Identifying Older Adults' Expectations of Privacy-Preserving Controls for Smart Home Devices

Chola Chhetri
George Mason University
Fairfax, VA 22030, USA
cchhetri@gmu.edu

Vivian Motti
George Mason University
Fairfax, VA 22030, USA
vmotti@gmu.edu

CSCW 2019 Workshop on Networked Privacy, "Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms", November 9, 2019, Austin, TX, USA.

Abstract

Privacy controls in smart home devices are largely lacking. To identify what privacy controls users need, we conducted a focus group study with 5 older adults. To understand the study participants' expectations of privacy controls in smart home devices, we analyzed the responses of the study participants. This paper reports the results of the study, including the design expectations that the study participants have. Participants expected smart home devices that provide privacy controls. In addition to limited sharing of information, the devices should be designed for visibility and anonymity. Lastly, a verification mechanism for privacy controls should be made available.

Author Keywords

Privacy; control; smart home devices; design; user studies.

ACM Classification Keywords

H.5.2.q User-centered design; D.4.6 Security and Privacy Protection; K.4.1.f Privacy.

Introduction

Smart home is a growing application in the Internet of Things (IoT) domain. In 2019, the estimated smart home adoption rate in the US was about 33.2%. Studies suggest it will exceed 53% by 2023 [10].

Smart home devices (SHDs) are characterized by devices used at home. Such devices are often connected to the Internet either directly or through a hub (centralized controlling device) and allow user control through a mobile application. The most common smart home devices include: televisions, door locks, doorbells, thermostats, and speakers (also known as intelligent personal assistants or IPAs), such as Google Home and Amazon Echo.

Thanks to the sensors embedded, SHDs are able to collect a large amount of data from users. Therefore, these devices have the potential to cause a number of privacy violations and data misuse, which include but are not limited to: inferring occupancy information, location information, and user activity information. Given these threats, SHDs raise privacy concerns in users. To address these concerns and minimize privacy risks, there is a growing need to develop privacy controls from a user-centric perspective [1,2].

A user-centric development approach includes users front and center in the implementation, first to understand their specific requirements and expectations and then to tackle the design of privacy controls in SHDs considering users' feedback and evaluation iteratively. To employ a user-centric approach in the design and development of privacy controls for smart home devices, the research study was driven by the following research question:

RQ1. What privacy controls SHD users, especially older adults, want in SHDs?

To answer this research question, we conducted a focus group. To study privacy controls for smart home devices we recruited older adults as research participants. Older adults are often overlooked in scientific research with user studies [8], however they have a higher potential to benefit from SHD usage [7]. We conducted one focus group involving 5 adults older than 62 years old. This paper presents the research findings about what participants want of privacy controls.

Background

Manufacturers, such as Samsung, Google and Amazon, often develop SHDs targeted towards older adults [7] because SHDs can serve as digital companions and assist in activities. However, older adults are known to have more privacy concerns when compared to a younger user population [4]. Even though older adults are more vulnerable to privacy risks as compared to other populations, they are less often included in user studies concerning the design and development of privacy controls [8].

Yao et al. (2019) conducted a participatory design study with 12 users, 7 interested users, and 6 non-users. They identified six factors to enhance the design of privacy controls for smart homes: data transparency and control, security, safety, usability, system intelligence, and modality [9]. This study provides a preliminary ground work to devise user-centric privacy controls for SHDs. However, it does not focus on older adults, hence additional user studies involving older adults are needed, not only due to the promising potential for ambient assisted living with SHDs, but also due to the growth of the aging population and lack of design guidelines.

The lack of privacy controls has been identified as an important barrier in the adoption of SHDs [5,6]. Some solutions have been developed in this regard. For example, Emami-Naeini et al. (2019) proposed prototype privacy labels to help users to integrate privacy into their IoT device purchase decisions [3]. More studies aimed at designing SHD privacy controls are necessary to meet user expectations.

Methods

To investigate the expectations that older adults have concerning privacy controls for SHDs, we conducted a focus group involving five older adults, who used smart home devices. Table 1 summarizes the demographic profile of the 5 study participants. The study protocol included prompts to discuss the rationale behind the use of smart home devices, privacy concerns regarding the use of smart home devices, and privacy controls in smart home devices. The Institutional Review Board of the university approved the study prior to data collection.

We recruited participants through purposeful sampling. In practice, we recruited participants from the Apple Pi: a group of older adults from the community (Northern Virginia) who meet in a regular basis to discuss technology-related topics. We announced our study using an IRB-approved verbal script. We advertised it as a SHD-related study. We audio-recorded the discussion for transcription. The study lasted about one hour and took place after the participants attended a privacy talk. The talk was open to the community (Apple Pi) and it took place at the university.

Results

Participants owned an average of 5 smart home devices. Examples of SHDs that participants owned are: Amazon Echo, WeMo switch, Ring doorbell, televisions, and lights. The age of the study participants ranged from 62 to 84 years old, average age was 74.6 years (SD = 8.08). Among the focus group participants, 4 were male and 1 was female (Table 1).

	Gender	Age	SHDs
P1*	Male	77	Echo, TV
P2	Male	73	Thermostat, TV
P3	Male	84	Echo dot, Home, doorbell, TV
P4*	Female	77	Thermostat, TV, light, switch
P5	Male	62	Echo, switch, TV, Homepod

Table 1: Participant Information. Asterisk (*) next to P1 and P4 denotes that these participants reported having a technology background (i.e. academic major was related to technology).

Expectations of Privacy Controls (RQ1)

We prompted participants for SHD-related concerns. We let the participants bring specific concerns to the discussion. Participants brought up privacy concerns without prompting. All participants had privacy concerns from SHDs and stated they would like some privacy controls in the SHDs.

More specifically, the most commonly desired privacy control was default-off configuration for access and sharing of data in SHD apps. Participants stated they preferred options to turn off sharing and access to contacts, locations, microphone, and recording device by default. They suggested there should be also be an option to allow users to turn on sharing and access when so desired. One participant suggested that the smart home app should begin with a clear message about what data the app will keep and what it will share:

*"App starts with 'I won't keep or share your contacts, location, audio, and video'. This would elevate privacy to users and encourage sensitivity to privacy intrusion." (*P1, male, owner of IPA and TV*)*

Another privacy control was a clear, convenient and visible mechanism to turn SHDs on and off. Participants said SHDs should provide visible, easy-to-recognize power switches for convenient on/off functionality. One participant said he would like the device to provide a reaffirmation that the device is off when turned off:

*"An easy way to turn devices on/off without having to enter a password. I would like to see some clear, redundant indication that device is off when set to off." (*P2, male, owner of thermostat and TV*)*

Another privacy control expected by participants was a mechanism that showed the device is actively operating, or recording audio and video. One example of such indicator would be an LED light:

*"A way to know, even with an LED light, whether a device is actively looking/listening." (*P3, male, owner of IPA, doorbell and TV*)*

Participants were mainly against unessential universal data collection. One participant specified that he did not want any data collection and recording of audio in his home. Other participants recognized that some data collection may be necessary for device operation, functionality, personalization, and other features. In such cases, they expected that data be deleted after the intended action/purpose and that control be provided to users as well. Another expectation was that data should not be tied to personal information such as name and address. Three design expectations of privacy controls in this context were choice of data collection, choice of deletion and anonymity of data. For example, as P3 stated:

*"An assurance, or choice, of data that is collected/recorded is not kept—that it is routinely and systematically deleted". (*P3, male, owner of IPA, doorbell and TV*)*

Participants also discussed the need for an infrastructure for verification of privacy controls in SHDs. An agency or organization that verifies privacy controls that a device maker claims to have on a SHD. This agency can be a third-party organization that has the capability to verify privacy controls in SHDs. Third-party verification may be a good source of trust or assurance for SHD users and can help users compare privacy controls among multiple SHDs while deciding which SHD meets their privacy expectations.

Conclusion

This focus group was a part of a larger research project aimed at investigating what end users want in the design of privacy controls in smart home devices. In the focus group, we identified some SHD privacy control requirements from a small sample of 5 older adults. Participants of the focus group wanted privacy controls in SHDs. The controls include: default-off configuration for data access and sharing, visible power switch, visible activity indicator, absent or limited data collection, anonymity, and an agency for verification of privacy controls.

The findings from the focus group inform the design of privacy controls for SHDs. Manufacturers should further explore and incorporate trust and verification of SHD privacy controls.

In future work, we will expand the research including other populations, such as young adults. We will also use other user-centric methods, such as interviews, to complement the findings from the focus group.

Acknowledgements

This research was funded by 4-VA. We thank them for their support. Any opinion, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of our research sponsor. We would also like to express our gratitude to the study participants who voluntarily joined the focus group and the anonymous reviewers for their feedback.

References

1. Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2016. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *Data and Algorithmic Transparency Workshop (DAT)*.
2. Chola Chhetri and Vivian Genaro Motti. 2019. Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. In N.G. Taylor, C. Christian-Lamb, M.H. Martin, and B. Nardi, eds., *Information in Contemporary Society, Proceedings of iConference, LNCS 11420*. Springer Nature, Switzerland AG, 1–11.
3. Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, 534:1--534:12.
4. Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow. 2010. *How Different Are Young Adults From Older Adults When It Comes to Information Privacy Attitudes & Policies?* .
5. A Jacobsson and P Davidsson. 2015. Towards a model of privacy and security for smart homes. *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 727–732.
6. S A Kumar, T Vealey, and H Srivastava. 2016. Security in Internet of Things: Challenges, Solutions and Future Directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772–5781.
7. Xinru Page, Paritosh Bahirat, Muhammad I Safi, Bart P Knijnenburg, and Pamela Wisniewski. 2018. The Internet of What?: Understanding Differences in Perceptions and Adoption for the Internet of Things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4: 183:1--183:22.
8. Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. *Proceedings of the 2017 New Security Paradigms Workshop*, ACM, 122–130.
9. Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ACM, 198:1--198:12.
10. 2019. Smart Home - United States. *Statista*. Retrieved February 1, 2019 from https://www.statista.com/outlook/279/109/smart-home/united-states.