Exploring Usability of Data Flow Visualizations in a Privacy-focused Smart Home Dashboard

Brennan Vanden Bos
Western Washington University
Bellingham, USA

Victor Calzada
Western Washington University
Bellingham, USA

Raghav Puri
Woodinville High School
Bellingham, USA

Shrirang Mare
Western Washington University
Bellingham, USA

ABSTRACT

An increasing number of people are introducing smart home devices into their homes, creating significant concerns about personal privacy. Smart home dashboards can offer valuable feedback to users about the status of the devices and any resulting privacy exposure. However, there is limited work on how to present this information in a way that is easy to understand.

In this paper, we explore the usability of a data flow visualization in a smart home dashboard by conducting an in-lab semi-structured study of 18 adults. We asked participants to interact with a sample smart home dashboard that visualized the network activity of smart devices in a test smart home, perform tasks, and provide feedback on the dashboard. Overall, we found that participants found data flow visualization helpful but limited in utility. Compared to the volume of data flow and destination, they expressed a need for more information about the type of data collection and its privacy implications, and control over data flow. Based on these findings, we present four concrete design recommendations for privacy-focused smart home dashboards.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

Internet of Things, Smart Home, Security, Privacy, Dashboard, Visualization

ACM Reference Format:
Brennan Vanden Bos, Victor Calzada, Raghav Puri, and Shrirang Mare. 2024. Exploring Usability of Data Flow Visualizations in a Privacy-focused Smart Home Dashboard. In *Proceedings of the Sixth Workshop on CPS&IoT Security and Privacy (CPSIoTSec '24), October 14–18, 2024, Salt Lake City, UT, USA.*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3690134.3694823

1 INTRODUCTION

Smart home devices have been steadily growing in popularity over the past decade. Consumers view smart devices as an easy way to improve their quality of life. Smart home assistants can be used to play music, set timers, answer phone calls and text messages, and search the Internet. Smart lights can be programmed to turn on and off at set intervals, or have controllable hues. Smart security systems can record footage to the cloud, monitor foot traffic, or lock and unlock doors. These are just some of the multitude of ways smart home devices can interact with daily human life. These products promise to make life simpler and entertaining. As more of the world desires to integrate technology into their daily lives, the demand for smart home devices is likely to continue to increase.

However, smart home devices pose privacy risks to home residents and visitors. These devices can collect and transmit sensitive information about our daily habits and routines [11], such as when we are home or away, what we watch on TV [20], and even our daily conversations [16]. This information can be accessed by the manufacturer, and may be shared with third-parties without the user's knowledge. There have even been recent examples of smart cameras producing unencrypted video streams [8]. As the world becomes more connected with smart devices, it is imperative that consumers understand the associated privacy risks. Unfortunately, many consumers do not fully understand the risks to their privacy posed by the smart devices [24].

Recently, there has been work on both educating consumers on smart home privacy risks [18], and improving the control consumers have over their smart home privacy [10, 19]. In particular, there has been recent development towards smart home dashboards that can provide feedback to users if their privacy is at risk [9, 17, 22]. However, there is limited work on the usability of visualizations in smart home dashboards, focusing on how to present information in a way that is easy to understand. We developed data flow visualizations based on prior work [21, 22] and conducted a user study with 18 participants to evaluate the usability of the visualization and gather feedback on the design of a privacy-focused smart home dashboard. Specifically, our research questions are:

RQ1 To what extent can participants understand the data flow visualizations in a smart home dashboard? Do visualizations increase awareness of privacy risks?

RQ2 What features do participants expect in a privacy focused smart home dashboard?

From our interviews, we found that participants were able to understand the data flow and were more intrigued by unexpected

CPSIoTSec '24, October 14–18, 2024, Salt Lake City, UT, USA.

ACM ISBN 979-8-4007-1244-9/24/10
https://doi.org/10.1145/3690134.3694823

data flows. They had varying levels of trust in smart home devices and perceived only audio/video recording devices as privacy risks. They expressed a desire for transparency and control over their data, among other things. Based on our findings, we synthesized four design recommendations for privacy-focused smart home dashboards.

2 RELATED WORK

2.1 Smart Home Privacy

Recently there have been a number of research projects detailing privacy and security concerns with smart home devices. Mandalari et al. [12] analyzed common household IoT devices to determine what traffic is non-essential and can be blocked. Of the 31 devices these researchers examined, 16 of them had at least one non-essential traffic destination. This work relied on blocklists specific to each device. Zou et al. [25] developed IoTBeholder, a platform that was able to determine both smart home device identification and behavior, and from that they infer user activity and patterns with high accuracy. Haar and Buchmann [7] created an IoT firewall named FANE, which can create specific firewall rules based on network traffic from smart home devices. Although this work was more focused on the security risks of smart home devices, monitoring and segmenting network traffic from smart home devices is essential for privacy work as well. Park et al. [15] conducted a study with 32 privacy-conscious smart home power users and found that, overall, their participants wanted more transparency and control over their smart home devices. Zheng et al. [24] conducted eleven interviews with smart homeowners to discuss their viewpoints and actions they have taken regarding smart home privacy. Their work found that users often trusted device manufacturers but did not do any verification of privacy protections. They also found that many users were unaware of the potential privacy risks of data traffic from and to smart devices. This unawareness towards potential privacy risks is why the implementation of privacy dashboards is so important.

In 2017, Apthorpe et al. [1] took a more macro view and surveyed over 1700 American adults via the Amazon Mechanical Turk platform to determine privacy norms and best practices for IoT device manufacturers. Interestingly, their work found that the average consumer viewed data leaving the household as unacceptable unless the device owner had explicitly granted consent. Marky et al. [13] took a novel look at the privacy considerations of smart home households by examining the concerns of visitors to the home. Their work stated that visitors have similar concerns to owners, but that they lacked the ability to determine what privacy violations are at risk. The authors then proposed data visualizations as a method to provide visitors with feedback on the data collected from the environment. Emami-Naeini et al. [5, 6] took an active approach towards solving privacy concerns with smart devices by considering what should be on a smart device *nutrition label.*

2.2 Smart Home Privacy Dashboards

Recently there has been some work with privacy dashboards specifically designed for smart homes. Huang et al. [9] developed IoT Inspector, an open source tool that uses crowdsourced labeled network traffic to visualize the activity of IoT devices and help identify when devices are vulnerable to security risks. Although a powerful tool, IoT Inspector lacks live visualization and is too technical for the average smart home user. Windl et al. [22] developed a digital dashboard combined with a physical dashboard titled “SaferHome”. In their work, participants were alerted via both a physical and digital dashboard of security vulnerabilities in their smart home devices and given feedback on solutions. Their work found that users were particularly concerned with the capabilities of voice assistants. A similar approach to our work was taken in 2020 by Seymour et al. [17] with their Aretha project. Aretha provides real-time feedback on network traffic leaving the house, and provides visualizations of both the volume of traffic and the destinations of the traffic. While the researchers for this project deployed their probe in three households, only one of those households had a smart device (a smart speaker), and the rest of the devices were laptops and phones. This limited the insight into privacy concerns specific to smart homes. In our study, we used four different types of smart devices and focused only on smart device network traffic.

3 METHOD

Our study was advertised as a “Research Study on Smart Devices” via flyers and mailing lists, without any explicit mention of privacy as the focus of the study to minimize participation bias. The study was approved by University IRB. All participants were over the age of 18, and were compensated for participating in our study.

3.1 Study design

The study was designed as an in-lab semi-structured interview with a sample smart home dashboard as a probe. Participant interviews were split into three stages.

In the first stage, participants were asked to describe smart devices and how they work. We also asked participants about any privacy concerns they had with smart devices and what steps, if any, they took to manage their privacy. This stage was designed to understand participants' mental models of smart devices and their privacy concerns, if they had any.

In the second stage, participants were shown a sample smart home dashboard and asked to peruse it while describing their initial impressions; we used the think-aloud method here. The dashboard showed controls for smart devices connected to a test smart home in the lab, and participants could turn on/off the devices and observer the change in the device in real time. We designed the dashboard (more on this in 3.2) to help ground the conversation in a concrete example. We then asked participants specific questions about the shown data visualizations to check if they understood the visualizations and if they can navigate the dashboard. The questions were, for example, “which device has contacted servers in Australia?”, “what are some of the websites that were contacted by the smart plug in the last hour?”, and “Which device sends the most data outside of the home?”.

In the third and last stage of the interview, we asked participants which devices in the test smart home they felt were most and least privacy conscious. We also asked them to describe what features they felt were missing from the dashboard, or which aspects of the dashboard they found confusing or unintuitive. We ended the interview by asking them basic demographic questions (age, gender, education level).

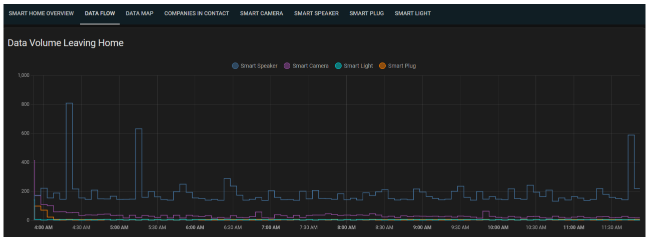


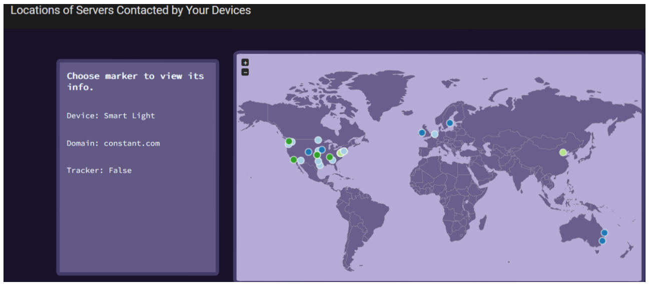
Figure 1: Visualization showing data flow (number of packets) for each devices.

Participant interviews were recorded and then transcribed using Descript followed by manual correction. We then analyzed the transcripts using thematic analysis [3].

3.2 Dashboard UI

We built a sample dashboard to help participants visualize a smart home dashboard interface and provide input on what features they would like to see in a privacy-focused smart home dashboard. The dashboard UI was built using the open-source software Home Assistant. The dashboard was connected to our test smart home in the lab, which consisted of a smart light and smart plug from Kasa, a home security camera from Tapo, and an audio Chromecast from Google. When designing the dashboard UI, we took inspiration from previous smart home dashboard development, most prominently Aretha [17], which builds on prior work by Van Kleek et al. [21]. Van Kleek et al. [21] proposed a visualization called X-Ray Refine to show the network flow of smartphone applications. Building on the design and recommendations in prior works, we designed the dashboard UI to display the network activity of each device, geographic location of external IP traffic, total volume of external traffic, and the domain names of servers being contacted by the devices. This gives users feedback on the companies in contact, the countries in contact, and the total amount of data being sent outside the home.

The UI itself consisted of four overview tabs displaying different information and four device tabs. The initial tab titled "Overview" displayed controls and feedback on the states of the various smart home devices and a live feed from the camera. The second tab was titled "Data Flow" and had a graph showing the number of packets leaving the local network from different connected devices during the last eight hours (see Figure 1). There was a colored line for each device. The third tab was titled "Data Map" and displayed a world map with overlaid colored dots that indicated the locations of servers that had been in contact with smart devices in the test smart home (see Figure 2). Clicking on a dot would display the domain name of the server, the smart device in contact with it, and whether the domain was a tracker. The fourth tab was titled "Companies in Contact" and consisted of a log of all domains contacted by each smart device in the last eight hours (see Figure 3). Each device had its own swim lane, and by hovering over the log you would see the domain name of the company in contact, and the time of occurrence. Finally, the UI had four device tabs, one for each smart device in the test smart home. The device tab had controls for the device in question, and also had a *data flow* graph specific to that device.



Choose marker to view its info.

Device: Smart Light

Domain: constant.com

Tracker: False

Figure 2: Data map visualization showing destinations for data sent/received by smart devices.

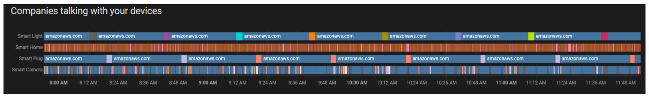


Figure 3: Visualization showing companies in contact with smart devices.

The network traffic displayed on the dashboard consisted of a pre-recorded network traffic log that could be replayed for each participant. This ensured that all participants were shown the same history of data. Participants were not informed that it was a prerecorded log.

3.3 Limitations

Our recruitment was done via convenience sampling. This has resulted in a relatively small size and the demographics of our participants being skewed towards young, college-educated males. This limits the applicability of our findings to the general population. While the recommendations determined from our study contribute to the broader design guidelines for privacy-focused smart home dashboards, performing a similar study with a more diverse population would be valuable to determine the generalizability of our findings.

4 FINDINGS

Eighteen adults participated in our study. Thirteen of these interviews were conducted in person and five were conducted remotely via Zoom. All participants were in the age range of 18–35 years old. Of the 18 participants, 14 identified as male, two as female, and two as non-binary.

Among the participants, smart voice assistant was the most commonly used device (n=13; 72% participants), followed by smart light bulbs (n=3), smart plugs (n=1), smart cameras (n=1), and smart hub (n=1). Three participants did not use any smart home devices. Below, we present the five themes that emerged from our interviews.

4.1 Varying levels of trust in companies

The participants we interviewed had different opinions when discussing large tech companies and their data collection. Several participants expressed lack of trust in companies to protect user privacy and helplessness towards the extent of data collection by companies. "I do not trust Microsoft, Google, Apple, any of them to maintain my data in any of their smart devices like that. In fact, I would not be surprised if they actively sold that." (P16) Participants felt that there was nothing that could be done at this point to protect their privacy from these large companies. "Privacy is one of those things where I've just kind of accepted that I don't have any. Like, it's not ideal, but it's kind of just the world we live in." (P3) This sentiment was also echoed by P10: "I have said for a very long time that I think that privacy is dead online."

However, some embraced data collection and saw that as a price to pay for convenience: "I like using Google. I'm fine to pay the price of having some of my data be sold if I can just have everything be kind of easier and more unified." (P8) Participants expected big companies (e.g., Google, Amazon) to be responsible with data collection and processing, but questioned to what extent their data was misused. "With Google and that stuff, I feel like they handle it properly, but maybe misuse it just cause like you'll be talking about one thing, the next thing you know, ads pop up about it." (P13)

4.2 Concerns about audio/video recording devices

Several participants expressed strong concerns for devices with camera and/or microphone, particularly with voice assistants such as Amazon Alexa and Google Home. Their concerns stemmed from their news reports and their own experiences with voice assistants.

> Amazon Alexas do record your the audio that it captures, even if you don't say whatever activation word it has. So that's that's a red flag. Cause sometimes it has been used to like, solve it has been used to help with solving a crime and whatnot. So in that regard, it's good. But at the same time, it's also That's never something you're going to have to deal with. They're still recording this information and collecting it from you. (P12)

Several participants mentioned how what they say somehow always leads to targeted advertising and that fueled the concern about devices (especially phones and voice assistants) always listening. The following quotes by P11 and P10 illustrate this concern: "I think the one thing is like everybody says that they're like listening to you, which like I don't. I don't want to be crazy or anything, but I do think that sometimes they are listening." (P11) "It has happened so many times where like I will be having a conversation with someone about, like a product or a topic, and it'll pop up in my search engine or just like show up as an ad." (P10)

Participants were concerned about continuous data collection from audio and video devices, and the data being stored and potentially misused by companies or other entities. Some mentioned that they do not use voice assistants or smart speakers due to these concerns. Others who use these devices expressed the associated privacy risk but either accepted it as a trade-off for convenience or felt that there was nothing they could do to protect their privacy.

> I know that the microphone is always on and listening to what is being said in the room by people that aren't specifically addressing Alexa. Whether or not that information is being kept somewhere, I'm sure it is, but I kind of just ignore that and hope that my ignoring it makes it go away (P2).

Compared to devices with camera and microphone, participants expressed less (or no) concern about devices that do not have audio or video recording capabilities.

While some participants acknowledged the potential security risks inherent in bringing any kind of Wi-Fi device onto a network, most of them had the attitude that the data collected from smart bulbs and plugs had little to no privacy risk, as P3 expressed "what are they gonna do with that, honestly". Participants said they were not concerned about these devices because they "don't have microphone or camera" This lack of concern for non-audio and non-video data collection echoes the findings of previous research [24].

For devices such as smart door locks, participants expressed some concern as these devices can have a direct impact on their physical safety. Some participants expressed security concerns with smart locks. "They can just unlock it from outside the home, get inside, maybe steal stuff, commit some kind of crime, and then just leave and lock it again without anybody knowing." (P10) Participant P2 expressed similar concerns with smart locks, and stated that knowing which companies received data from their smart lock would affect how worried they were about security.

4.3 Usability of the dashboard

Even among college-aged participants, who are generally more tech-savvy than most Internet users, we found varying levels of technical knowledge, which affected their interpretation and understanding of the dashboard. Many participants found the dashboard easy to navigate. For example, P11 stated, "I think it's pretty easy to navigate. I think it's pretty straightforward." But some participants were confused about some aspects of the UI such as colors in the data flow visualization, units on the graphs, and the meaning of the domain names in the companies in contact visualization. For these participants, we answered their questions about the UI and let them explore the dashboard further until they were comfortable with it.

To test participants' understanding of the dashboard, we asked them specific questions about the data visualizations. For example, which device sends the most data outside of the home, which device has contacted servers in Australia, and so on. All participants were able to correctly answer the specific questions about the data visualizations on the dashboard, indicating that they understood the visualizations and could navigate the dashboard.

Among the dashboard UI elements, participants particularly liked the visualizations of the data flow and the world map. From the data flow and world map, participants could see which devices were more chatty and where the data was being sent, as P12 expressed "Definitely like the map view, knowing where things are being contacted in part, cause that could also help with Why is this taking so long for it to do?" From the visualization, participants were able to identify unexpected data flows. For example, P16 expressed surprise when they saw a data flow to the .gov domain. "Hold on, dot gov, why is your, why is this contacting the government? That also feels concerning." (P16) Based on participants' reactions and questions about the data flow, we believe that the visualization increased awareness about the extent of the data flow among participants.

Before exploring the dashboard, when we asked participants about privacy risks associated with smart home devices, most of the participants discussed types of data that can be collected (e.g. location, Wi-Fi details, voice through voice assistants, activity in house) and associated privacy in the form of risk to personal information (voice, location) and daily routines. With respect to concerns about potential privacy risks, most participants expressed concern with only audio and video recording device, and considered other types of devices (e.g., smart bulbs, smart plugs) as having little to no privacy risk. After exploring the data flow visualization, participants were curious not just about the type of data collected by a device, but also where the data was being sent, and why it was being sent.

4.4 Desire for transparency over data flow and collection

All participants expressed a desire for transparency in data collection and data flow. When asked what information they would like to know about how their smart devices behave, participants expressed a desire to know what data was being collected, where it was being sent, and how it was being used. After seeing the data map (Figure 2) and the data flow (Figure 1) on our dashboard, almost all participants expressed increased concern about privacy with respect to smart devices.

The map visualization (Figure 2) was particularly interesting for participants. Several participants expressed surprise when they saw that their devices were contacting servers in other countries and questioned why this was happening. Participant P9 remarked "I don't know why people in Australia or like kind of on the other side of Europe need my information. That's a little interesting to me. [...] why is information being collected from way over there?" Participant P6 had similar questions about why servers outside the US were being contacted "Why are there so many servers very far away from you contacting?" For some participants, only certain countries were of concern, with P8 stating that server location would only matter if "something were to be sent to like Russia or North Korea". Some participants mentioned that they would be concerned if their devices contact oddly named servers or servers in specific countries, such as Russia or China.

> [..] the smart speaker just because it is contacting 1e100.net, which is setting off some red flags. Other than that, no, just because there's not any connections to any countries I'd be concerned of, China and Russia mainly. (P13)

The tab of our dashboard titled "Data Flow" displayed a graph of data volume leaving the house similar to visualizations created by previous smart home dashboards such as IoT Inspector and Aretha [9, 17]. Although some participants liked the visualization, with P4 remarking "I think that's awesome [..] you can see how the smart speakers have those big spikes, and then I would start thinking, oh wait, what's going on here?", many participants felt that the traffic volume was insufficient to determine the privacy risk. When discussing spikes in network data traffic, P8 mentioned "with this data flow thing, that's the main one is like, what's all the stuff that's leaving?". P3 had similar sentiments, stating

> This is just saying there is data leaving, but I have no idea what that data is or where it's going. [...] It's interesting, but I don't know how useful it is in terms of actually assessing the privacy of something.

Some participants felt the traffic flow information may be difficult to understand for someone who is not tech-savvy.

> I would say maybe this is a little jumbled. I don't know if jumbled is the right word, but just a lot? Yeah, I would say this might be a lot, especially to somebody who might not be, like, super well versed in this type of stuff. But, it's not, I don't think it's necessarily bad. I think this is probably a pretty hard UI to learn. (P13)

Overall, participants liked the simplicity and cleanliness of the user interface, but questioned its practicality. "I like the interface. I think it's pretty intuitive, I think it's nice and clean." (P1) But also didn't think they would use this UI to regularly monitor their devices. "It seems like if I was using this on a day-to-day basis I wouldn't want to go to my computer and mess with all these things" (P2).

4.5 Desire for assistance in understanding the behavior of the device

A common theme brought up during the interviews was the idea of *anomaly detection*. When interacting with the various graphs and visuals on the dashboard, many participants were unsure if what they were seeing was expected behavior or not. P6 noted: "When I see these graphs, it's just big number, probably bad, small number better, but I really don't know what's going on in this dataset". While spikes in data volume were easy to spot by participants, they felt they lacked the context to understand whether they should be concerned. When asked what features would help ease concerns when adding new devices to a network, P6 stated that they would expect averages along with the log:

> say you expect it to be six, but you plug it in and you're seeing a lot of eights, so you could be kind of concerned, you know, with why is that bulb sending so much data compared to what the average would be.

P1 echoed a similar sentiment, stating "as long as it can tell me that things are looking like normal and it's doing something that's appropriate for the device, then I think that would be interesting to see".

Some participants mentioned that they would like to see more information about devices on their network. For example, any known vulnerabilities for the devices or if the devices are contacting known malicious servers. Participant P7 expressed a desire for a security scan of devices: "It would be nice to do a security scan of those devices that get added when they get onboarded and look for open ports and known vulnerabilities on them". Many participants expressed the need for more contextual information about the devices on their network to help them understand the data flow and the privacy risks. For example, not just the amount of data being sent, but what data is being sent, to whom, and how that data is being used. A few participants also expressed a desire for controls to block data flow to certain servers or at certain times (e.g., when they are not home).

After observing the data flow and data map, participants indicated even greater concern about the privacy of their smart devices.

However, the data presented on the dashboard (which is similar to what commonly available smart home dashboards provide) is not sufficient to help users understand the privacy risks associated with their devices.

5 DISCUSSION

Based on the findings from our interviews, we present four design recommendations for designing a privacy-focused smart home dashboard. These recommendations echo with prior work at a high level, but the explorations of data flow visualizations in this study highlight focus areas for future work.

5.1 Provide overview of data flow with clear explanations

A smart home dashboard should provide an overview of the data flow from smart devices. For data transmitted by devices, it should show the volume of data, when it is sent, where it is sent (e.g., the domain name of the server, as well as region or country), the type of data being sent, and the purpose of the data being sent.

Showing data flow —volume of data sent outside the network, the destination of the data, and the type of data being sent —is necessary for a privacy-focused smart home dashboard, but not sufficient. Participants appreciated the transparency provided by the data flow visualization, and it increased their awareness about the extent of data being sent outside the network. However, many participants expressed a desire for more contextual information to make sense of the data flow. Specifically, the type of data being sent and the purpose of the data. Several participants indicated that this information was more important to them than the total volume of data sent outside.

However, this information is not readily available from network traffic and is an open research question. One possible approach could be to use a crowd-sourced database of smart device data collection practices, similar to the approach taken by IoT Inspector [9], and present that information to the user as possible data types sent outside the network.

5.2 Show expected behavior and alert on anomalies

A visualization of network traffic is helpful to review the behavior of smart devices. However, on a day-to-day basis, as participants expressed, users may not want to spend time reviewing network traffic logs and would prefer to be alerted to anomalous behavior. Thus, the dashboard should include a model of normal behavior for each smart device and alert the user when the device's behavior deviates from that model. The concept of normal behavior for smart devices can cover both security and privacy considerations; for example, how often a device contacts a server, the volume of data it sends, and where it sends data. Furthermore, it will be helpful if the alert clearly explained the anomaly, its potential implications, and the possible actions that users can take, so that users can make an informed decision. In addition, users will find it helpful when reviewing device traffic if the visualization showed how the device's current behavior compares to that model of normal behavior. The concept of anomaly detection for network traffic has been well explored [2], and there is recent work showing promising results in anomaly detection in smart homes [23]. Another approach is using labelled network traffic data to model normal behavior and detect anomalies [14].

5.3 Provide security and privacy awareness

As many users consider the risk of malicious attack to be as much of a privacy concern as normal data collection, any smart home dashboard with an emphasis on privacy should be designed with security in mind. Smart home dashboard should alert users to known security vulnerabilities in their smart devices. A potential avenue for this could be through network scanning [4]. An alternative security solution could be achieved through vulnerability reports similar to the SaferHome [22].

In addition, the dashboard should also educate users about potential privacy risks and how to mitigate them. Similar to most participants in our study, many people may not be aware of the privacy risks posed by smart devices, especially when it comes to devices that do not record audio or video. Providing awareness of potential privacy risks from non-audio/video recording devices is important. Many participants expressed concern about their data being misused by companies but were unsure if smart devices posed any privacy risks and, if so, how to mitigate them. This information could be presented in the form of a privacy guide or a FAQ section within the dashboard.

5.4 Allow users to control their data

Finally, a smart home dashboard should allow users to control their data. Some participants expressed concerns about their devices connecting to servers in foreign countries. This could be achieved by providing users with the ability to block data transmission to specific servers or regions. Indiscriminately blocking all foreign servers could result in loss of functionality, so it is important to alert to the user and help them make an informed decisions about which servers to block. Another possibility would be to try and identify non-essential traffic [12] and only allow essential traffic outside the country. Several participants reported that they unplugged their devices as a way to protect their privacy. Thus, the ability to block data transmission from a device when it is not in use could be a valuable feature.

6 CONCLUSION

Seeking to better understand consumer attitudes and perceptions towards smart home devices, and how to best design a privacy-focused smart home dashboard, we conducted semi-structure interviews with 18 adults focusing on their smart home usage and views. Our interviews revealed varying levels of trust and knowledge among participants, a consensus that audio and video collection is more privacy invasive than other forms of data collection, and the desire for transparency and control over data collection. Based on the feedback of the participants, we present four concrete design recommendations for privacy-focused smart home dashboards for future development and study.

REFERENCES

[1] Noah Apthorpe, Dillon Reisman, and Nick Feamster. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*, 2017.

[2] Monowar H Bhuyan, Dhruba Kumar Bhattacharyya, and Jugal K Kalita. Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, 16(1):303–336, 2013.

[3] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[4] Nicholas DeMarinis, Stefanie Tellex, Vasileios P Kemerlis, George Konidaris, and Rodrigo Fonseca. Scanning the internet for ros: A view of security in robotics research. In *2019 International Conference on Robotics and Automation (ICRA)*, pages 8514–8521. IEEE, 2019.

[5] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020.

[6] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.

[7] Christoph Haar and Erik Buchmann. Fane: A firewall appliance for the smart home. In *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2019.

[8] Sean Hollister. Anker finally comes clean about its eufy security cameras, Jan 2023. Online at https://www.theverge.com/23573362/anker-eufy-security-camera-answers-encryption.

[9] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(2), 2020. DOI 10.1145/3397333.

[10] Mahsa Keshavarz and Mohd Anwar. Towards improving privacy control for smart homes: A privacy decision framework. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–3. IEEE, 2018.

[11] Jacob Kröger. Unexpected inferences from sensor data: a hidden privacy threat in the internet of things. In *First IFIP International Cross-Domain Conference on Internet of Things. Information Processing in an Increasingly Connected World, IFIPIoT*, pages 147–159. Springer, 2019.

[12] Anna Maria Mandalari, Daniel J Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. Blocking without breaking: Identification and mitigation of non-essential iot traffic. *Proceedings on Privacy Enhancing Technologies*, 2021(4), 2021.

[13] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "you just can't know about everything": Privacy perceptions of smart home visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*, 2020.

[14] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. HomeSnitch: behavior transparency and control for smart home IoT devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, pages 128–138, New York, NY, USA, May 2019. Association for Computing Machinery. DOI 10.1145/3317549.3323409.

[15] Sunyup Park, Anna Lenhart, Michael Zimmer, and Jessica Vitak. "Nobody's Happy": Design Insights from {Privacy-Conscious} Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control. 2023. Online at https://www.usenix.org/conference/soups2023/presentation/park.

[16] Anne Pfeifle. Alexa, what should we do about privacy: Protecting privacy for users of voice-activated devices. *Wash. L. Rev.*, 93:421, 2018.

[17] William Seymour, Martin J Kraemer, Reuben Binns, and Max Van Kleek. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020.

[18] Joseph Shams, Nalin AG Arachchilage, and Jose M Such. Vision: why johnny can't configure smart home? a behavioural framework for smart home privacy configuration. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 184–189. IEEE, 2020.

[19] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. Network-level security and privacy control for smart-home iot devices. In *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)*, pages 163–167. IEEE, 2015.

[20] Carlotta Tagliaro, Florian Hahn, Riccardo Sepe, Alessio Aceti, and Martina Lindorfer. I still know what you watched last sunday: Privacy of the hbbtv protocol in the european smart tv landscape. In *NDSS*, 2023.

[21] Max Van Kleek, Reuben Binns, Jun Zhao, Adam Slack, Sauyon Lee, Dean Ottewell, and Nigel Shadbolt. X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1–13, New York, NY, USA, April 2018. Association for Computing Machinery. DOI 10.1145/3173574.3173967.

[22] Maximiliane Windl, Alexander Hiesinger, Robin Welsch, Albrecht Schmidt, and Sebastian S Feger. Saferhome: Interactive physical and digital smart home dashboards for communicating privacy assessments to owners and bystanders. *Proceedings of the ACM on Human-Computer Interaction*, 6(ISS), 2022.

[23] Masaaki Yamauchi, Yuichi Ohsita, Masayuki Murata, Kensuke Ueda, and Yoshiaki Kato. Anomaly detection in smart home operation from user behaviors and home conditions. *IEEE Transactions on Consumer Electronics*, 66(2):183–192, 2020.

[24] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW), 2018.

[25] Qingsong Zou, Qing Li, Ruoyu Li, Yucheng Huang, Gareth Tyson, Jingyu Xiao, and Yong Jiang. Iotbeholder: A privacy snooping attack on user habitual behaviors from smart home wi-fi traffic. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(1):1–26, 2023. DOI 10.1145/3580890.