"It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes

Parth Thakkar
parthkt1@umbc.edu
University of Maryland, Baltimore County
Baltimore, MD, USA

Shijing He
shijihe@cisco.com
Cisco Systems, Inc.
San Jose, CA, USA

Shiyu Xu
shiyuxu@umich.edu
University of Michigan
Ann Arbor, MI, USA

Danny Yuxing Huang
dhuang@nyu.edu
New York University
New York, NY, USA

Yaxing Yao
yaxingyao@umbc.edu
University of Maryland, Baltimore County
Baltimore, MD, USA

ABSTRACT

The opaque data practices in smart home devices have raised significant privacy concerns for smart home users and bystanders. One way to learn about the data practices is through privacy-related notifications. However, how to deliver these notifications to users and bystanders and increase their awareness of data practices is not clear. We surveyed with 136 users and 123 bystanders to understand their preferences of receiving privacy-related notifications in smart homes. We further collected their responses to four mechanisms that improve privacy awareness (e.g., Data Dashboard) as well as their selections of mechanisms in four different scenarios (e.g., friend visiting). Our results showed the pros and cons of each privacy awareness mechanism, e.g., Data Dashboard can help reduce bystanders' dependence on users. We also found some unique benefits of each mechanism (e.g., Ambient Light could provide unobtrusive privacy awareness). We summarized four key design dimensions for future privacy awareness mechanisms design.

CCS CONCEPTS

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

KEYWORDS

Privacy, Smart Homes, Privacy Awareness, Bystanders, Notifications, Multi-Stakeholder

ACM Reference Format:
Parth Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3491102.3502137

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04…$15.00
https://doi.org/10.1145/3491102.3502137

1 INTRODUCTION

Smart homes have been increasingly prevalent in recent years due to their great efficiency and conveniences. A typical smart home consists of various Internet of Things (IoT) devices that can be remotely controlled, accessed, and monitored. These IoT devices, equipped with various sensors and the ability to connect to the Internet, can collect a massive amount of data of the surrounding environment and pose great privacy risks to users. Seemingly innocent (e.g., the on/off status of a smart light bulb) can be used to infer sensitive information about users (e.g., daily schedule) [2].

However, general users have very limited ways to learn about these data practices. Privacy policies of these smart home IoT devices offer some knowledge, but typically not in a meaningful way [28, 34, 35]. As a result, the data practices of smart home IoT devices are typically opaque to general users. Such opaqueness has caused users' privacy concerns about sensitive data collection [45], data sharing [44], and data misuse [23, 24]. Furthermore, it also leads to significant privacy concerns of other stakeholders, or *bystanders*, in smart homes (e.g., visitors, roommates, other family members) since their personal data can potentially be collected without their knowledge. Thus, privacy awareness mechanisms to combat the opaqueness and increase both users' and bystanders' awareness of data practices of smart home IoT devices are in desperate need.

In this paper, we define **smart home users** as those who own smart home devices in their home and **smart home bystanders** as those who do not own smart home devices but may be subject to the data collection by smart home devices [41, 42]. We also denote mechanisms that raise people's awareness of the data practices of surrounding smart home devices as **privacy awareness mechanisms** [32]. We aim to investigate users' and bystanders' preferences of privacy awareness mechanisms in smart homes. Our overarching research question is, **how to deliver privacy notifications and raise users' and bystanders' awareness of data practices in smart homes?** This is an important question because

raising awareness is one of the fundamental principles in privacy protection and the consideration of multiple stakeholders . The answer to this research question can provide insights into the design and development of future privacy notifications for multiple stakeholders in smart homes, raise different stakeholders' awareness of surrounding data collections and eventually, help people make informed privacy decisions [35, 40]. Our research question is also inspired by Schaub et al.'s prior work on the design space of privacy notice [36]. They developed a design space that can help researchers and practitioners identify privacy notice requirements, but given the increasing complexity and connectivity of IoT devices and the multiple stakeholders environment, how to operationalize the design space in the context of smart homes remains unclear. We further break down this research question into the following questions:

RQ1: What factors influence users' and bystanders' preferences of receiving privacy notifications in smart homes?

RQ2: Which modality do users and bystanders prefer to receive privacy notifications in smart homes?

RQ3: How do the preferences differ between users and bystanders in smart homes?

To answer these research questions, we conducted a survey study with 136 smart home users and 123 smart home bystanders. Our survey study focuses on understanding participants' general preferences of receiving privacy notifications in smart homes as well as their perceptions of four privacy awareness mechanisms: an interactive data dashboard that displays the data practices of nearby smart home devices (i.e., Data Dashboard), a smartphone app that sends a push notification regarding the data practices of smart home devices (i.e., Mobility App), an ambient light that shows data collection status through color changes (i.e., Ambient Lighting), and a smart speaker that talks about data practices (i.e., Privacy Speaker). Our results reveal the perceived pros and cons of each mechanism, highlighting the differences in users' and bystanders' perceptions. For example, users may favor Data Dashboard due to the detailed information provided through the dashboard. However, bystanders might be concerned about the possibility of violating the social norm in other people's homes since they would need to interact with other people's devices. Through the scenario-based questions, we found that even though the smartphone app is the most widely accepted privacy awareness mechanism, other mechanisms may still provide unique benefits in certain scenarios (e.g., Ambient Lighting can provide unobtrusive privacy notices when needed).

Our paper makes the following three contributions. First, to the best of our knowledge, we are the first study that examines people's preferences of mechanisms that raise their awareness of smart home devices data practices from both users' and bystanders' perspectives. Second, our results highlight the pros and cons of four privacy awareness mechanisms and uncovered the contextual needs and mismatches between users and bystanders. Third, we proposed key design dimensions to guide the design of privacy notifications in smart homes.

2 RELATED WORK

2.1 Smart Home Users' and Bystanders' Privacy

Broadly speaking, there are two types of stakeholders involved in a smart home, i.e., users and bystanders. Extensive research has been done to investigate people's privacy concerns and experiences in smart homes from both perspectives. For users, they are typically concerned about their personal data being collected, shared, and analyzed, as well as their home being hacked [41, 44]. There are many factors that can potentially influence people's privacy perceptions in smart homes, such as the types of devices, contexts, types of data collection, purposes of data collection, as well as their perceived trustworthiness of the device manufacturers or service providers [5, 9, 29, 45]. For example, users have expressed strong concerns about their data being shared with third parties by smart speakers [24], but such concerns can potentially be mitigated or reduced if the users trust the manufacturers of the speaker [22]. In the context of smart TVs, when people are not sure about how the TV handles their data, they tend to be concerned about the data collection, data usage, and data sharing with third-parties [23].

Another stream of studies on smart home privacy concerns and risks focuses on bystanders. For example, in smart speakers, the data of secondary users (i.e., users who are in the background) can potentially be collected, posing privacy risks to them [22]. Nannies, who can be considered as bystanders, have concerns related to surveillance by the homeowner when smart security cameras are installed [6]. Smart home visitors were generally unaware of the data collection around them, putting their privacy at risk [26].

When comparing users and bystanders, literature has also suggested differences in their perceptions from two aspects, i.e., device control and privacy expectation. In terms of device controls, primary users have more controls on smart home devices comparing those of bystanders in a multi-user home [16]. They sometimes would restrict other people's access and control to certain devices [44], except for some situations where primary users would like to increase the safety and security of their home [37]. In the latter case, the primary users can sometimes grant remote access to their devices to trusted families and friends [37].

In terms of privacy expectations and mitigation strategies, bystanders tend to prioritize their relationships with the users and potential social confrontations in privacy protection over their own privacy [42]. As a result, while users may want to have straightforward mechanisms to protect their own privacy, bystanders generally prefer to have a communication channel where they can negotiate their privacy needs with the users [41, 42]. In the context of Airbnb, even though the guests and hosts have similar views on data collection, their expectations on data access are different. For example, 90% of guests did not wish to share their browsing history while 20% hosts would like to access that information [25].

2.2 Privacy Notice

An extensive body of research has studied different aspects of privacy notices, such as usability issues [4, 11, 18], new privacy notice interfaces [12, 14, 19, 20], privacy notice design spaces [35, 36], and technologies and policies to better support privacy notice [17, 21, 33]. In particular, to increase the transparency in the context of mobile privacy [38] and facial recognition [39], a multi-stakeholder

process has been initiated in response to the Consumer Privacy Bill of Rights [3]. Notably, the smart home context has also turn into a multi-stakeholder environment [25, 37, 42], yet the majority of prior work on smart home privacy notice has been focusing on either individual stakeholders or individual devices. For example, Emami-Naeini et al. proposed the IoT Nutrition Label as a way to inform potential device buys of the data practices of the device [14]. Marky et al. found that smart home visitors, even though they had their privacy expectations, generally lack the means to judge the consequences of data collection [26].

2.3 Summary

Drawing from the literature, this paper shifts the focus from examining people's privacy concerns and expectations in smart homes to investigating how to deliver privacy notices to users and bystanders and help them be more aware of the data practices in smart homes. Besides users' and bystanders' reactions to four privacy awareness mechanisms, we also aim to understand their selections of mechanisms in different scenarios and investigate any mismatches between users and bystanders in terms of their preferences.

3 METHODOLOGY

We conduct a survey study to investigate users' and bystanders' preferences of privacy awareness mechanisms regarding the data practices of smart home IoT devices. To compare the preferences of users and bystanders, we design and implement two versions of the survey, one for users and one for bystanders. The two versions use the same set of questions following the same flow, but some questions are framed slightly differently to account for the different perspectives. In the following section, we will describe our survey flow in detail. The complete survey protocol for both versions can be found in the supplementary materials. The study was approved by the university IRB.

3.1 Survey Design

Background questions. We start the survey by asking participants about their experiences of using smart home devices, including the devices they have used/own, purposes, and location of these devices. We then ask participants to indicate their experiences and preferences of receiving notifications in smart homes in general, including what types of notifications they have received, how they generally receive notifications, and their willingness to receive notifications. We finish this section by asking participants their overall concern level regarding the data collection in smart homes using Likert scale questions.

Privacy Awareness Mechanisms. Then, we introduce four privacy awareness mechanisms to participants. These mechanisms include: 1) a Privacy Dashboard (i.e., a dashboard that provides detailed information about the data practices of surrounding smart home devices); 2) a Mobility App (i.e., an app that provides push notifications regarding the data practices of nearby smart home devices); 3) an Ambient Light (i.e., an ambient light that can change colors and brightness based on the volume and privateness of collected data); and 4) a Privacy Speaker (i.e., a speaker that broadcasts the data practices of connected smart home devices through audios).

The choices and design of the four mechanisms are motivated by four considerations. First, existing smart home devices generally send notifications to users in four different ways, i.e., visual signals (e.g., LED indicator), audio cues (e.g., voice reminder), push notification through associated apps, and interactive web apps. Thus, when we design privacy awareness mechanisms, we aim to leverage these modalities in our designs. Second, instead of leveraging the built-in functions in smart home IoT devices, we choose to design standalone devices for delivering privacy-related notifications since the notification features in most off-the-shelf smart home devices are not designed to inform users of data practices. Thus, we take an alternative route and design *external* awareness mechanisms to offer more possibility (e.g., the Mobility App is partially inspired by Colnago et al.'s prior work on Personalized Privacy Assistant [10]). Third, each of the four mechanisms represents a combination of different factors, including the amount of information available to people (e.g., the Privacy Dashboard shows more information while the Ambient Light contains fewer details), whether users need to take actions, and the amount of effort required from users. Lastly, we also consider the technical feasibility of each mechanism to ensure that they are not unrealistically speculative. For example, the Data Dashboard can be feasible when built on top of prior work (e.g., IoT Inspector [17]); we have also built an early prototype of the Ambient Light to demonstrate its feasibility.

For each mechanism, we include a short description along with two to three images to illustrate the design of the mechanism. The descriptions for the user branch and bystander branch are framed slightly differently to be considerate of the different perspectives. We iteratively revise these descriptions through internal testing within the research team, initial external testing with friends and families, and final external testing with participants from Prolific. Next, we present the description and example design of each mechanism from the user's perspective.

Data Dashboard (Figure 1). The Data Dashboard is a physical device developed to give your details regarding the data practices of smart home devices (e.g., data generated and shared by these devices) in your home. It can be mounted anywhere in the house based on your preferences. On the home screen, you can get an overview of how much data each device has collected and with whom your data has been shared. You can also check out the details of each individual device in your home network and see the details of the data practices of the device you pick. In addition, the dashboard can also send you notifications regarding the data collection and sharing in your smart home. You can set up different criteria (e.g., when sensitive personal information is collected) to trigger the notification function, then the app will send notifications when the criteria is met.

Mobility App (Figure 2). The Data Protector is an app on your phone which is designed to provide details of data usage status in your smart home. When you connect your phone to your home network, the app will scan your home network and identify all smart home devices that are connected to your home network. It can monitor all devices and provides clear information for data collection status from these devices, including device info, data collection, and sharing status, etc. It can also send you notifications regarding data collection and sharing in your smart home. You can set up different criteria (e.g., when sensitive personal information

Figure 1: Data Dashboard

Figure 2: Mobility App

is collected) to trigger the notification function, then the app will send notifications when the criteria are met.

Ambient Lighting (Figure 3). Ambient lighting is a smart bulb-based product that is dedicated to provide users notifications regarding the data collection and sharing in their smart home. The lighting notification is defined in two dimensions. The colors of the light represent outbound data collection security. Green light means the data is encrypted and safe, and red light means the data is being tracked and not safe. The brightness of the light represents how much data the device is collecting. The dark light represents less data collection, and bright light represents more data collection. Once you see the light changes color, you can then ask the owner for details of the data collection if you are interested to know more.

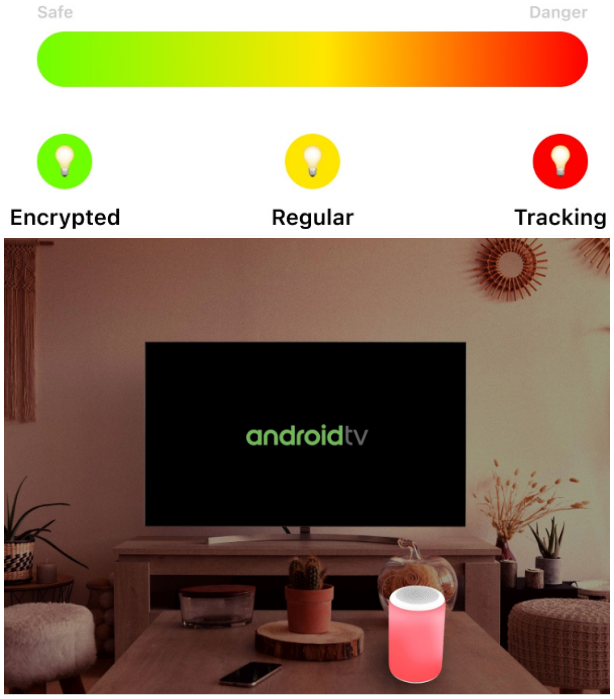

Figure 3: Ambient lighting

For example, the Ambient light can notify you of the data collection status by a smart TV. When the smart TV is displaying "Android TV" and the system now is standing by, the TV will take and track a lot of data. At the same time, the system is vulnerable, so the light becomes bright red. When the system is fully opened and is playing a video, it still shares a lot of data (e.g., due to playing videos) but the data is secure, so the light changes to bright green. At this time, if you are interested to know more about the details of the data collection, you can ask the owner for help.

Privacy Speaker (Figure 4). The privacy speaker is an audio IoT network traffic notification system for smart homes. The privacy speaker informs its users about outbound data traffic from all smart devices connected in the smart home with enabled audio notifications. For example, a smart TV requires a large amount of data traffic when it opens up, but at the same time, it can be vulnerable. When a smart TV starts up, the speaker will inform the users, "Your LG Smart TV is collecting a large amount of data and could be very privacy-invasive". Then, if you are interested to know more about the details of the data collection, you can ask the owner for help.

Then, we ask participants to rate each mechanism based on their *perceived* effectiveness, *perceived* ease to use, and comfortableness to use through 5-points Likert scale questions. These three aspects are inspired by [43]. In the end, we ask an open-ended question for participants to briefly explain their answers. All mechanisms are presented to the participants in random order.

Figure 4: Privacy Speaker

Scenario-based questions. In the last part, we provide participants four hypothetical scenarios since people's privacy perceptions are deeply rooted in and can be influenced by specific contexts [30, 31]. These scenarios include a Biometric Security scenario, a Friend Visiting scenario, a Work from Home scenario, and a Health Data Tracking scenario. When crafting the scenarios, we deliberately considered several factors, such as types of devices, purposes of device usage, social relationships, etc. We also frame each scenario description from both users' and bystanders' perspectives. Below is an example of the Friend Visiting scenario from both users' and bystanders' perspectives.

Friend Visiting scenario - User version. You own a smart home with various smart home devices in it (e.g., smart speakers, smart security cameras, smart lighting, smart appliances, etc.). In particular, you have smart speakers and security cameras installed in your dining room. This weekend, you are inviting your close friends to come over to your place for a movie night. When they arrive, you and your friends first have dinner in the dining room where you chat for a long time. Then, after dinner, you all move downstairs to watch a movie. You notice that some of the ads at the beginning of the movie are very relevant to the topic you discuss at dinner.

Friend Visiting scenario - Bystander version. Your friend, Bob, owns a smart home with various smart home devices in it (e.g., smart speakers, smart security cameras, smart lighting, smart appliances, etc.). In particular, he has smart speakers and security cameras installed in his dining room. This weekend, you are invited to go over to his places for a movie night. When you arrive, you and other friends first have dinner in the dining room where you all chat for a long time. Then, after dinner, you all move downstairs to watch a movie. You notice that some of the ads at the beginning of the movie are very relevant to the topic you discuss at dinner.

Similarly, all scenarios are presented to the participants in random order. After each scenario, we ask for participants' comfortableness of using smart home devices in this scenario, their interests in learning about data practices as well as receive privacy-related notifications, and which mechanisms they would like to use. We end the survey by asking them to briefly explain their answers through an open-ended question.

3.2 Participants

We implemented both surveys branches on Qualtrics and recruited survey participants from Prolific, a crowdsourcing platform. Participants would qualify for the user survey if they have owned smart home devices in their own homes. This qualification check was completed by a built-in filter provided on Prolific. We did not have a requirement on bystanders' prior experiences with smart home devices because anyone can be a bystander in some contexts, regardless of their experiences or ownership of smart devices. For both surveys, eligible participants also need to 1) be located in the US; 2) be over 18 years old; 3) have at least 95% task approval rate.

In total, we collected 300 responses, with 150 responses from each survey branch. After removing the low-quality responses, we receive 136 valid responses from the user survey (U) and 123 valid responses from the bystander survey (B) after excluding low-quality responses. The average time to finish the survey is 21 minutes and each valid response receives $4 as its compensation.

3.3 Study Flow

Before officially launching the main survey, we ran three rounds of pilots (one round with friends and families, two rounds with real participants on Prolific) on the user and bystander branches and collect participants' feedback on potential improvement on the survey design. After we finalized the survey design, we launched both surveys in batches with 30 participants in each batch. We launched these batches at different times of different days throughout the week so that we could account for participants' various working schedule (e.g., weekday vs. weekend, morning vs. evening) and their geographic location (e.g., east coast vs. west coast).

3.4 Data Analysis

Our surveys contain both quantitative data (i.e., binary questions, multiple selection questions, and 5-point Likert scale questions) and qualitative questions (i.e., open-ended questions). Upon completion of data collection, three researchers went through all data several times to familiarize themselves with the data, and at the same time, identify low-quality responses. For qualitative responses, we conducted a thematic analysis [7]. Three researchers first coded a subset of the data together to establish a basic common understanding of the coding and came up with an initial codebook. The three researchers then independently coded another subset of the dataset. Upon completion, they met, discussed, and reconciled their codes to resolve any disagreement, then updated the codebook. Using this codebook, the same researchers divided the rest of the data and finished the coding independently. In the process, they constantly checked each other's codes to make sure the coding is done properly. Next, we present the findings of our study.

4 RESULTS

4.1 Participants

Table 1 summarizes the age, gender, past smart home experiences, and general privacy concern level of our participants. In summary,

	Users	Bystanders
Age	63.9% 18-24 years old 32.3% 25-34 years old 3.6% 35 - 44 years old	60.2% 18-24 years old 26.0% 25-34 years old 8.9% 35-44 years old 4.9% 45-54 years old
Gender	30% Male 66.3% Female 3.7% non-binary	31.1% male 62.4% female 6.5% non-binary
Experiences	100% have experience	82.7% have experience 17.3% no experience
Concerned?	24.7% not at all 65.2% somewhat 10.1% very concerned	30.1% not at all 52.8% somewhat 17.1% very concerned

Table 1: Demographic information of users and bystanders.

both users and bystanders represent a diverse background in terms of their age and gender. All of our user participants have prior experiences with smart home devices while 17% of our bystanders participants do not have prior experiences. The majority of both users and bystanders are either somewhat concerned or very concerned about data collections by smart home devices.

4.2 Notification Mechanisms

Next, we present participants' responses to each mechanism. For the Likert scale questions, we merged "agree" and "somewhat agree" to represent positive attitudes. Similarly, we merged "disagree" and "somewhat disagree" to represent a negative attitude.

4.2.1 Data Dashboard. Data Dashboard is well perceived by both users and bystanders in terms of its perceived effectiveness (users: 89% positive; bystanders: 79% positive) and perceived ease to use (users: 81% positive; bystander: 67% positive). However, the comfortableness of adopting the dashboard drops for both users (57% positive) and bystanders (54% positive). We conducted thematic analysis on the open-ended questions and conclude the main pros and cons below.

Pro: providing detail information (both). Both users (n=54) and bystanders (n=46) appreciated the detailed information provided by the Data Dashboard. They believed that a data dashboard could provide all the information they might need to know regarding the data practices of smart home devices (e.g., data collection, data sharing, data volume, types of data, etc.). For example, U80 found the Data Dashboard to be very detailed and believed that it would reduce his privacy concerns, *"I think this is probably the best one. It gives many details and I would probably buy and use it. It would help alleviate my concerns a bit." (U80)*

Pro: a centralized source of information (both). Another advantage brought up by both users (n=22) and bystanders (n=17) is the centralization of the information. Participants appraised the device since they would be able to see all the details of the data practices across all smart home devices they have. Given that a relatively large portion of our participants (see Table **??**) have more than one smart home device, the centralized source of information reduces the amount of effort from our participants to understand the data practices. U102 explained this point nicely, *"In theory, this Data Dashboard sounds like an effective way to understand data usage from smart home devices. I think that it would definitely take some time to understand how it works, but having everything in one place seems like an easy way to understand data usage across smart devices." (U102)*

Pro: reduce dependence on users (bystanders). Several bystanders (n=11) appreciated the Data Dashboard being a standalone device. With this device, if bystanders wanted to learn about the data practices of surrounding smart home devices, they could simply check out the details on the devices instead of asking the owner, which could sometimes be awkward due to the power dynamics of social relationships. B60 commented, *"This provides a very easy way to look over all data being collected from any device at any time. You don't have to rely on the owner to educate themselves on how to find the information about what's being collected as it is all neatly packaged via this device." (B60)* In this example, the Data Dashboard provides an alternative way of accessing information about data practices rather than asking the users for help.

Con: lack of control (both). One major concern shared by both users (n=24) and bystanders (n=23) is the lack of control in the Data Dashboard. They argued that simply providing details of data practices would not help with alleviating their privacy concerns as they could not do anything about it. This concern highlights a fact that privacy awareness alone is not enough in the context of smart homes, as people would also expect to have control of their data. For example, B39 illustrated her view on this point, indicating that not having access to stop the recording did not help with mitigating her privacy concerns. *"If I am a bystander and not the owner of this device I wouldn't have access to changing the features or anything according to my preferences which would not alleviate any fears." (B39)*

Con: violating social norms (bystanders). Another major concern from bystanders (n=26) is the possibility of violating general social norms in other people's homes. On the one hand, the Data Dashboard would contain all the information about the users, possibly including a list of devices they own at their home, personal data, their device settings, etc. It would be a violation of the users' privacy if they interact with the device. On the other hand, many bystanders believed that checking other people's devices at their homes would simply be rude. The following example from B42 illustrates this point. *"It is set up by the owner, the owner may not have settings for bystander information. I am also not going to violate their privacy by going through their PERSONAL data dashboard. " (B42)* B103 further commented that using the Data Dashboard could potentially cause his social anxiety because he would need to find information on data practices from other people's devices in their homes. Even though the Data Dashboard would always be accessible to the bystanders, using other people's devices randomly could potentially put him in an awkward social situation and thus cause anxiety. *"It would probably turn into a social faux-pas to look at someone's security panel. My social anxiety hates this idea." (B103)*

Con: an additional piece of device (users). Some users (n=9) express the concern that they would need to purchase another device for their home, making it a less appealing option. This is particularly true if the Data Dashboard is only able to provide details of the data practices without enabling any controls to limit the data collection, as U102 put it, *"I like how detailed this device is*

but I would not want to have another device mounted in my house if all it does is give me feedback about data." (U102)

Con: digital literacy required (both). Some users (n=9) believed that they need to have at least some digital literacy to be able to use the Data Dashboard. A few bystanders (n=7) also shared a similar concern. They thought that the information provided by the Data Dashboard could be overwhelming for someone who does not have enough knowledge of smart home devices, which might further lead to emotional anxiety. Some bystanders (n=3) also wondered whether the users would have enough digital literacy to set up the Data Dashboard properly. For example, B54 wondered whether the owner would be capable of properly setting up the device, *"I think the data dashboard would be helpful assuming the owner is capable of setting it up to send notifications to the bystander." (B54)*

Con: lack of trust on device settings (bystanders). One interesting concern held by several bystanders (n=4) relates to their trust towards the Data Dashboard, or more specifically, towards the users. They tend to believe that the users could easily set up the device to not display any useful information when their data was collected. B29's responses showed such a lack of trust towards the user, *"I don't think this option would be good for bystanders because the owner of the device could easily set the notifications to not go off when data is being collected" (B29).* Additionally, a small number of bystanders also did not trust the technical capability of the Data Dashboard and believed that the information provided on the dashboard may not be the full picture.

4.2.2 Mobility App. As seen in Figure 5, the Mobility App is consistently rated the highest among all four mechanisms in terms of its perceived effectiveness (users: 95% positive; bystanders: 93% positive), perceived ease to use (users: 90% positive; bystander: 85% positive), and the comfortableness of adopting the app (users: 81% positive; bystanders: 80% positive). The thematic analysis of the open-ended questions indicates the following themes to explain the high ratings.

Pro: accessible from their private devices (both). Many users (n=55) and bystanders (n=47) acknowledged that they relied on their mobile phones in many cases as mobile phones are highly private devices that they trust. The Mobility App provides a direct and convenient way to check the data collection status of the surrounding smart home devices, especially if sensitive data is collected. Some users also pointed out another advantage of the app, i.e., they could still receive notices of the data practices even when they are away from home. *" I like the idea of more visibility into who and what is using my data. I also have my phone with me at all times and appreciate getting notified on my phone. This would work great if I wasn't home but there were privacy concerns and I can see it on my phone." (U56)*

Pro: detailed information (both). Similar to the Data Dashboard, both users (n=37) and bystanders (n=31) believed that the app would be able to provide detailed information regarding the data practices, which largely increases their awareness. More importantly, interacting with the app did not have a deep learning curve compared to the Data Dashboard. B110 spoke highly about providing privacy awareness through the app, believing that it would be an effective way to be aware of his personal details,*"I think having an app to explicitly tell you when sensitive information is being collected is both effective and discrete. It's an optimal way to be informed your most sensitive details are being picked up by a nearby ever-listening machine." (B110)*

Pro: overcome social awkwardness (bystanders). One key benefit of the app was that it can help bystanders (n=17) avoid the pressure of any potential social norms, mostly because bystanders generally were more comfortable interacting with an app on their own devices than interacting with a device mounted on the wall in a home where they were guests. As a result, they did not need to deal with potential social awkwardness. In addition, the app could also reduce bystanders' dependence on users in order to learn about data practices of surrounding smart home devices, further increasing their autonomy in privacy protection, as B67 suggested, *"This app allows you to protect yourself regardless of where you go. You don't have to depend on the owners of the smart devices to have a separate device to warn you about data usage/collection." (B67)*

Con: invasion to users' privacy (bystanders) One main concern raised by many bystanders (n=21), similar to the concern of the Data Dashboard, was that the app may invade the users' privacy since bystanders would need to connect to the users' home Wi-Fi and scan all connected devices at the users' home. They deemed this as an invasion of the users' privacy. *"As a bystander, I don't feel comfortable having other people's information it seems to me like an invasion of privacy." (B116)*

Con: security concerns (users). One concern regarding the app from the users (n=5) was the potential security issue that comes with it. Based on the mechanism description, the app would need to connect to the home Wi-Fi in order to scan all connected devices. However, that may also open up potential security issues, such as hacking. U72 explained his concern on his specific issue, noting that if bystanders could connect to his home network, anyone should be able to do it fairly easily, *"I would need more information on this, for the homeowner all people have to do is download an app and they can see the smart devices you have setup. From that point what all does it take just to connect and hack into these devices?" (U72)*

4.2.3 Ambient Light. Compared to the previous two mechanisms, both users and bystanders were less positive towards the Ambient Light across all three aspects, i.e., its perceived effectiveness (users: 72% positive; bystanders: 69% positive), perceived ease to use (users: 71% positive; bystander: 65% positive), and the comfortableness of adopting the app (users: 54% positive; bystanders: 63% positive). One interesting phenomenon here is that bystanders were more comfortable with using the Ambient light to understand the data practices of surrounding smart devices. The thematic analysis results in a few major themes to help explain the phenomenon.

Pro: easy to understand (both). Many users (n=65) and bystanders (n=42) considered the Ambient Light as an easy-to-understand mechanism. The color and brightness of the light provided simple information for participants to quickly understand the current status of the surrounding smart home devices. U14 indicated that the light presents a binary case and allowed her to quickly understand whether her data was collected or not. *"This is a great, very simplified way of communicating data usage and tracking to a user. It is very black and white with how it communicates information which would make it very easy for many people." (U14)*

Pro: unobtrusive (both). Another advantage of the Ambient Light, as brought up by both users (n=14) and bystanders (n=11), was its ability to blend into the background and remain unobtrusive. Since the light could adjust the colors and brightness by itself, it would not interrupt people's ongoing activities or reveal too much information. B114 noted on this latter point, saying that *"this device is much less invasive and can state things without telling everything about a person's data" (B114).* Some users also mentioned that the Ambient Light provides them more autonomy in controlling their personal data. For example, when U80 saw the changes in the light, they had the choice to either ignore it or take more action to investigate the details. *" This way I'm not constantly being interrupted by the smart device–it just changes color and I can choose what to do from there. I would probably use this." (U80)*

Con: not informative (both). Although the Ambient Light was perceived as easy to understand, some users (n=19) and bystanders (n=23) believed that the light itself did not contain enough information for them to understand the details of the data practices, such as which devices collect the data and where the data goes. Several bystanders (n=4), such as B52, also mentioned that if it was not their own home, they might not have knowledge of the meanings of the colors, making the notification less understandable. *"As a bystander, I wouldn't know what the different colors or brightness levels on the device stand for, so I wouldn't be learning about my data being tracked by observing this device." (B52)*

Con: requiring too much effort (both). Some participants believed that the Ambient Light required too much effort from them as users (n=13) or bystanders (n=7). The unobtrusiveness, on the other, also meant that people would need to constantly check on the status of the light if they would like to be alert of the data collections around them. Moreover, they had to stay in the room to be able to notice the change. For bystanders, if they did not know the meaning of the colors, they would need to learn those first before they could understand messages from the light. B31 nicely illustrated these points through her response, *"I think this option is too static and requires too much active attention dedicated to watching the light for possible changes to be effective. If I move to a different room and am no longer in a sightline to the light then it becomes completely useless. Additionally, I'm not sure, without initial explanation, that I would intuitively understand the various changes in lighting and if the owner needs to explain it to me at the outset they should just explain what data is being collected and skip this middle step." (B31)*

Con: psychological burden (bystanders) Some bystanders (n=4) brought up the possibility that changes in the colors could lead to negative emotional impact or psychological burden. When the light changes color from white to red, a bystander probably would only notice the room turns red without realizing what is going on. Such a case could potentially cause discomfort for some people, such as B115. *"It is easy to understand but it is also kind of scary. I would just get a really bad feeling if the whole room just turned red and I didn't know why right away since I'm a bystander. I would rather get a notification on my phone that I could check there instead of the lighting changing." (B115)*

4.2.4 Privacy Speaker. Many users and bystanders are positive about the Privacy Speaker in terms of its perceived effectiveness (users: 79% positive; bystanders: 81% positive) and perceived ease to use (users: 76%; bystanders: 69%). However, both users' and bystanders' attitude drops when asking their comfortableness of using Privacy Speaker (users: 37%; bystander: 50%). Here, we also noticed that similar to the Ambient Light, Privacy Speakers also received a higher rating from bystanders than users when asking about their comfortableness of using it. Our open-ended responses surfaced some rationales.

Pro: effortless (both). Similar to the Ambient Light, many users (n=21) and bystanders (n=31) believed that the Privacy Speaker would be able to provide some level of details without additional efforts from them. Particularly, some bystanders, such as B78, deemed the Privacy Speaker as "bystander friendly" since it could reduce their dependence on the users to be aware of the data collection. *"The Voice Recorder would require little to no knowledge about smart homes to be able to use it and see what data is being collected, therefore it is bystander friendly." (B78)*

Pro: reduce social confrontations (bystanders). Several bystanders (n=10) also considered the Privacy Speaker as a way to reduce the potential social awkwardness when they wanted to be aware of the data collection in other people's homes. As B31 explained in her response, by delivering the information directly through voice, the Privacy Speaker could potentially reduce her dependence on the users. *"It would be helpful since it gives notifications out loud and I understand I could ask the owner for more information, but they may not be apt to give it to me. Therefore I agree that this would make me more aware of what's going on around me." (B31)*

Related, when compared to the Data Dashboard, the Privacy Speakers may also reduce the possible confrontation since they did not need to actively look for the Data Dashboard which, as mentioned before, was considered as rude. *"As a bystander in a home you are naturally less inclined to navigate the home with as much familiarity as a homeowner would. These messages would be effective in letting me know about potential risks." (B8).*

Con: annoying and intimidating (both). One of the main reasons why many users (n=34) and bystanders (n=22) preferred not to use the Privacy Speaker was that the consistent voice reminders could quickly become very annoying. In some cases, some bystanders may even felt intimidating by the voice reminders, as B116 noted, *"I like that the Privacy Speaker is transparent with the user, though I might feel a bit uneasy hearing that every I go to relax if I am, for example, on a leisure vacation. I would rather the info be given in writing on the screen or by the person whose home I am using" (B116).* In this case, B116 would prefer to have a written notice instead of the voice reminder.

Con: not informative (both). Although the Privacy Speaker is capable of providing useful information, many users (n=12) and bystanders (n=5) still thought that it was not as informative, especially when compared with the Data Dashboard or the Mobility App. A few users also mentioned that the audio output from the Privacy Speaker could be embarrassing even when only a limited amount of information is provided, as some of the information might be sensitive. *"I think this device would not particularly make me feel safer about my sensitive info and data. It's too general, and it doesn't display the information being collected, only that it speaks it audibly for everyone to hear. Which is another thing; if my sensitive data is*

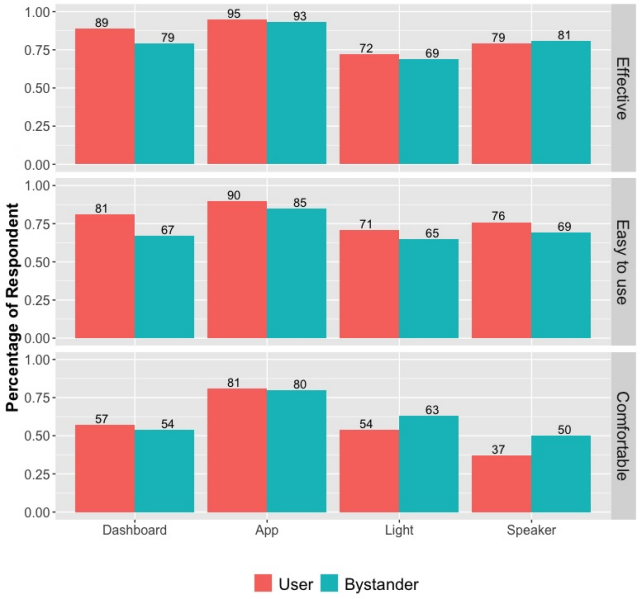

Figure 5: Percentages of users and bystanders who either "agree" or "somewhat agree" of a notification mechanism's perceived effectiveness, perceived ease to use, and their comfortableness of using it. The four mechanisms include (left to right): Data Dashboard, Mobility App, Ambient Light, and Privacy Speaker.

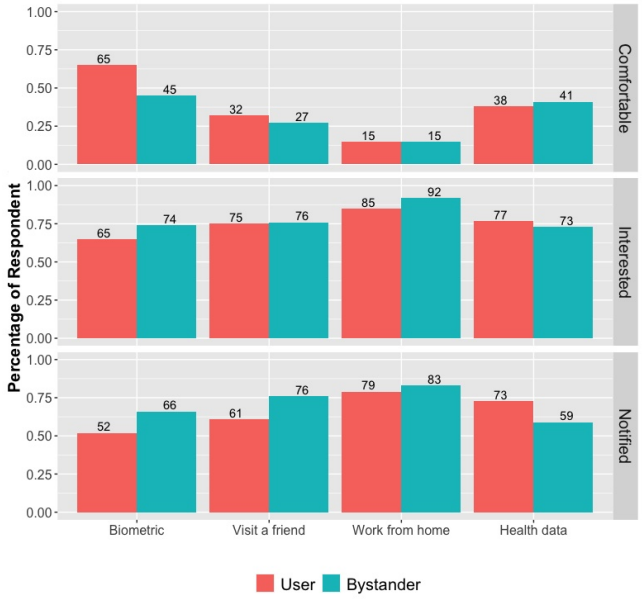

Figure 6: Percentages of users and bystanders who are comfortable using smart home devices, would like to learn about the data practices and would like to receive privacy-related notifications in each scenario. The four scenarios include (left to right): Biometric Security, Visiting a Friend, Working from Home, and Health Data Track

being collected I might feel embarrassed and not want everyone in the room to know." (U5)

Con: voice goes off very quickly (bystanders). When bystanders (n=7) were in other people's homes, the voice reminders could go off very quickly before they are able to capture the information. Some bystanders also mentioned that the Privacy Speaker could start talking when they were in the middle of a conversation or doing leisure activities. In those cases, as B87 further explained below, the voice reminder would not be useful. *"I think an audio reminder of the data information would be easily forgotten and potentially annoying if it is going off instead of an alert on a device. I don't think I would continue to listen to this device depending on the frequency of the alerts." (B87)*

Con: cause more anxiety (bystanders) The last concern mostly shared by bystanders (n=4) was the possibility of more anxiety. This is because, when they heard a voice message about their data being collected, they most likely were not able to take any immediate actions or investigate the case in detail. As a result, rather than alleviating their privacy concerns, the voice reminders only increased their anxiety. As B102 noted below, in such cases, he would be very anxious to receive privacy-related notifications through the speaker. *"In this situation, I do not know what the consequences are of having my data shared and privacy invaded. While I appreciate the notification, I think it would stir more anxiety in me regarding others' access rather than motivate me to do something since, as I said, I don't know what to do. Though I know that 'ignorance is bliss' is maybe not the best stance." (B102)*

4.3 Scenario-based questions

Next, we present the findings from the scenario-based questions. In the survey, we presented four scenarios to all participants and asked them to answer the following four questions from both users' and bystanders' versions: 1) whether they are comfortable of using smart home devices in the scenario; 2) whether they are interested in learning about the data practices of surrounding devices in the scenario; 3) whether they are interested in receiving notifications regarding the data practices, and 4) which mechanisms they would like to use in the scenario and why. All participants chose their more preferred individual notification mechanisms and many of them also selected multiple mechanisms together.

In this section, we first present a summary of the data from the above questions for each scenario, including the quantitative data and qualitative data. Then, we compare the data from each scenario and discuss the insights and takeaway messages. Our results suggest that the Mobility App is consistently recognized as the most preferred mechanism across all four scenarios. Despite that, the choice of other notification mechanisms varied across different scenarios. Our results highlight participants' contextual preferences in receiving privacy-related notifications.

4.3.1 Summary of Participants' Notification Preferences. Figure 6 shows a summary of the percentages of participants' perceived comfortableness of using smart home devices, interests in learning about data practices, and willingness to receive privacy-related notifications in each scenario.

Scenario 1: Biometrics Security. In this scenario, 65.4% users and 44.7% bystanders were comfortable using/being around smart home devices. 65.4% users and 74.0% bystanders were interested in learning about the data practices, while 52.2% users and 65.9% bystanders are interested in receiving notifications regarding the data practices of the smart home devices.

Scenario 2: Visiting a Friend. In this scenario, 31.6% users and 26.8% bystanders were comfortable using/being around smart home devices. 75.0% users and 75.6% bystanders were interested in learning about the data practices while 61.0% users and 66.7% bystanders were actually interested in receiving notifications.

Scenario 3: Work from Home. In the Working from Home scenario, both users and bystanders were considerably less comfortable using/being around smart home devices. Only 15.2% users and 15.4% bystanders reported being comfortable. As a result, 85.2% users and 91.9% bystanders were interested in learning the data practices, and 79.4% users and 82.9% bystanders were interested in receiving notifications. These percentages remain the highest across all four scenarios, indicating a higher level of privacy concerns for both users and bystanders.

Scenario 4: Health Data Tracking. In the Health Data Tracking scenario, 38.2% users and 40.4% bystanders were comfortable using/being around smart home devices. 76.5% users and 73.1% bystanders were interested in learning about the data practices, and 72.8% users and 58.5% bystanders would like to receive notifications.

4.3.2 Summary of Participants' Notification Mechanisms Choices. Figure 7 shows a summary of the percentages of participants' choices of notification mechanisms under four scenarios. Based on the graph, we were able to draw four conclusions.

Mobility App is the most popular choice across all scenarios. With that being said, the reasons why the Mobility App remains the most popular choice differ between users and bystanders. For example, in the Health Data Tracking scenario, being able to easily access detailed data practices of smart devices through an app on their phones boosts the convenience factor for users. However, several bystanders mentioned that the Mobility App, aside from the convenience factor, also provides them more agency in being aware of and controlling their own data.

Data Dashboard is the second most popular choice across the four scenarios. However, bystanders' choice of Data Dashboard varied between Visiting A Friend scenario and Work from Home scenario. The key impacting factor here, as noted by many bystanders in the qualitative responses, is the social norms embedded in the scenario. In the Work from Home scenario, bystanders believed that since they were dealing with their immediate family members, they would be more comfortable with using the Data Dashboard. In the Visiting a friend scenario, bystanders felt more obligated to follow the embedded social norm and not to be rude, thus less inclined to use the Data Dashboard.

Ambient Light and Privacy Speaker are more preferable in the Visiting a Friend scenario and Work from Home scenario. As participants explained in the open-ended responses, aside from the convenience factors, another critical consideration is to have an unobtrusive mechanism for notification delivery so that they would not be distracted from their activities with friends (n=10) or their work (n=5).

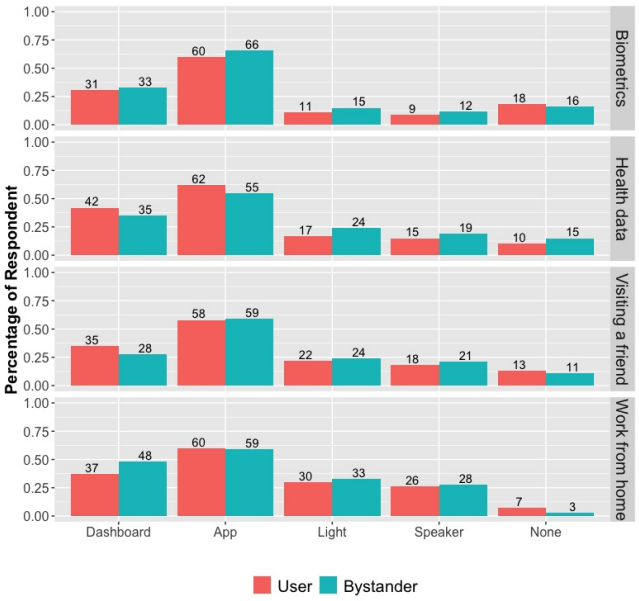

Figure 7: Summary of users' and bystanders' selection of notification mechanisms in each scenario.

Many participants selected the "None" option, indicating that they prefer not to receive any notifications. Similarly, users and bystanders have different rationales. For example, in the Biometric Security scenario, for users who selected none, the main reason (n=17) is they just did want to receive any notification or they did not care about the data collection. On the contrary, bystanders indicated a few reasons. One notable reason (n=10) is the fact that these notification mechanisms can potentially invade the users' privacy. B35 selects "none" and comments, *"The apps would be less interruptive than the other three. However, I would even lean towards "none" on the grounds that this scenario involves my friend's privacy more than my own."* In this example, this bystander considers the impact of the notification mechanisms on his friends and decides not to receive any notification, even though he expresses interest in the prior questions. Another reason (n=4) is bystanders' perceived lack of control. Simply receiving the notification of data practices without the ability to take measures (since they do not own the devices as bystanders) can adversely increase their psychological burden. As an alternative, they refuse to receive any notifications.

5 DISCUSSION

Our results reveal the pros and cons of the four notifications mechanisms in smart homes from both users' and bystanders' perspectives. In addition, our results also highlight the different rationales why users and bystanders select certain notification mechanisms in four hypothetical scenarios. In this section, we discuss the key lesson learned from the study and present implications for designing future privacy awareness mechanisms in smart homes.

5.1 Similarities and differences between users and bystanders

Literature on smart home privacy consistently suggests two main points, i.e., bystanders do have privacy concerns in smart homes, but they often have mismatched privacy expectations compared to those of the users [1, 13, 27, 41, 42]. For example, users tend to prioritize device utility over privacy protection, while bystanders tend to consider many social factors (e.g., social relationship, power dynamics) when they seek privacy protections in other people's homes [37, 42]. In this paper, some of our results echo the mismatches between users and bystanders as shown in the literature, while other findings present a new paradigm when delivering privacy awareness to users and bystanders in smart homes.

Similarities between users and bystanders. Our results show that the users and bystanders share many similar expectations for privacy awareness. One notable is example is that both users and bystanders, in general, prefer to have detailed information about data practices of surrounding smart home devices. Another notable example touches on the usability of the privacy awareness mechanisms, which includes whether they are convenient to access the notification, how much effort is involved in understanding the information, and whether privacy-related notifications are interruptive. In addition, both users and bystanders would prefer being able to take actions beyond solely being aware of the data practices. Failing to do so may result in a sense of helplessness for the users and generate psychological burden and anxiety for bystanders.

Mismatches between users and bystanders. Noticeably, there are also several mismatches between users and bystanders regarding their preferences of privacy awareness mechanisms. First, while users mostly considered the usability of these mechanisms, bystanders pay considerable attention to maintaining the social norms in users' homes. For example, as suggested in Section 3, bystanders tend to consider whether a particular mechanism can maintain the widely acknowledged social norms, reduce the potential social confrontation, and avoid certain social awkwardness. These considerations further indicate that privacy awareness mechanisms should be socially acceptable by both users and bystanders. Another notable mismatch concerns the users' privacy and security. Even though some bystanders in our study showed their considerations of users' privacy and refused to use mechanisms that may invade users' privacy, most bystanders did not take this into consideration. Ideally, privacy awareness mechanisms should not sacrifice users' privacy to meet the needs of bystanders. Additionally, when discussing the Mobility App, some users believed that the app might open doors for hacking, causing security issues to their home and their data. No bystander in our dataset mentioned a similar security concern, which further indicates the mismatches between users and bystanders.

5.2 Key Design Dimensions of Privacy Awareness Mechanisms in Smart Homes

Based on our findings, we summarize the following key design dimensions for future privacy awareness mechanisms in smart homes. We hope that these dimensions can be used as a design guideline for researchers and practitioners who work on new designs and systems to improve people's awareness of the data practices of surrounding smart home devices.

Easy access. Privacy awareness mechanisms should be easily accessed by both users and bystanders. Existing ways to convey privacy-related information in smart homes (e.g., device privacy policies, data recording history) are mostly designed for users to understand the data practices of their smart home devices. When bystanders are involved in the data collection, there is no easy way for them to learn about the data practices, especially when bystanders do not have prior knowledge or experiences of smart home devices. One concrete idea is to have a bystander mode. For example, if the Mobility App has a bystander mode, when bystanders are present, they should only be able to view any data that are related to them, not the users.

Unobtrusive modality. Researchers and practitioners may also explore possibilities for other unobtrusive modalities to raise privacy awareness. Our findings suggest that in some situations (e.g., work from home, friends visiting), people may prefer unobtrusive notifications to avoid any interruption in their current activities. The Ambient Light and the Privacy speakers in our study are examples of such unobtrusive mechanisms. However, given the connectivity of the Internet of Things, it is possible to have other modalities that take advantage of sensors and features in the "Things". For example, the haptic engine in some devices can be another possible modality for sending unobtrusive notifications, but future research is needed to further unpack the design opportunities.

Privacy awareness at the smart home level. Participants in our study appraised the Data Dashboard and the Mobility App since they provided a centralized place for them to know the data practices of all surrounding smart home devices. However, most existing privacy awareness mechanisms in smart homes (e.g., privacy policies) are only concerned with individual devices (except when several devices are made by the same manufacturer). Future mechanisms should consider delivering privacy-related notifications from the smart home level rather than individual devices level.

Enabling privacy controls along with raising awareness. Both users and bystanders in our study indicate their need to go beyond the privacy notifications and have some control of their data when they are more aware of their privacy situations. This is particularly important for bystanders, as bystanders are generally in a disadvantaged position to take actions to protect their privacy when they do not have access to the devices as the users do. Feng et al. argued that in the context of IoT, the relationship between privacy notices and choices can be decoupled (i.e., a system does not provide users notice and choice at the same time), integrated (i.e., a system provides users notice and choices together or sequentially), or mediated (i.e., privacy notice and choice are mediated by privacy-enhancing technologies) [15]. Our results suggest that participants, especially bystanders, prefer to have privacy notices integrated with privacy choices so that they can take action when they have privacy concerns.

5.3 Limitations and Future Work

Our study has the following limitations. First, our sample is skewed towards the female and younger population. This is likely due to a recent incident on TikTok which influenced the gender balance

on Prolific [8]. However, the purpose of this study is to investigate users' and bystanders' reactions to the four privacy awareness mechanisms and explore the design opportunities. We do not claim any generalizability of our results. Thus, we believe our results are still valid. Future research can continue the research from a representative sample.

Second, we only explored four individual privacy awareness mechanisms. Although by no means comprehensive, we chose these four mechanisms to provide a broad coverage along the following axes: interactive vs passive use; visual vs audio; and detailed vs brief. We omitted other possibilities or a combination of different mechanisms (e.g., a privacy speaker with built-in ambient light). Future research can continue to explore more mechanisms or leverage existing devices (e.g., ambient lights on TVs).

Similarly, the four scenarios cover a range of locations (i.e., my home vs someone else's home), data sensitivity (i.e., health vs non-health), human activities (i.e., work vs non-work), and different types of bystanders (i.e., roommates, friends, and spouses). Again, by no means are these scenarios exhaustive, but we hope that our results, based on the four mechanisms and the four scenarios, provide a starting point to qualitatively explore privacy notices under a wide variety of conditions. Future research can further quantitatively examine how these factors impact people's preferences of privacy awareness mechanisms.

Third, due to the technological complexity and difficulty, we choose to describe the privacy awareness mechanisms through text and images rather than having the participant interact with the prototypes. We also situated our participants in hypothetical scenarios rather than real-world scenarios and only collected self-reported data. Future research can provide interactive prototypes for participants to experience and potentially run experiments in real-world contexts through field studies.

Lastly, our study only focuses on mechanisms that are used to improve users' and bystanders' awareness and does not touch on their expected controls. Future research can further investigate how users and bystanders would like to control their privacy after being aware of the situation.

6 CONCLUSION

One effective way to combat the opaque data practices in smart homes and increase smart home users' and bystanders' awareness is through privacy notices. However, how to deliver effective privacy notices to users and bystanders remains understudied. In this study, we surveyed 136 smart home users and 123 smart home bystanders to understand their preferences for receiving privacy notices in smart homes, their perceptions of four privacy notice mechanisms, as well as their choice of mechanisms in different scenarios. Our results revealed factors that influence users' and bystanders' perceptions of each privacy notice mechanism, i.e., social awkwardness, and highlighted the similarities and mismatches in their perceptions. We summarized four key design dimensions for researchers and practitioners to consider when designing future privacy notice mechanisms.

7 ACKNOWLEDGEMENT

We thank all the anonymous reviewers for their valuable feedback.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[2] Noah Apthorpe, Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan, and Nick Feamster. 2019. Keeping the smart home private with smart (er) iot traffic shaping. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019).

[3] National Archives and Records Administration. 2012. We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online. https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

[4] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. 2014. Is your inseam a biometric? a case study on the role of usability studies in developing public policy. *Proc. USEC* 14 (2014).

[5] Natã Miccael Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. " What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proc. Priv. Enhancing Technol.* 2019, 4 (2019), 211–231.

[6] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 20)*.

[7] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. sage.

[8] Nick Charalambides. 2021. We recently went viral on TikTok - here's what we learned. https://blog.prolific.co/we-recently-went-viral-on-tiktok-heres-what-we-learned/

[9] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A Kientz. 2011. Living in a glass house: a survey of private moments in the home. In *Proceedings of the 13th international conference on Ubiquitous computing*. 41–44.

[10] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[11] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[12] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)* 13, 2 (2006), 135–178.

[13] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J Wisniewski. 2020. Exploring Smart Home Device Use by Airbnb Hosts. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.

[14] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.

[15] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–16.

[16] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[17] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. 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), 1–21.

[18] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. 471–478.

[19] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. 1573–1582.

[20] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3393–3402.

[21] Marc Langheinrich. 2002. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing*. Springer, 237–245.

[22] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–31.

[23] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the US. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK*.

[24] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019).

[25] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 436–458.

[26] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*. 83–95.

[27] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. " I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 1–11.

[28] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[29] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 399–412.

[30] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[31] Helen Nissenbaum. 2011. A contextual approach to privacy online. *Daedalus* 140, 4 (2011), 32–48.

[32] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView–Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[33] Joseph Reagle and Lorrie Faith Cranor. 1999. The platform for privacy preferences. *Commun. ACM* 42, 2 (1999), 48–55.

[34] Joel R Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia McDonald, Thomas B Norton, and Rohan Ramanath. 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Tech. LJ* 30 (2015), 39.

[35] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* (2017).

[36] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 1–17.

[37] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart home beyond the home: A case for community-based access control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[38] National Telecommunications and Information Administration. 2013. Privacy Multistakeholder Process: Mobile Application Transparency. https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

[39] National Telecommunications and Information Administration. 2016. Privacy Multistakeholder Process: Facial Recognition Technology. https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology

[40] Yaxing Yao. 2019. Designing for Better Privacy Awareness in Smart Homes. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 98–101. https://doi.org/10.1145/3311957.3361863

[41] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*. 1–12.

[42] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[43] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 6777–6788.

[44] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security ({SOUPS} 2017)*. 65–80.

[45] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.