, Benefit, Satisfaction, Burden questions [18]. Weeks 2 through 4 introduced additional design prompts with the weekly check-in questions and finally week 5 had an exit interview which closed with the Trust, Benefit, Satisfaction, Burden questions and general reflections of participants on their experiences.

D. Data Analysis

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

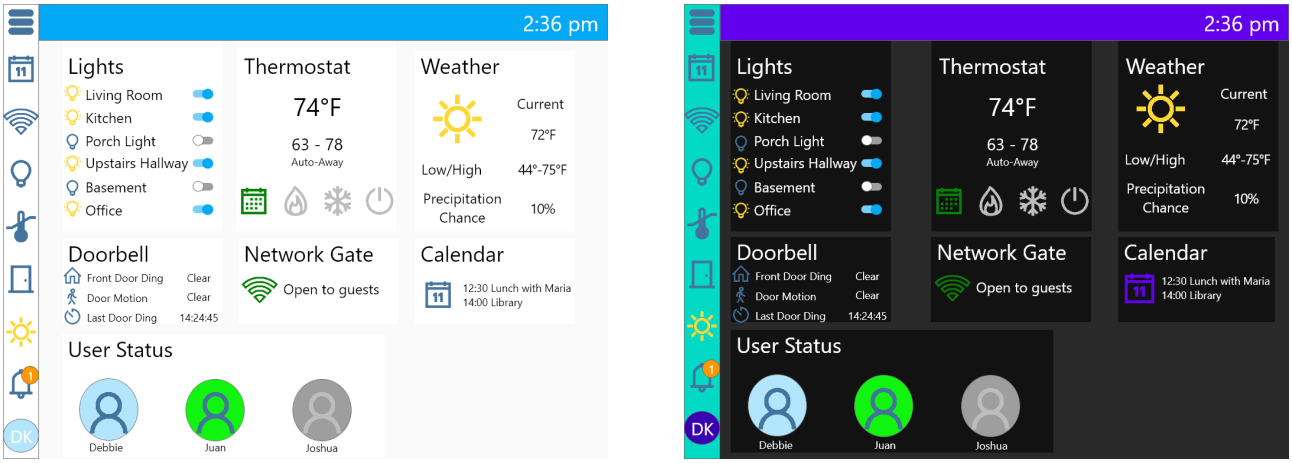

Fig. 2: Mock-up example of participant's dashboard viewed on tablet screen with light theme (left) and dark theme (right).

from the first two weeks to identify emergent themes and their related topics. From those themes, we developed an initial draft codebook and the four coders applied the codebook to an additional 8 interviews from weeks 1 through 5. New and emergent themes were added as appropriate before all 40 interviews from the five weeks were re-coded with the updated codebook. The four coders each individually coded 20 interviews so there was overlap with one other coder. Any conflicts in codes were brought to group consensus of all four coders.

IV. Findings

In this section we report our findings of the five-week study on deploying the IoT ecosystem in eight homes. These findings are discussed in greater detail below.

A. Participants

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

B. What is IoT and Who Uses it?

When asked about what IoT devices they previously had experience interacting with, two of our participants had smart lights previously, one had experience with security monitoring systems, and six of our participants mentioned having interacted with a digital voice assistant such as Google Assistant or Amazon's Alexa. Table II shows the breakdown of devices already owned by participants as self reported in the preliminary survey responses. For five of our participants the bundle of IoT devices they received was their first time setting up a system of IoT devices in their own homes.

When exploring their own familiarity with common IoT devices and whether any of their family or friends own any IoT devices in their homes, all of our participants (n=8) reported someone within their social circle owning a smart device or multiple devices.

> "My family has a lot of the ring cameras. And like the ring, I guess ecosystem and Alexa or like the echoes because those are a big one. So there's that - smart TVs are also big thing we like. We're all big into like streaming shows and stuff." (P3, 29, Man)

> "I have friends that have the Ring system. I'm trying to think, what else? You know some people have thermostats, but I don't know which brand, and I know people that have, a lot of people that have Amazon devices like Fire Stick or the Echo products, Alexa and that sort of thing... I like the fitness bands. Definitely, you can receive texts you can see you're texts on that. You can see if you have an incoming call, and some of them you can even answer your call. So I would say yeah, in that sense, I don't know anybody who has their phone calls hooked up to Echo. I don't even know if you can do that. I imagine you might be able to embed yeah, so mostly in that fitness bands arena, like an Apple Watch, that sort of thing." (P5, 47, Woman)

The only type of device that was mentioned by all participants (n=8) as being used by them or people in their social circles was a digital assistant device, such as a Google Home or Amazon Echo Dot. We specifically distinguished the use of digital assistants in interviews as distinct from their use with phones, such as Google Assistant on Android or Siri on iPhones, for the specific purpose of disambiguation with participants, as all participants (n=8) also reported using digital assistants through their smart phones.

While smart thermostats, cameras, and security systems were frequently mentioned and may often come to mind as

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

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

TABLE II: Types of devices participants reported already owning before participation in the in-home study.

Participant	P1	P2	P3	P4	P5	P6	P7	P8
Voice Assistant	X		X	X	X		X	
Smart TV	X		X	X	X	X	X	X
Door/Window Sensor				X				
Motion Sensor				X	X			
Smart Security System				X				
Smart Camera	X		X	X				
Smart Lights			X	X				
Smart Thermostat			X	X	X			
Smart Power Outlet			X	X	X			

IoT devices, the majority of participants (n=6) also identified additional devices which are not always considered as IoT. For example, P5 mentioned smart watches and fitness trackers which might frequently be thought of by the term wearables rather than the category of IoT devices.

When asked about who had access to their IoT devices and network, half of participants (n=4) responded that they were the only person to have access as they lived alone. While this study was conducted during a time period of suggested limited social gatherings due to COVID-19, a few participants (n=3) did express the introduction of the IoT devices to roommates or family members. One such example was P8 who introduced her roommate to the system and shared access.

> "I just told [my roommate] about the the Philip lights for the kitchen. I leave the tablet like in the main room. But other than the lights, [she did] not really seem interested in checking out the security footage or anything like that. So yeah, I mean, she has the option to use it...It was just mostly like, here's all of the stuff here. Here's the code for the tablet. So you can turn the lights on and off. Here's what each of the things are and well, since I have them all in one corner, I just point to the corner and say things are there." (P8, 22, Woman)

The participant being the lead in controlling the devices and interacting the most in shared households was a common trend echoed in all homes with multiple individuals. Even when access was shared and provided, it did not lead to engagement for most shared households as reported by the interviewed participants.

> "Just showing but no one interacted with it. So I'm just living with my wife and my daughters. So I will just show my wife about the streaming camera. And we're showing that this camera, we have the camera here and we can see what our daughter is doing right now in the living room and that's it. But she was not interacting or doing anything at all with the home assistant to this day." (P6, 36, Man)

Following the trend of participants controlling access to their devices and home networks, we questioned if they had previous experience of setting up equipment for others. While most (n=7) of our participants mentioned past experiences of helping others such as parents or grandparents with various technology not specific to IoT, we found a particularly strong example of someone acting as a 'family technologist' with P2.

> "So I usually set, I pretty much know all their username and passwords, which is kind of amazing because I've got to, I have to remember grandparents and both of my parents that I have to remember usually, they'll usually text me and ask me 'What's my password for this?' And I had to send it. But as far as the privacy settings and everything, well, when I was living at home, I set it all up and set it up so I can access it as well. And then as soon as I moved out, I disabled that. So then I can't see anything on the ring cameras or anything like that. That's usually the way I set up. I set up their accounts and their usernames and everything like that. And then if I need to, I can get into it like remotely, which is kind of nice. But like if my grandma has the problem with her legs, I'm from [location redacted], so that's four hours north. So I'm not going to drive four hours north to deal with it. I can most of the time do it remotely. So that's kind of nice." (P2, 22, Man)

P2's experience with family is similar to findings from Gerber and Marky [24] where people who were more adept

with security and privacy aspects of technology were not only found to often serve as technologists for their social circles, but also as tech support and educators. The ease of access to troubleshoot offered by remote access is a trade off when compared to being able to talk someone through the steps of a process and transfer knowledge. P2 was the only participant who mentioned having ever setup remote access, while other participants had assisted with other technology issues for knowledge transfer face to face or over the phone.

Allowing remote access is often designed in to many IoT devices as it allows users to check the status of their devices from a distance, typically through a dedicated application for a specific device. Using the dashboard frameworks (see Fig. 2) we asked participants about the perceived benefits of a status indicator for users connected to their network. All participants were presented with three icons in varied colors with names beneath: blue icon Debbie - representing the current user of the dashboard, green icon Juan - representing another user connected to the network and online, and gray icon Joshua representing a user who is offline and disconnected from the network. All participants identified the grayed out user as being offline, yet there was some confusion regarding distinction between the blue and green coloring for user status. All participants thought the green indication meant the user was online in some manner, but a few (n=3) were uncertain if the blue user indicated if they were in control or just connected. The majority of participants (n=7) expressed an idea that it could be useful to see if someone else was connected to/using their network, but as they were not having anyone over they did not see a need.

C. Sustainability of IoT and Mitigation Strategies for Difficulties

While we were interested in how the various IoT devices functioned during the time of the study, we were also curious of any issues participants had experienced previously with devices breaking, whether from a software or hardware issue, in the past. Only two participants (P4, P5) specifically mentioned previous experience with IoT devices becoming unusable.

> "I have a phone connecting box where you can connect a telephone to Google Voice and it gets you, basically you get a home phone line for free. I've had one of those for a really long time and the hardware actually still works but Google made a change to that. So like their version one box quit working, not because it couldn't work, because they needed a software update they didn't want to do... I hate that have to buy a new one because the software is out...Other things like I have a bunch of old computer hardware that like I've got the scanners and printers and they just don't like, some of the scanners are old enough and printers, they were 16 bit drivers and they never made it 32-bit driver. And so they're just gone. You know the hardware? It totally works, but like you need to hook up an old enough computer, and you could use it, but because of software support, it's gone. And I just saw speaking of IoT devices, Samsung smart things are things that they call theirs? They're dropping support for the version one hub. And so everyone who has a Samsung version one hub is just out because these are all cloud-based. If you don't have the Cloud, you don't have - you basically have this piece of junk." (P4, 59, Man)

An issue discussed by some participants (n=3) that echoed the situation of P4 was the concern of devices no longer being supported by a company or a company no longer existing to support the device.

> "So it just kind of sitting there collecting dust...I already told you I'm moving, I am packing things away and I just found my old tablet still in the box. 'Oh, hello. You're brand new.' If it's still brand new, I mean, that would probably make it easier to like resell to somebody like it's not even been opened. Like it's an old tablet now. So I don't even know that specific brand of tablet is still supported...That seems to be one of the issues is, what do you do with the old devices when things are no longer supported?" (P7, 26, Woman)

Though not every participant experienced concerns with devices becoming obsolete or breaking as P1's response to the question of any previous experience with devices breaking:

> "I don't really think so. I guess my sister did step on my laptop once in, like the screen broke. And then I had to get a new one. But I don't I don't really think that I've ever capture device so long that it kind of like went out on me" (P1, 22, Woman)

Given most participants lacked direct experience of troubleshooting or dealing with broken IoT devices we did probe and ask them if they ever ran into problems with their devices, who they usually would ask help from and what they might do to try to fix anything.

> "So since I'm living in an on-campus apartment, I would I will contact the [IT department] from the campus for any technology trouble. That there will be my first, my first for a technology problem. And then maybe as a friend, there's one of my friend here who live in my apartment which is working out at IT area. And he also was helping installing a couple of things when I was moving here in my first year of my study. Yeah. So I think those two will be your sources in asking for help for those questions." (P6, 36, Man)

The majority of participants (n=7) said they would ask a friend or family member for help troubleshooting a device or dealing with a technological problem. Only P6 mentioned contacting a formal party such as the IT department of their university. Just over half (n=5) of the participants discussed that they would search online for answers before asking for help.

> "P1: Yeah. I would say sometimes I have to ask my fiance some questions. Like the settings on my computer running slow. And he's really the most tech savvy. I think I usually just ask for help, but it might help me out more to do a quick Google search on Help feature on my computer and find that." (P1, 22, Woman)

There was a slight preference of participants towards searching out written steps and articles over videos when troubleshooting (n=5), but not a single participant mentioned contacting a customer help or device manufacturer in their interviews when mentioning their ideas of potential strategies for troubleshooting broken or unsupported devices.

D. Dashboard Interactions and Feedback

When asked "And how often would you say that you look at the dashboard display to review the status of your home?" P1 (22, Woman) responded "Probably every few days, if not daily." This regularity was echoed by the majority of participants throughout the study, with a noted exception of P2 whose apartment flooded during week 4 of the study.

> "So I was checking it pretty regularly and then it quit working when my apartment flooded. So the whole situation? Yeah. When the dashboard was working, I was checking especially humidity because my thermostat was ancient and you can't tell if it was 65 or 95 degrees." (P2, 22, Man)

However, the number of times participants checked the dashboard or interacted with the different devices did not translate to adjustments of device settings. Almost all participants reported that they simply reviewed statuses or had simple interactions, such as dimming lights or arming the security alarm.

> "So I view them, I wouldn't feel super often, but maybe a couple times a week now. Maybe one time a day, twice at most. I don't really switch off anything as I feel like I know what's going on there." (P7, 26, Woman)

When asked about their preferences for the dashboard interface, all participants expressed a preference for viewing the dashboard on the tablet in a landscape view rather than portrait. A few cited that it was more familiar to how it would look when viewed through a browser on a laptop. Additionally all participants expressed positive feedback towards the dashboard allowing an overview and some control for all devices in one location.

> "I think it's pretty effective just because with them all being right there in one place, it makes it more accessible to them." (P1, 22, Woman)

> "I just like seeing everything in the same place." (P8, 22, Woman)

However, not all feedback was positive as P7 (26, Woman) noted "The Home Assistant only allows me to do a slider for the lights, but it doesn't let me do another cool setting that the Philips Hue app lets me do." as the specific app for a device allowed more customization and control options than the limited options available through the dashboard.

E. Notification Preferences

We asked participants if they were subscribed to any services for receiving notifications for local updates or notifications, and if so what method they preferred to receive communications. The majority of participants (n=7) received emergency notifications from their local university regarding weather and safety announcements.

> "Probably text messages and emails. If it's really severe, maybe a phone call or different app notification, kind of what happens when there's like a normal emergency that they put out those alerts, I don't know what those are called. You probably know what I'm talking about. The ones that are like, buzz on everybody's phone and everything. They're location-based, but those would be kind of nice, especially in a real emergency situation." (P2, 22, Man)

> "I'd prefer to have it all in e-mail instead of having some an e-mail or SMS text. Because I don't know, I feel like to me text is like I think we talked for the next level of urgency. And mostly things to me, aren't urgent." (P4, 59, Man)

Only one participant expressed a strong preference for a specific single method of notification as email (P4), all other participants mentioned leaning to multiple types of notification methods with variations based on location or the severity of the situation or message.

> "I would honestly prefer either e-mail or some sort of notification coming through an app, simply because if it's an email, I can kind of group it together and create a folder for all of this sort of notifications and have things automatically filter into there. And that having present on an app would also help, especially as you have some sort of dashboard that you look at for all of your information." (P7, 26, Woman)

For the remaining seven participants their responses were a mix of: SMS messages (n=6), emails (n=5), push notifications (n=4), and phone calls (n=2) as their desired methods of notification for potential issues with their IoT devices and network.

V. Discussion & Implications

During the interviews participants described their own perspectives and experiences with technologies they considered to be included within the Internet of Things. Our analysis provided feedback from a deployment study of a smart home ecosystem and a dashboard user interface to manage the presentation of information and basic functionality of multiple devices in a single location. In this section we elaborate on the reported interactions and motivations of participants to build upon recommendations of previous studies and the

implications our findings hold for designing new dashboards and control mechanisms for IoT devices.

A. IoT is Broadly Inclusive of Device Types

Page et al. and Poongodi et al. argued for a broader inclusion of wearable devices such as health and fitness trackers in consideration as IoT devices [47], [49]. We add to their recommendation and suggest broadening our idea of what types of devices we as designers and researchers consider to be IoT devices. Different participants have different opinions and attitudes of what makes a device an Internet of Things device, as they have shown in our interviews, specific to not only their personal usage scenarios but those of their social circles to which they have been exposed. This could support the use of a Contextual Inquiry framework, as developed by Apthopre et al. [6], to investigate what devices are considered more aware and when as the context does seem to matter.

B. Sustainability of IoT and Strategies for Encountering Issues

While participants described the potential benefits of using different smart home devices and those they desired to use in the future, very few had prior experience encountering issues with an IoT device breaking previously. Modarress et al. referenced the threats of IoT devices on environmental sustainability by electronic waste (e-waste) [45]. The majority of participants had experienced other failings with technologies suffering software or hardware failures that required them to have the device repaired or replaced, yet a number maintained the broken or non-functioning devices as they expressed no method for safely disposing of the product other than throwing in the trash. Accordingly, smart device manufacturers and designers should continue to work together to promote more sustainable design and promote education of methods and programs for reducing e-waste [12], [10].

C. Dashboards - One Window with Many Views

Participants expressed positive interactions with the Android dashboard that allowed them to see the status of all the IoT devices in their ecosystem, echoing findings from Jakobi et al. [29]. However the ability to control various devices through one location improved utility and increased engagement, yet still left participants wanting more. As discussed in Section 4.5 with notification preferences, there could be potential for the dashboard to be used as a method of notification of any issues with the IoT system, echoing Jakobi et al. who found participants engaged more with the dashboard over the long term only when something went wrong [30]. In the use case we studied it was specifically in the context of within the home environment, but other contexts may have differing levels of engagement, such as dashboards used inside a vehicle [26] or those monitored inside a manufacturing facility [54]. The use of co-design methodology in developing and evaluating dashboards for IoT systems [34], [48] could benefit from incorporating the insights of users with different backgrounds and adapt the presentation of visualized IoT data in a meaningful way based on context to specific use cases [25].

VI. Limitations and Future Work

While the initial study was designed prior to COVID-19, we were required to change certain elements of the study design due to the restrictions on human subject studies for health concerns and conducted all portions of the study remotely. Given the small number of participants and all residing in the same state, their is a limit to the generalizability of our findings. The majority of our participants not being college students may reflect different perceptions compared to if users had been college students or lived in dormitories. Our participants installed the IoT ecosystem on their own with remote check-in post installation, therefore all data is self-reported and was not observed in real time with a think aloud as initially planned. Furthermore, we report on installation and use for five weeks of an in-home IoT systems study, while an extended study with high level of habituation may have yielded different results.

In future work, observing participants installing devices in their homes with a think aloud scenario could provide additional insights into any frustrations or difficulties. Additionally, testing scenarios for sending notifications to participants of different errors or events and exploring whether their perceived preferences would match implemented usability is an open question for future research.

VII. Conclusion

Our three research questions were: 1) what experiences did participants have with IoT devices and how do they define the IoT, 2) how did participants engage with the devices and the IoT ecosystem, and 3) how did users interact with information on the IoT dashboard and what were their preferences? After the five weeks of our study, we found that participants had an inclusive mindset of what devices could be classified as IoT, beyond just smart lights and thermostats to also include things like fitness trackers, streaming devices, smart TVs, and smart watches to name just a few. We also found that participants usually used the dashboard to view the status of their ecosystem regularly and controlled devices through it unless more fine grained control was required. We found that in addition to many of the findings from previous research being echoed, some were unexpected. One such unexpected occurrence was the flooding of P2's apartment and the subsequent damage to some of the equipment, brought a discussion of how a notification of high humidity detection might have warned him of flooding, or of waterproofing the IoT devices. While these were outside the scope of the project, it did contribute to the larger discussion of IoT being a potential threat to e-waste when there is not information or practices in place to empower people to handle the end of their IoT devices' life cycles.

In the future, we would like to extend this study and explore sending notifications through the dashboard and other modes of communication to identify if expressed preferences match as intended. Since IoT home devices are increasingly operating as components withing smart homes, this study contributes to an understanding of what people consider being within the realm of IoT and by investigating their concerns we can build

a better platform to deliver meaningful information to users identified in previous user studies of IoT devices.

ACKNOWLEDGMENT

Thanks to all of our participants for their efforts and feedback in our study. This research was supported in part by the National Science Foundation awards CNS 1565375 and under grant # 2127309 to the Computing Research Association for the CIFellows Project. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the US Government, the National Science Foundation, the National Security Agency, Indiana University, Purdue University, nor Western Washington University. We acknowledge support from the US Department of Defense [Contract No. W52P1J2093009].

REFERENCES

[1] "'I Don't Own the Data': End user perceptions of smart home device data practices and risks."

[2] J. Abbott and S. Patil, "How mandatory second factor affects the authentication user experience," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: ACM, 2020, p. 1–13. [Online]. Available: https://doi.org/10.1145/3313831.3376457

[3] L. Alghamdi, A. Alsoubai, M. Akter, F. Alghamdi, and P. Wisniewski, "A user study to evaluate a web-based prototype for smart home Internet of Things device management," in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed. Cham: Springer International Publishing, 2022, pp. 383–405.

[4] A. AlHogail, "Improving IoT technology adoption through improving consumer trust," *Technologies*, vol. 6, no. 3, 2018. [Online]. Available: https://www.mdpi.com/2227-7080/6/3/64

[5] T. Ammari, J. Kaye, J. Y. Tsai, and F. Bentley, "Music, search, and IoT: How people (really) use voice assistants," *ACM Trans. Comput.-Hum. Interact.*, vol. 26, no. 3, apr 2019. [Online]. Available: https://doi.org/10.1145/3311956

[6] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster, "Discovering smart home Internet of Things privacy norms using contextual integrity," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 2, July 2018. [Online]. Available: https://doi.org/10.1145/3214262

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128610001568

[8] P. Bahirat, Y. He, A. Menon, and B. Knijnenburg, "A data-driven approach to developing IoT privacy-setting interfaces," in *23rd International Conference on Intelligent User Interfaces*, ser. IUI '18. New York, NY, USA: ACM, 2018, p. 165–176. [Online]. Available: https://doi.org/10.1145/3172944.3172982

[9] J. Bernd, R. Abu-Salma, and A. Frik, "Bystanders' privacy: The perspectives of nannies on smart home surveillance," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[10] D. Bol, J. De Vos, F. Botman, G. de Streel, S. Bernard, D. Flandre, and J.-D. Legat, "Green SoCs for a sustainable Internet-of-Things," in *2013 IEEE Faible Tension Faible Consommation*, 2013, pp. 1–4.

[11] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: Challenges and opportunities," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, p. 2115–2124. [Online]. Available: https://doi.org/10.1145/1978942.1979249

[12] C. Cairns, "E-waste and the consumer: Improving options to reduce, reuse and recycle," in *Proceedings of the 2005 IEEE International Symposium on Electronics and the Environment, 2005.*, 2005, pp. 237–242.

[13] J. Camp, R. Henry, T. Kohno, S. Mare, S. Myers, S. Patel, and J. Streiff, "Toward a secure Internet of Things: directions for research," *IEEE security & privacy*, vol. 18, no. 4, pp. 28–37, 2020.

[14] M. Carcary, G. Maccani, E. Doherty, and G. Conway, "Exploring the determinants of IoT adoption: Findings from a systematic literature review," in *International Conference on Business Informatics Research*. Springer, 2018, pp. 113–125.

[15] N. Castelli, C. Ogonowski, T. Jakobi, M. Stein, G. Stevens, and V. Wulf, "What happened in my home? an end-user development approach for smart home data visualization," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, p. 853–866. [Online]. Available: https://doi.org/10.1145/3025453.3025485

[16] P. R. Center, "Implications of the Internet of Things connectivity binge," Aug 2020, [Online; Accessed 9. Feb. 2022]. [Online]. Available: https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications

[17] S. Constantinou, A. Konstantinidis, P. K. Chrysanthis, and D. Zeinalipour-Yazti, "Green planning of IoT home automation workflows in smart buildings," *ACM Trans. Internet Things*, vol. 3, no. 4, sep 2022. [Online]. Available: https://doi.org/10.1145/3549549

[18] G. Corbie-Smith, A. S. Ammerman, M. L. Katz, D. M. M. St. George, C. Blumenthal, C. Washington, B. Weathers, T. C. Keyserling, and B. Switzer, "Trust, benefit, satisfaction, and burden: A randomized controlled trial to reduce cancer risk through african-american churches," *Journal of General Internal Medicine*, vol. 18, no. 7, pp. 531–541, 2003.

[19] F. Corno, L. De Russis, and T. Montanaro, "A context and user aware smart notification system," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 645–651.

[20] N. Dahlbäck, A. Jönsson, and L. Ahrenberg, "Wizard of Oz Studies — Why and How," *Knowledge-based Systems*, vol. 6, no. 4, pp. 258–266, 1993.

[21] S. Dow, B. MacIntyre, J. Lee, C. Oezbek, J. D. Bolter, and M. Gandy, "Wizard of Oz support throughout an iterative design process," *IEEE Pervasive Computing*, vol. 4, no. 4, pp. 18–26, 2005.

[22] P. Dudhe, N. Kadam, R. M. Hushangabade, and M. S. Deshmukh, "Internet of Things (IoT): An overview and its applications," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 2650–2653.

[23] R. Garg and J. Kim, "An exploratory study for understanding reasons of (not-)using Internet of Things," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '18. New York, NY, USA: ACM, 2018, p. 1–6. [Online]. Available: https://doi.org/10.1145/3170427.3188466

[24] N. Gerber and K. Marky, "The nerd factor: The potential of *s&p* adepts to serve as a social resource in the user's quest for more secure and privacy-preserving behavior," in *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022, pp. 57–76.

[25] A. Gibson and R. Martinez-Maldonado, "That dashboard looks nice, but what does it mean? towards making meaning explicit in learning analytics design," in *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, ser. OZCHI '17. New York, NY, USA: ACM, 2017, p. 528–532. [Online]. Available: https://doi.org/10.1145/3152771.3156171

[26] S. Hind, "Dashboard design and the 'datafied'driving experience," *Big Data & Society*, vol. 8, no. 2, p. 20539517211049862, 2021.

[27] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare," in *2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, 2014, pp. 304–307.

[28] Home Assistant, Feb 2023. [Online]. Available: https://www.home-assistant.io/

[29] T. Jakobi, C. Ogonowski, N. Castelli, G. Stevens, and V. Wulf, "The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017, p. 1620–1633. [Online]. Available: https://doi.org/10.1145/3025453.3025799

[30] T. Jakobi, G. Stevens, N. Castelli, C. Ogonowski, F. Schaub, N. Vindice, D. Randall, P. Tolmie, and V. Wulf, "Evolving needs in IoT control and accountability: A longitudinal study on smart home intelligibility," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 4, dec 2018. [Online]. Available: https://doi.org/10.1145/3287049

[31] P. Jayashankar, S. Nilakanta, W. J. Johnston, P. Gill, and R. Burres,

"IoT adoption in agriculture: the role of trust, perceived value and risk," *Journal of Business & Industrial Marketing*, 2018.

[32] C. Jensen and C. Potts, "Privacy policies as decision-making tools: an evaluation of online privacy notices," in *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 2004, pp. 471–478.

[33] H. Jia, M. Wu, E. Jung, A. Shapiro, and S. S. Sundar, "Balancing human agency and object agency: An end-user interview study of the Internet of Things," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ser. UbiComp '12. New York, NY, USA: ACM, 2012, p. 1185–1188. [Online]. Available: https://doi.org/10.1145/2370216.2370470

[34] J.-E. Kim, M. Bessho, N. Koshizuka, and K. Sakamura, "Enhancing public transit accessibility for the visually impaired using IoT and open data infrastructures," in *Proceedings of the First International Conference on IoT in Urban Space*, ser. URB-IOT '14. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014, p. 80–86. [Online]. Available: https://doi.org/10.4108/icst.urb-iot.2014.257263

[35] Y. Kim, Y. Park, and J. Choi, "A study on the adoption of IoT smart home service: using value-based adoption model," *Total Quality Management & Business Excellence*, vol. 28, no. 9-10, pp. 1149–1165, 2017. [Online]. Available: https://doi.org/10.1080/14783363.2017.1310708

[36] T. Kubitza, A. Voit, D. Weber, and A. Schmidt, "An IoT infrastructure for ubiquitous notifications in intelligent living environments," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, ser. UbiComp '16. New York, NY, USA: ACM, 2016, p. 1536–1541. [Online]. Available: https://doi-org.proxyiub.uits.iu.edu/10.1145/2968219.2968545

[37] A. Lazar, C. Koehler, T. J. Tanenbaum, and D. H. Nguyen, "Why we use and abandon smart devices," in *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2015, pp. 635–646.

[38] H. Lee and A. Kobsa, "Privacy preference modeling and prediction in a simulated campuswide IoT environment," in *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2017, pp. 276–285.

[39] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[40] L. Linkous, N. Zohrabi, and S. Abdelwahed, "Health monitoring in smart homes utilizing Internet of Things," in *2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 2019, pp. 29–34.

[41] S. Luthra, D. Garg, S. K. Mangla, and Y. P. Singh Berwal, "Analyzing challenges to Internet of Things (IoT) adoption and diffusion: An Indian context," *Procedia Computer Science*, vol. 125, pp. 733–739, 2018, the 6th International Conference on Smart Computing and Communications. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917328624

[42] A. N. Makam, H. J. Lanham, K. Batchelor, B. Moran, T. Howell-Stampley, L. Kirk, M. Cherukuri, L. Samal, N. Santini, L. K. Leykum *et al.*, "The good, the bad and the early adopters: Providers' attitudes about a common, commercial EHR," *Journal of Evaluation in Clinical Practice*, vol. 20, no. 1, pp. 36–42, 2014.

[43] S. Mare, F. Roesner, and T. Kohno, "Smart devices in Airbnbs: Considering privacy and security for both guests and hosts," *Proc. Priv. Enhancing Technology*, vol. 2020, no. 2, pp. 436–458, 2020.

[44] K. Marky, S. Prange, M. Mühlhäuser, and F. Alt, "Roles matter! understanding differences in the privacy mental models of smart home visitors and residents," in *20th International Conference on Mobile and Ubiquitous Multimedia*, ser. MUM 2021. New York, NY, USA: ACM, 2022, p. 108–122. [Online]. Available: https://doi-org.proxyiub.uits.iu.edu/10.1145/3490632.3490664

[45] B. Modarress Fathi, A. Ansari, and A. Ansari, "Threats of Internet-of-Things on environmental sustainability by E-Waste," *Sustainability*, vol. 14, no. 16, 2022. [Online]. Available: https://www.mdpi.com/2071-1050/14/16/10161

[46] O. B. Olushola, "Factors affecting IoT adoption," *IOSR Journal of Computer Engineering (IOSR-JCE) Volume*, vol. 21, pp. 19–24, 2019.

[47] X. Page, P. Bahirat, M. I. Safi, B. P. Knijnenburg, and P. Wisniewski, "The Internet of what? understanding differences in perceptions and adoption for the Internet of Things," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 4, dec 2018. [Online]. Available: https://doi.org/10.1145/3287061

[48] O. Pastushenko, J. Hynek, and T. Hruška, "Evaluation of user interface design metrics by generating realistic-looking dashboard samples," *Expert Systems*, vol. 38, no. 5, p. e12434, 2021, e12434 10.1111/exsy.12434. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/exsy.12434

[49] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, "Wearable devices and IoT," in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Springer, 2020, pp. 245–273.

[50] A. Protopsaltis, P. Sarigiannidis, D. Margounakis, and A. Lytos, "Data visualization in Internet of Things: Tools, methodologies, and challenges," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: ACM, 2020. [Online]. Available: https://doi.org/10.1145/3407023.3409228

[51] N. Rathnayake, D. Meedeniya, I. Perera, and A. Welivita, "A framework for adaptive user interface generation based on user behavioural patterns," in *2019 Moratuwa Engineering Research Conference (MERCon)*, 2019, pp. 698–703.

[52] B. Reeder, H. Molchan, E. Gutierrez, E. Pena, K. Caine, G. Demiris, K. A. Siek, and K. Connelly, "HomeSHARE: Implementing multi-site smart technology infrastructure," in *American Medical Informatics Association*, Washington DC, USA, 2019.

[53] M. Sharma, S. Joshi, D. Kannan, K. Govindan, R. Singh, and H. Purohit, "Internet of Things (IoT) adoption barriers of smart cities' waste management: An Indian context," *Journal of Cleaner Production*, vol. 270, p. 122047, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959652620320941

[54] Y. S. Tan, Y. T. Ng, and J. S. C. Low, "Internet-of-things enabled real-time monitoring of energy efficiency on manufacturing shop floors," *Procedia CIRP*, vol. 61, pp. 376–381, 2017.

[55] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, and B. Lepri, "The privacy implications of cyber security systems: A technological survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 2, pp. 1–27, 2018.

[56] A. Voit, T. Machulla, D. Weber, V. Schwind, S. Schneegass, and N. Henze, "Exploring notifications in smart home environments," in *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, ser. MobileHCI '16. New York, NY, USA: ACM, 2016, p. 942–947. [Online]. Available: https://doi-org.proxyiub.uits.iu.edu/10.1145/2957265.2962661

[57] D. Weber, A. Voit, P. Kratzer, and N. Henze, "In-situ investigation of notifications in multi-device environments," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '16. New York, NY, USA: ACM, 2016, p. 1259–1264. [Online]. Available: https://doi-org.proxyiub.uits.iu.edu/10.1145/2971648.2971732

[58] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang, "Privacy perceptions and designs of bystanders in smart homes," *ACM Humam-Comput. Interaction*, vol. 3, no. CSCW, nov 2019. [Online]. Available: https://doi.org/10.1145/3359161

[59] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, Jul. 2017, pp. 65–80. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[60] E. Zeng and F. Roesner, "Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study," in *Proceedings of the 28th USENIX Conference on Security Symposium*, ser. SEC'19. USA: USENIX Association, 2019, p. 159–176.