Mozilla Iot Class Project. Draft #1

Rajib Dey
University of Central Florida
Orlando, Florida, USA
rajib@cs.ucf.edu

Sayma Sultana
University of Central Florida
Orlando, Florida, USA
sayma@knights.ucf.edu

Dr. Pamela Wisniewski
University of Central Florida
Orlando, Florida, USA
e-mail address

ABSTRACT

As the internet becomes more ubiquitous, it contributes to burgeon the use of sharing economy. In this paper, we are mostly interested in sharing of properties, where the user most of the time if not all the time shares their house with complete strangers through the internet. As they are sharing (with) and using smart home devices (light, door lock, sensors, security cameras etc) that can be controlled by strangers, it creates a security and privacy risk for the guest and the host of the sharing economy. As there is a lack of understanding about what kind of access control is needed in this kind of setting, in this paper, we aim to explore the perspectives of both the guests and the owners of houses in a sharing economy regarding the shared use of smart devices in the property. We will conduct interview with 10 guests and owners of such property to understand present situation and demand of both the owners and the guests of these houses with smart home devices. This research will allow us to give recommendations for future application developers and smart home device manufacturers who are interested in designing applications and devices for such scenarios.

Author Keywords

Security and Privacy; AirBnB; Sharing Economy; Access control; Smart Home Devices; Internet of Things.

CCS Concepts

•**Human-centered computing** → **Human computer interaction (HCI);** *Haptic devices;* User studies; Please use the 2012 Classifiers and see this link to embed them in the text: https://dl.acm.org/ccs/ccs_flat.cfm

INTRODUCTION

The increasing amount of internet use is enabling users to monetize different kinds of (mostly underutilized) properties they own by sharing. This act of sharing is often termed as "Sharing Economy" and it is getting very popular day by day [1]. In a sharing economy, users share their car (Turo[2]), home (AirBnB[3], vrbo[4], homeaway[5], flipkey[6]), storage space(Vertoe[7]), etc with other users from the internet.

CHI'20, April 25–30, 2020, Honolulu, HI, USA

ISBN 978-1-4503-6708-0/20/04…$15.00

DOI: https://doi.org/10.1145/3313831.XXXXXXX

According to one of the most popular property sharing site airbnb's (which is only 12 years old) press release, it has more than 7 million listings worldwide, covering more than 100 thousand cities in 191 countries [8].

To manage these properties securely and efficiently the home owners are installing smart home devices like smart door lock, monitoring camera, smart lights etc on their property. According to International Data Corporation (IDC), almost 833 million smart home devices have been shipped globally just this year alone [9]. Some manufacturers are even developing products just for this use case [10].

When these smart home devices are installed in the property and guest(s) rents that property, they share these devices during their stay. Most of the time if not all the time, this sharing happens with complete strangers. This creates a security and privacy risk for smart home users who are participating in the sharing economy. As the owners are sharing their smart home devices (light, door lock, sensors, security cameras etc) with strangers, there is a growing sense of fear for the loss of information and physical privacy among them[11].

It is true for the other way also. As the guests of these houses with smart devices are also using products that are owned and controlled (most of the time) by the owners who are most likely to be a stranger, the feeling of their data being misused is mutual. To make this work, they kind of have to trust each other with their information and physical privacy. What makes this trust-building exercise tougher is that the owner and the guest can have varied needs and concerns out of those devices.

Unfortunately, smart home device manufacturers and app developers are not serious about these varied requirements from different users in a multi-user scenario. Most of these devices are designed just like a personal device[12]. Where to give someone else access to the device you will have to share your login credentials with them. You have to either share the device entirely or can not share it at all. There is no granular control of the sharing of access. Researchers have found the need for supplementary access control options in these devices [12]. In another research paper [13], Zeng et al. found that smart home devices lack transparency and privacy features. But unfortunately, most of the commercially available smart home devices provide elementary controls for security and privacy. While some systems do not provide any control at all[14].

This lack of transparent access control might work well in a close trusted group of people (i.e family members, partners, close friend etc), where there is mutual trust between the users

and they kind of know from their social interaction that the other person(s) will not use the device and related data in any way to harm or disturb anyone else. But this does not bode well among conflicting user groups. Such as smart home device users in a sharing economy (i.e airbnb), who are complete strangers. For example: a guest might not like the fact that he is being recorded by a camera outside his room. Even though AirBnB has rules for all kinds of recording devices including security cameras [15], the guest might not trust the owner with the data that he is collecting through smart home devices. On the other hand, the owner might not trust the guest with his own smart home devices. This trust can be built easily by the proper implementation of a transparent sharing access control of these devices [16].

In this paper, we aim to explore the perspectives of both the guests and the owners of houses in a sharing economy regarding the shared use of smart devices in the property. We hope to present the results of the initial survey and the interview. From this survey and interview we will be able to understand the needs of both the owners and the guests of these houses with smart home devices. This research will give us the opportunity to give recommendations for future app developers and smart home device manufacturers who are interested in designing applications and devices for such scenarios. Our research questions are:

- RQ1: Which smart home IoT devices do the users of sharing economy are currently sharing and want to share with others (from the perspective of hosts) or want to be shared with them (from the perspectives of guests) in future?
- RQ2: How and why smart home devices are being currently shared in a sharing economy (airbnb, homeaway etc)?
- RQ3: What kind of security and privacy issues the guests and the hosts are currently facing or think they will face while sharing smart homes?
- RQ4: What specific (degree of) granular access control do hosts and guests want while sharing?

With this research work, we hope to have the following contributions

- We aim at synthesizing the current scenario of sharing smart homes in share economies. Which will help us identify what kind of access control settings is needed and for which device in a sharing economy.
- As all of the sharing economy participatory companies have to go through some sort of government approval, we wish to provide recommendation for lawmakers on privacy and security issues that need to be taken care of at the government and the policy level. So that the users can feel more at ease and boost the use of this kind of infrastructure.
- After the interviews with the guests and the hosts, we hope to develop a concise perception of their demand on controlling access for guests and security concerns. Through user study we hope to provide recommendations for access-control module for guests in sharing economy so that future apps and devices can be designed with user-friendly, secure, privacy-preserving and granular access control. We also provide scope for more discussions for designers and researchers.

RELATED WORK

At first, we discuss research work that explores smart-home access control issues. Then we discuss security and privacy issues in a close-trusted circle and among users with conflicting agendas.

Smart-Home access control

Smart devices have so many use cases that it should have been already in each and every household by now. Even though it is estimated to reach the global market value of more than 7 Trillion dollars [17], it has failed to be ubiquitous so far. Reasons for this failure include security and privacy concerns among users and shoddy management systems [18]. Although researchers [19] have shown that the cost of hardware is not an issue when implementing security and privacy for IoT devices, it seems that device manufacturers are rushing to release IoT devices to market. Which is causing those devices to have security and privacy issues for the end-users. These issues include being eavesdropped, losing control of the devices in question, loss of private data, etc [20].

As a result, in a recent action taken against Google [21] by German regulators, they have banned Google from listening to Google home [22] devices for a limited amount of time throughout Europe [23] fearing the data might be misused by them. Other researchers [24] found that control systems can be so complicated that the end-user sensed that they have less control over their devices. Page et al [25] discuss that IoT devices that are designed for the consumers tend to follow an agentic technology viewpoint, where the user-centric viewpoint takes a backseat. To make matter worse, other research [26] shows that apps (i.e SmartThings by Samsung) controlling the IoT devices can have more access than necessary, making the devices insecure. This can be exploited to steal key security information (i.e Door lock codes), disable some security features and even make false fire alarm. These apps can accumulate additional and unnecessary access just by asking users for more permissions [27]. It's been found that users tend not to pay much heed to these requests for more permissions, they just accept them [28].

Fernandes et al. [26] along with others [29] [30] have proposed limiting and reconsidering permission granted to those apps to solve this problem. Researchers interviewed 20 people who do not yet use smart home devices to understand the user's need for proper access control policies [31] [32]. According to these interviewees, the capability of requesting permissions to be approved or denied, proper logging of devices and physical presence are useful criteria for a well-designed access-control policy.

Security and privacy in a close trusted-circle

He et al. discussed how sharing of IoT devices inside a home occurs among relationships and how they differ based on time of the day, scenarios, location of the device, etc. They also

discussed ways to authenticate users so that the IoT devices stay secure while upholding the usability of the device [12]. This work, however, does not discuss sharing IoT devices with people living outside of their homes or with people the owner does not trust.

Previous research [33] finds that even if the IoT system is designed to share in between users, the kind of access control it has is very much different from the kind of access control the user has in his/her mind. They also show that most of the time the user needs a complex access control policy and they try to achieve that by using makeshift methods. For domestic IoT devices, the access control decisions are especially complex because of the varied amount of data and the kind of trust users have between themselves [34].Kostianinen et al. [35], tried to introduce an access control policy for smart home networks limited to family members which would pose a nominal amount of burden on the end-user by testing a few access control policies.

Security and privacy between conflicting user groups

Researchers find that giving guests access to your IoT device in a smart home and being specific with policies regarding the shared devices are important but can be a complex task [36] [35]. Few research studies [37] [13] show that the multi-user scenario can be perceived as a privacy and security concern to users. This concern exists because of the social relationships between the users and they can vary depending on the relationships such as guests [36], roommates [34], and children [20] [38]. Microsoft research [39] found that even when sharing IoT devices and sensors among neighbors can help increase the security of the neighborhood, the level of trust they have between themselves can interfere with this sharing. Providing users the information about the data being monitored by the sensors in a smart-home setting can help pacify the privacy concern and strengthen the trust they have, but at the same time it is perceived as being burdensome [40].

An empirical study on 15 families done by Microsoft research [41] reveals that family members trust each other while keeping separate profiles on IoT devices. One of the reasons they do this is to block strangers with malicious intent. This is why it is highly desirable among users to have access-control policies based on time (for guests), special preventive measures for highly sensitive devices like cameras and locks, limiting of application's access to devices. [42]

Another research work by Microsoft [43] found that the access control system of popular IoT devices (that are used in Sharing economy), like the Kwikset door lock and Philips Hue lighting system is so isolated that it is useless in simple use cases where the user wants to share the devices with other users like the guest of the property temporarily. There is also a trust deficit for the smart home devices, because when the user is away from home, the access control of the home IoT devices has to be trustworthy enough to operate on their own [44]. This plays a major factor in deciding which smart home device to use while sharing the property with strangers.

METHOD

We will use two methods - online survey and Interview, for the user study. For this purpose, We will recruit sharing economy hosts and guests who have already used or want to use IoT devices from different states of the country. At first, we will conduct a survey among sharing economy hosts and guests and select a subset of participants based on experience and interest in using IoT appliances at home. Then we will collect qualitative data about participant's experience and demand on sharing IoT devices through follow up interviews. We expect to have at least 10 participants (including hosts and guests of sharing economy) for interviews. Survey and interview questions will be updated in supplemental Data.

Recruitment

To recruit participants for the online study we will gather contact information of hosts and guest-users of different sharing economies like Airbnb, Vrbo, HomeAway, FlipKey from these websites and contact them through email, website, ads on IoT related forums and social media posts. We aim at contacting at least a total of 150+ hosts who are involved in renting their houses or rooms and guests who have experience in taking rent of houses through sharing economy sites. Then, we will introduce our study to them and call to participate in an online survey. We want to include people with variable household, ethnic background, and age to get a clear snapshot of our intended study. We will need 5-6 days to contact the intended number of people and arrange them for a preliminary survey. Hopefully, we will be able to find at least 15 hosts and 15 guests interested in an online survey.

Online Survey

Our target population for the online survey is the hosts and guests of the sharing economy who will agree and give consent to participate in our study. The initial survey intends to select potential interviewees who can give us more insight into smart home-sharing situations with people only known through the sharing economy platform. We will send an invitation to participate in our study through email. Through this survey, we will also have an idea of the present scenario of sharing smart home IoT devices from both the perspective of hosts and guests. Participants will also be asked about their interests and requirements to share those devices in the future. We have designed a survey consists of 52 questions that will need at most 15 minutes to complete.

Follow up Interview

After the online survey, we will select a few participants based on their response and interest in sharing IoT devices and will conduct a follow-up interview via phone call. The interview will be semi-structured and recorded via Google Voice. Each participant will be awarded a $10 gift card.

We will ask interviewees who have rented their houses through SE , which devices they have shared or want to share with guests, which capabilities of devices they have shared or want to share with guests, for how long they have started sharing those or under which circumstance or features they will start sharing, how they manage to disable access to their smart homes when guests leave their house. If the interviewee has

taken rent of any house through sharing economy we will ask for which smart home IoT devices of homeowners, they have received access or want to have access, which capabilities of devices they had access or want to have access, how the smart homeowners have handled disabling access to IoT devices when they left their houses.

Then we will ask about their concern on privacy and security while sharing smart home devices. We will ask about any issue or incident that triggered their decision on sharing, any challenge they face while sharing those devices, any situation they have anticipated at any time when their privacy or security is not maintained. We will also ask them about the advantages they have received through sharing, access-control features that can increase their willingness to share any device, advantages they might have through sharing any device in the future. To have an understanding of their concerns and demand to increase the usability of smart home devices we will ask them to discuss their thoughts elaborately.

Finally, we will ask them whether they would like to have a share of smart home devices from the opposite perspective e.g. if the interviewee is currently renting his house through sharing economy, what does he think about having access to smart home devices of other homeowners while he is staying there as a tenant? This discussion will help us to have a broader view of their different points of interest and outlook.

Ethics

We hope that our research methods will be approved by the IRB board at the University of Central Florida. Smart homeowners have to be the age of 18+ and agreed to consent to participate.

Feasibility Analysis

We have planned to contact at least 150+ hosts and guests of sharing economy within 5-6 days after submitting a proposal. We have allocated most of our study time in this primary work as they may need some time to respond, we may have to contact with them multiple times to give a clear understanding of our study and purpose. Again, many of them may not be convinced enough to participate in an online survey. In the meantime, hopefully, we will have our IRB approval and be able to conduct our initial survey.

Step	Study Method	Number of participants	time(days)
1	Invitation to survey	150	5-6
2	Initial Survey	30	2-3
3	Response Processing & selecting for interview	-	1-2
4	Interview	10	3-4
5	Data Analysis & Results	-	4-5
		Total	15-20

. Table 1. Project time Management

We will keep our survey questions concise and clear enough so that participants can respond in their convenience within a very short period. Table 1 contains our time management plan. We are planning to receive all responses within 2-3 days. We are expecting that, to analyze responses and select participants for interviews 1-2 days will be required. After that, we will set for semi-structured interviews with each participant. We are assuming each interview will take a maximum of 30 minutes and will be able to complete 10 interviews within 2-3 days by two researchers. We aim at completing user study and data collection within two weeks and spend 4-5 days to analyze that data thoroughly. Overall, in our estimation, about 3 weeks will be required to complete our data collection and analysis.

Data Analysis

Questions of the online survey have been arranged in such a way that responses will be in both free text and multiple-choice forms. A codebook will be developed for various reasons for sharing, interest on sharing, concerns on privacy and security. Later, text answers will be analyzed according to that. For the interview, we will transcribe the data and classify those according to the common theme. We will execute a collaborative coding process by individual researchers to prevent any bias and resolve any conflict or ambiguity with discussion. We will focus on gathering qualitative data through our small sample size. At last, we will use a code aggregation tool to extract higher-level themes from data.

RESULT

We will present the findings from our user study and general findings of participants′ desired features and use cases. We will begin by exploring the situations which have encouraged participants to share smart home IoT devices with almost stranger people and further granular access control and form of access control mechanisms - they want to possess in the future. Some hosts can remain to be concerned about guests accidentally or willingly making changes to access control policies, automation or device configuration and so will not be favorable much to share access-control. Again, smart homes can amplify comfort and make guests' day to day life easier while their short or long term living as a tenant. For some devices, hosts may feel that any supervision is not necessary e.g. smart light. Guests may want restrictions on surveillance using some sensitive devices, such as cameras in the bedroom, locks. Participants will also provide some ideas for design principles for the access-control module to mitigate harms, introducing more transparent methods about how sensitive devices can be used or overriding protections against illegal activities and harassment.

CONCLUSION

This research will give application developers and device manufacturers of future smart home devices guidelines on what kind of access control, data and physical privacy the user wants in a sharing economy. We propose an easy to understand, flexible, not technical, transparent, nuanced and restricted access control system which will give users confidence about the kind of access shared in a sharing economy where smart devices are being used. As privacy and security are a multidisciplinary

concept, this research work should also guide the policymakers of sharing economy to enact appropriate laws to enable and force the use of such an access control system.

ACKNOWLEDGMENTS

We thank Dr. Pamela Wisniewski for her kind guidance and help which helped shape this paper to what it is today.

REFERENCES

[1] The rise of the sharing economy. https://www.economist.com/news/leaders/21573104-internet-everything-hire-rise-sharing-economy. Accessed: 2019-10-03.

[2] Turo car sharing marketplace. https://turo.com/en-us. Accessed: 2019-10-03.

[3] Vacation rentals, homes, experiences & places - airbnb. https://www.airbnb.com/. Accessed: 2019-10-03.

[4] Vrbo | book your vacation rentals: beach houses, cabins, condos & more. https://www.vrbo.com/. Accessed: 2019-10-03.

[5] Homeaway.com | book your vacation rentals: beach houses, cabins, condos & more. https://www.homeaway.com/. Accessed: 2019-10-03.

[6] Vacation rentals - beach houses, cabins, condos, cottages, vacation homes & villas | flipkey. https://www.flipkey.com. Accessed: 2019-10-03.

[7] Vertoe | luggage storage near you - all over usa @ $5.95/day. https://vertoe.com/. Accessed: 2019-10-03.

[8] Fast facts - airbnb. https://press.airbnb.com/fast-facts/. Accessed: 2019-10-03.

[9] Adam Wright. Double-digit growth expected in the smart home market, says idc. https://www.idc.com/getdoc.jsp?containerId=prUS44971219. Accessed: 2019-10-03.

[10] Vivint smart home + airbnb. https://www.vivint.com/airbnb. Accessed: 2019-10-03.

[11] Abraham. It′s time to decentralize airbnb & loyalty –the age of blockchain & cryptocurrencies. https://www.smarthosts.org/posts/zr4w8sek5bh42cpzf/airbnb-blockchain-loyalty-travel/. Accessed: 2019-10-03.

[12] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 255–272, 2018.

[13] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 65–80, 2017.

[14] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. Consumer smart homes: Where we are and where we need to go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications*, HotMobile '19, pages 117–122, New York, NY, USA, 2019. ACM.

[15] What are airbnb's rules about security cameras and other recording devices in listings? https://www.airbnb.com/help/article/887/what-are-airbnbs-rules-about-security-cameras-and-other-recording-devices-in-listings. Accessed: 2019-10-03.

[16] M. N. Islam and S. Kundu. Poster abstract: Preserving iot privacy in sharing economy via smart contract. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 296–297, April 2018.

[17] Chin-Lung Hsu and Judy Chuan-Chuan Lin. An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, 62:516 – 527, 2016.

[18] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home automation in the wild: Challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2115–2124, New York, NY, USA, 2011. ACM.

[19] B. Pearson, L. Luo, Y. Zhang, R. Dey, Z. Ling, M. Bassiouni, and X. Fu. On misconception of hardware and cost in iot security and privacy. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–7, May 2019.

[20] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. Computer security and the modern home. *Commun. ACM*, 56(1):94–103, January 2013.

[21] Google. https://www.google.com/. Accessed: 2019-10-03.

[22] Google home. https://store.google.com/us/product/google_home?hl=en-US. Accessed: 2019-10-03.

[23] James Orme. German regulator bans google from listening to google home recordings for three months across europe. https://techerati.com/news-hub/german-regulator-bans-google-from-listening-to-google-home-recordings-for-three-months-across-europe/. Accessed: 2019-10-03.

[24] Dave Randall. *Living Inside a Smart Home: A Case Study*, pages 227–246. Springer London, London, 2003.

[25] Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela J. Wisniewski. The internet of what?: Understanding differences in perceptions and adoption for the internet of things. *IMWUT*, 2:183:1–183:22, 2018.

[26] E. Fernandes, J. Jung, and A. Prakash. Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 636–654, May 2016.

[27] W. Enck, M. Ongtang, and P. McDaniel. Understanding android security. *IEEE Security Privacy*, 7(1):50–57, Jan 2009.

[28] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, New York, NY, USA, 2012. ACM.

[29] Yunhan Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, and Atul Prakash. Contexlot: Towards providing contextual integrity to appified iot platforms. In *NDSS*, 2017.

[30] Yuan Tian, Nan Zhang, Yueh-Hsun Lin, XiaoFeng Wang, Blase Ur, XianZheng Guo, and Patrick Tague. Smartauth: User-centered authorization for the internet of things. In *Proceedings of the 26th USENIX Conference on Security Symposium*, SEC'17, pages 361–378, Berkeley, CA, USA, 2017. USENIX Association.

[31] Tiffany Hyun-Jin Kim, Lujo Bauer, James Newsome, Adrian Perrig, and Jesse Walker. Challenges in access right assignment for secure home networks. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, HotSec'10, pages 1–, Berkeley, CA, USA, 2010. USENIX Association.

[32] T. H. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Access right assignment mechanisms for secure home networks. *Journal of Communications and Networks*, 13(2):175–186, April 2011.

[33] Michelle L. Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger, and Michael K. Reiter. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 645–654, New York, NY, USA, 2010. ACM.

[34] Vassilios Lekakis, Yunus Basagalar, and Pete Keleher. Don't trust your roommate or access control and replication protocols in "home" environments. In *Proceedings of the 4th USENIX Conference on Hot Topics in Storage and File Systems*, HotStorage'12, pages 12–12, Berkeley, CA, USA, 2012. USENIX Association.

[35] K. Kostiainen, O. Rantapuska, S. Moloney, V. Roto, U. Holmstrom, and K. Karvonen. Usable access control inside home networks. In *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–6, June 2007.

[36] Matthew Johnson. Usability of security management: Defining the permissions of guests. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols*, pages 284–285, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[37] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, pages 399–412, Berkeley, CA, USA, 2017. USENIX Association.

[38] Stuart Schechter. The user is the enemy, and (s)he keeps reaching for that bright shiny power button! In *Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*, July 2013.

[39] A.J. Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In *CSCW 2013*. ACM, February 2013.

[40] Simon Moncrieff, Svetha Venkatesh, and Geoff West. Privacy and the access of information in a smart house environment. In *Proceedings of the 15th ACM International Conference on Multimedia*, MM '07, pages 671–680, New York, NY, USA, 2007. ACM.

[41] A.J. Brush and Kori Inkpen. Yours, mine and ours? sharing and use of technology in domestic environments. In *Ubicomp 2007*. Springer, September 2007.

[42] Colin Dixon, Ratul Mahajan, Sharad Agarwal, A.J. Brush, Bongshin Lee, Stefan Saroiu, and Paramvir Bahl. An operating system for the home. In *Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*, pages 337–352, San Jose, CA, 2012. USENIX.

[43] Blase Ur, Jaeyeon Jung, and Stuart Schechter. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014, July 2013.

[44] W. Keith Edwards and Rebecca E. Grinter. At home with ubiquitous computing: Seven challenges. In *Proceedings of the 3rd International Conference on Ubiquitous Computing*, UbiComp '01, pages 256–272, Berlin, Heidelberg, 2001. Springer-Verlag.

Survey Instrument

SCREENING QUESTIONS

Research Study: Smart Home in the context of share economy: Exploring the perspective, security and privacy concerns of both hosts and guests of share economy who use smart home IoT devices.

Thank you for your interest in this participating in this following research study. To verify that you are eligible to participate, please answer some questions.

Q1.1 In which country do you currently reside? .....

Q1.2 What is your age? .....

Q1.3 Have you ever used any share economy platforms e.g. AirBnB, HomeAway, ShortTermStays? .....

Q1.4 What is your role on share economy context?
From the list below, please check ALL that apply.

- ☐ Host(You have shared your house with any person through SE platform)
- ☐ Guest (You have stayed in any house rented through any SE platform)
- ☐ ⊗ None of the above

Q1.5 Smart home devices are internet-connected electronics that are installed in your home and can be remotely controlled over the internet, typically by using a mobile app.

From the list below, please select all of the internet-connected smart home device(s) that you currently have in your home. The specific brands provided in parentheses are shown as examples. Please select any category of smart home device that you own even if it is a different brand. Please check ALL that apply.

- ☐ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)
- ☐ Smart Display (e.g. Google Home Hub, Amazon Echo Show)
- ☐ Light (e.g. Philips Hue, LIFX, Eufy)
- ☐ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)
- ☐ Thermostat (e.g. Nest Thermostat, Ecobee)
- ☐ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)
- ☐ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)
- ☐ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)
- ☐ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)
- ☐ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)
- ☐ Motion/Contact Sensor
- ☐ ⊗ None of the above

Q1.6 How many different types of smart home devices do you own? .....

Q1.7 If you have been guests only in SE context(have not been host anytime), do you want to have access to any smart home devices of that house while being tenant?

- ○ Yes
- ○ No

Q1.8 **From the list below, please select all of the internet-connected smart home device(s) that you want to have access to while being tenant in any house.** The specific brands provided in parentheses are shown as examples. Please select any category of smart home device even if it is a different brand. Please check ALL that apply.

- ☐ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)
- ☐ Smart Display (e.g. Google Home Hub, Amazon Echo Show)
- ☐ Light (e.g. Philips Hue, LIFX, Eufy)
- ☐ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)
- ☐ Thermostat (e.g. Nest Thermostat, Ecobee)
- ☐ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)
- ☐ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)
- ☐ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)
- ☐ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)
- ☐ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)
- ☐ Motion/Contact Sensor
- ☐ ⊗ None of the above

CHI'20, April 25–30, 2020, Honolulu, HI, USA

ISBN 978-1-4503-6708-0/20/04…$15.00

DOI: https://doi.org/10.1145/3313831.XXXXXXX

If you are willing to have access to any other devices not listed above, please write down below.

_____
_____
_____
_____

Participants passed the screening survey if they live in USA, at least 18 years old, they are currently sharing or have shared their houses through SE and have at least 2 smart home devices from the list or have been guest through any SE sites and willing to have access to smart home devices while being tenant. Qualified participants were then shown the consent form and asked to consent. Following questions were shown to the participants who consented to participate in the survey.

COMPREHENSION CHECK

Participants who have two chances to select the correct answer. Participants who failed twice were disqualified from the survey and did not see the rest of the questions.

Q2.1 If you are a host, we are going to ask you about your concerns about sharing smart home devices with the people to whom you have given rent your house through SE. More specifically, we will ask you about experiences or expected security, privacy and usability features of smart home IoT devices with the people **not related to you by any means and you gave rent your house through SE**, if you have/had already given **access** to them or you would **like them to access** those in future **during their staying at your house**.

Please select the TRUE statement.

○ This survey asks about sharing my smart home devices with my relative when they visit my house.

○ This survey asks about sharing my smart home devices with someone who has taken rent through any SE and will access and/or control the devices.

○ This survey asks about remotely sharing my smart home devices with someone who has taken rent through any SE and will access and/or control the devices over-the-internet.

Q2.2 If you have been guest in any house through SE, we are going to ask you about your experience about sharing smart home devices of owners from whom you have taken rent through SE. More specifically, we will ask you about experiences or expected security, privacy and usability features of smart home IoT devices owned by the home owners who are **not related to you by any means and you have taken rent their house through SE**, if you have/had already received**access** to IoT devices or you would **like them to access** those in future **during your staying at their houses**. Please select the TRUE statement.

○ This survey asks about sharing my smart home devices with home owners from whom I have taken house rent through SE.

○ This survey asks about accessing smart home devices of home owners from whom I have taken house rent through any SE while being tenant.

○ This survey asks about remotely accessing smart home devices of home owners from whom I have taken house rent through any SE , over-the-internet.

Following questions were shown for each person participants listed in the question 3

DEVICES SHARED

Q5.1 If you are a host,for which of the following smart home device(s) you have given **already accesses** to your guests**(only known through SE)** while their staying at your home?

□ Other devices I own (Please specify)

□ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)

□ Smart Display (e.g. Google Home Hub, Amazon Echo Show) (3)

□ Light (e.g. Philips Hue, LIFX, Eufy)

□ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)

□ Thermostat (e.g. Nest Thermostat, Ecobee)

□ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)

□ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)

□ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)

□ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)

□ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)

□ Motion/Contact Sensor

□ ⊗ None of the above

Q5.2 If you are a host,for which of the following smart home device(s) you want to give **accesses** to your guests**(only known through SE)** while their staying at your home **in future**?

□ Other devices I own (Please specify)

□ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)

□ Smart Display (e.g. Google Home Hub, Amazon Echo Show) (3)

□ Light (e.g. Philips Hue, LIFX, Eufy)

□ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)

□ Thermostat (e.g. Nest Thermostat, Ecobee)

- ☐ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)
- ☐ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)
- ☐ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)
- ☐ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)
- ☐ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)
- ☐ Motion/Contact Sensor
- ☐ ⊗ None of the above

Q5.3 If you are/have been guest**(only through SE)** ,for which of the following smart home device(s) you want to have **accesses** while being tenant?

- ☐ Other devices I own (Please specify)
- ☐ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)
- ☐ Smart Display (e.g. Google Home Hub, Amazon Echo Show) (3)
- ☐ Light (e.g. Philips Hue, LIFX, Eufy)
- ☐ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)
- ☐ Thermostat (e.g. Nest Thermostat, Ecobee)
- ☐ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)
- ☐ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)
- ☐ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)
- ☐ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)
- ☐ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)
- ☐ Motion/Contact Sensor
- ☐ ⊗ None of the above

Q5.4 If you are/have been guest**(only through SE)** ,for which of the following smart home device(s) you want to have **accesses** while being tenant **in future**?

- ☐ Other devices I own (Please specify)
- ☐ Smart Speaker or Personal Voice Assistant Hub (e.g. Google Home, Amazon Echo)
- ☐ Smart Display (e.g. Google Home Hub, Amazon Echo Show) (3)
- ☐ Light (e.g. Philips Hue, LIFX, Eufy)
- ☐ Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ)
- ☐ Thermostat (e.g. Nest Thermostat, Ecobee)
- ☐ Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam)
- ☐ Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro2)
- ☐ Smart Doorbell (e.g. Ring Doorbell, Nest Hello)
- ☐ Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm)
- ☐ Fire/Flood/Freeze Alarm (connected smoke/CO sensors)
- ☐ Motion/Contact Sensor
- ☐ ⊗ None of the above

CAPABILITIES SHARED

We randomly selected three three services that participants listed in section 5.1-5.4 and showed capability related question only for those three devices.

Q6.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Speaker or Personal Voice Assistant hub (e.g. Google Home, Amazon Echo) while they stay at your house.

- ☐ View the device usage history (ability to listen to the past voice commands and view the time of the commands)
- ☐ Delete the past voice commands stored in the cloud
- ☐ View which other devices are connected to the voice assistant hub
- ☐ Control the other devices using the voice assistant from outside of home
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Dropping in on the listed smart speakers and displays, when you 'drop in' on a device, you will be able to listen to all activities surrounding that device and will also be able to speak through the speaker
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

Q6.2 If you are a host, please indicate how you want to let have **additional accesses** of the Smart Speaker or Personal Voice Assistant hub (e.g. Google Home, Amazon Echo) your guests**(only known through SE) now or in future**. [1]

Q7.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Display (e.g. Google Home Hub, Amazon Echo Show) while they stay at your house.

- ☐ View the device usage history (ability to listen to the past voice commands, view the time of the commands, view the call history and watch history)

[1]Question similar to 6.2 will be shown for each of the different devices that people currently share. Hence we are skipping it for rest of the devices

- □ Delete the past voice commands stored in the cloud
- □ View which other devices are connected to the voice assistant hub
- □ Control the other devices using the smart display from outside of home
- □ Access the video feed when the camera integrated into the smart display is used as security and surveillance cam
- □ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- □ Install latest software and security updates
- □ Other (Please specify)

Q8.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Light (e.g. Philips Hue, LIFX, Eufy) while they stay at your house.

- □ View the light state, whether the light is currently on/off, the color and brightness of the light
- □ Remotely turn off/on the light and change it's brightness or color
- □ Configure the lights to automatically turn on/off or change it's brightness/color based on time or state of other devices.
- □ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- □ Install latest software and security updates
- □ Other (Please specify)

Q9.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Lock/Garage Door Opener (e.g. Schlage, Kwikset, August, Chamberlain MyQ) while they stay at your house.

- □ View lock state, whether the lock is currently opened or closed
- □ View lock log, who entered the house and when
- □ Get notification when someone tries to tamper with the lock
- □ Remotely open/close the lock
- □ Configure the lock to automatically open/close based on time or state of other devices.
- □ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- □ Install latest software and security updates
- □ Other (Please specify)

Q10.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Thermostat (e.g. Nest Thermostat, Ecobee) while they stay at your house.

- □ View the current temperature in the Thermostat
- □ View the log of past temperature adjustments and who made them
- □ Delete energy or temperature adjustment history
- □ Remotely change the temperature
- □ Configure the thermostat to automatically turn on/off or change temperature based on time or state of other devices.
- □ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- □ Install latest software and security updates
- □ Other (Please specify)

Q11.1 If you are a host, please indicate how you let your guests **(only known through SE)** access Smart Indoor Camera (e.g. Nest Cam Indoor, WyzeCam) while they stay at your house.

- □ View the camera recordings stored in the cloud or local storage
- □ View live streaming
- □ Delete the video stored in the cloud or local storage
- □ Share the video stored in the cloud or local storage
- □ Remotely turn on/off the camera
- □ Change the camera angle or zoom settings
- □ Listen to what is happening in the area using the microphone and speak to people/pets using the speaker integrated into the camera
- □ Get notification when the camera detects movement or sound
- □ Configure the camera to automatically turn on/off based on time or state of other devices.
- □ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- □ Install latest software and security updates
- □ Other (Please specify)

Q12.1 If you are a host, please indicate how you let your guests **(only known through SE)** access Smart Outdoor Camera (e.g. Nest Cam Outdoor, Arlo Pro 2) while they stay at your house.

- □ View the camera recordings stored in the cloud or local storage
- □ View live streaming

- ☐ Delete the video stored in the cloud or local storage
- ☐ Share the video stored in the cloud or local storage
- ☐ Remotely turn on/off the camera
- ☐ Change the camera angle or zoom settings
- ☐ Listen to what is happening in the area using the microphone and speak to people/pets using the speaker integrated into the camera
- ☐ Get notification when the camera detects movement or sound
- ☐ Configure the camera to automatically turn on/off based on time or state of other devices.
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

Q13.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Smart Doorbell (e.g. Ring Doorbell, Nest Hello) while they stay at your house.

- ☐ View Live streaming of the door area
- ☐ Get notification when doorbell pressed or motion detected in the front door
- ☐ View recorded video stored in the cloud
- ☐ Remotely speak to the visitor
- ☐ Delete the video from the cloud
- ☐ Share the video stored in the cloud
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

Q14.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Burglar Alarm (e.g. ADT, Nest Protect, Ring Alarm) while they stay at your house.

- ☐ Get notification when alarm triggers
- ☐ View the status of the alarm, whether the alarm is armed/disarmed
- ☐ Remotely arm/disarm the alarm
- ☐ View log information, when the alarm was triggered, which sensor triggered the alarm, who armed/disarmed the alarm, when the alarm was armed/disarmed etc.
- ☐ Configure the alarm to automatically arm/disarm based on time or state of other devices
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

Q15.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Fire/Flood/Freeze Alarm (connected smoke/CO sensors) while they stay at your house.

- ☐ View the status of the sensors
- ☐ Get a notification when hazards happens
- ☐ Remotely silent the alarm, when the alarm triggers
- ☐ View log information, when the alarm was triggered, which sensor triggered the alarm, who silenced the alarm etc.
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

Q16.1 If you are a host, please indicate how you let your guests **(only known through SE)** access the Motion/Contact Sensor while they stay at your house.

- ☐ Get a notification when motion/contact is detected
- ☐ View the status of the sensor, whether the sensor is open/close, motion/no motion
- ☐ View log information, when the motion/contact was detected in the past, which sensor detected the motion/contact etc.
- ☐ Configure the sensors to automatically activate/deactivate based on time or state of other devices
- ☐ Add a new user to the device and give them different access as well as remove an existing user and revoke access
- ☐ Install latest software and security updates
- ☐ Other (Please specify)

OPEN-ENDED QUESTIONS FOR CURRENT SHARING

Q17.1 Why do you share your 'device(s)' and corresponding accesses with guests**(only known through SE)**?

Please provide **specific examples** of when and how sharing these devices is **beneficial** to you or to them when they stay at your house.

_____

_____

Q17.2 In your previous responses, you mentioned that you would like to **share** some **additional accesses** besides the ones you already shared for some devices with guests**(only known through SE)**.

Why **don't** you **currently share** those accesses for those devices?

OPEN ENDED QUESTIONS FOR FUTURE SHARING

Q19.1 Why would you like to share your 'device(s)' and corresponding accesses with guests **(only known through SE)**?

Please provide **specific examples** of when and how sharing these devices with guests**(only known through SE)**would be **beneficial** to you or to them when they stay at your house.

Q19.2 Why don't you **currently share** the remote access of 'device(s)' with guests**(only known through SE)** ?

RECIPROCAL SHARING

Q20.1 Now, we would like to reverse roles between you and your guests. We want to know if you rent any house**(only through SE)** , would you like to **have access** of their smart home devices with you while **staying as tenant**?

Please think broadly about all the devices you might want the person to remotely share with you now or in the future. Do not restrict yourself with the devices that person currently have.

Q20.2 Why would hosts or you want them to **let have access to** their smart home devices while staying as tenant? Please be specific about the person and the devices he/she already shares or you want him/her to remotely share with you in your answer.

Q20.3 Why wouldn't you want to have**access to** their smart home devices while staying as tenant?

The following questions were only shown to the participants who do not currently share and so not want to share their smart home devices with people outside of the home in the future.

Reason for not sharing the devices currently or in the future

Q21.1 Why don't you **share or foresee sharing** any of your smart home devices with guests**only known through SE** when they stay at your home? Please explain in detail using complete sentences.

Q21.2 Please explain if anything would **change** your **decision in future** regarding sharing your smart home devices with guests **only known through SE** when they stay at your home.

Think broadly about the circumstances in the future when it may be beneficial for you to remotely share your smart home devices with someone outside of your home.

DEMOGRAPHICS

You're almost finished! Lastly, we would like to learn more about you to group your answers with others like you.

[2]

Q22.2 What is the highest level of school you have completed or the highest degree you have received?

- ○ Less than high school degree
- ○ High school graduate (high school diploma or equivalent including GED)
- ○ Some college but no degree
- ○ Associate degree in college (2-year)
- ○ Bachelor's degree in college (4-year)

[2]Question similar to 6 -10 will be shown for each of the different devices for guests who have or want to have access to smart home IoT devices . Hence we are skipping it.

○ Master's degree

○ Doctoral degree

○ Professional degree (JD, MD)

Q22.3 Choose one or more races that you consider yourself to be:

□ White or Caucasian

□ Black or African American

□ American Indian or Alaska Native

□ Asian

□ Native Hawaiian or Pacific Islander

□ Other

Q22.4 What is your sex?

○ Male

○ Female

○ Other _____

Q22.5 Please indicate the answer that includes your entire household income in (previous year) before taxes.

○ Less than $ 15,000

○ $ 15,000 to $ 24,999

○ $ 25,000 to $ 34,999

○ $ 35,000 to $ 49,999

○ $ 50,000 to $ 74,999

○ $ 75,000 to $ 99,999

○ $ 100,000 to $ 149,999

○ $ 150,000 to $ 199,999

○ $ 200,000 year and above

○ Prefer not to answer

Q22.6 What is your primary occupation?

_____

Q22.7 Which type of residence do you you currently live in?

○ Single family home

○ Apartment

○ Condominium

○ Other _____

Q22.8 Which of the following best describes your current housing situation?

○ Home-Owner

○ Renter

○ Living with others, but not paying rent

○ Other _____

Q22.9 Whom do you live with (select all that apply)?

□ ⊗ Live alone

□ My spouse or partner

□ My child (young or adult)

□ Other relatives (e.g. parent, sibling, cousin)

□ Friend/Roommate

□ Other _____

Q22.10 You indicated that you currently share or want to share one or more of your smart home devices with guests**only known through SE**. We are excited to learn more about this.

We're curious if we can **schedule a follow up interview** with you. The interview will take approximately **30-40 minutes** and you would be compensated with a $**10** for your time. **Please enter your email address** below if you are interested. You may leave this space blank if you do not wish to participate.

_____

Q52.11 Thank you for completing the survey. Your responses have been recorded.

Please let us know if you have any other comments or insights on the topic of sharing smart home devices with people outside of your home (optional). We value your feedback.

_____

_____

_____

_____