End Users' Information-sharing Behaviours and Preferences within a Multi-user Smart Home

Yue Huang
University of British Columbia

Borke Obada-Obieh
University of British Columbia

Konstantin Beznosov
University of British Columbia

Abstract

The Internet of Things (IoT) is becoming increasingly popular in home environments, in which multiple users with complex social relationships can interact with the shared devices. As a result, many types of information associated with shared devices could be shared among multiple users. In this study, we seek to understand interactions among multiple people and devices in a smart home. We conducted an exploratory study to investigate users' information-sharing behaviors and preferences within a multi-user smart home. The findings can highlight the challenges users experience in multi-user smart homes and provide more usable, effective, and secure information-sharing default settings for smart home devices.

1 Introduction

The Internet of Things (IoT) is becoming increasingly popular in home environments. The number of smart home devices adopted worldwide, is predicted to be nearly 1.3 billion by 2022, with a five-year compound annual growth rate of 20.8% [3, 16]. With a variety of IoT devices, such as smart speakers, lighting, smart thermostats, and home security systems, users can automate their homes and improve their overall quality of lives in many ways. For instance, automated systems like lawn care can be set up, home security systems can be monitored remotely, and home energy usage can be optimized by manipulating other smart devices.

IoT devices are commonly adopted at homes, in which multiple users with complex social relationships can interact with these shared devices. Thus, many device manufacturers have now enabled multiple users to set up their own accounts on single devices. For instance, up to 25 users are able to share a single Nest Home with different levels of access, including at the owner-level, fully, and at the home entry only state [11]. As a result, by sharing devices in a smart home, multiple users can access many types of information that are associated with shared devices. For example, after being granted full access to Nest Home, one user can check the smart lock status, watch the video clips from the smart camera, and receive notifications from the smoke and carbon monoxide detector [10, 12, 29].

Without doubts, smart devices' sharing access feature can benefit to users, such as providing greater convenience. However, previous work suggests that users have privacy and security concerns toward their housemates in terms of sharing smart devices. As a strategy to address these concerns, users sometimes avoid using certain features, which deprives them from fully benefiting from their devices [15].

Most previous studies focused on investigating users' comfort levels in sharing IoT-related information with external entities, such as device manufacturers. A number of studies have revealed that users' information sharing preferences depend on a variety of factors such as the type of data recorded, the location where it is recorded, with whom the data is shared, the perceived value of the data and the benefits provided by the services using that data [2, 5, 6, 9, 19, 20, 22, 25]. For example, Naeini et al. [6] used vignettes to study many of these factors with over 380 different use cases across 1,000 users. The results reveal that a minority of participants expressed mistrust of or discomfort with sharing their data with the government and law enforcement agencies.

At the same time, users' desire for access control policies regarding housemates within a smart home have received little attention. Previous studies simply focus on investigating home users' controlling access to their digital files [24], social network accounts [17, 26, 27], digital photos [18], and electronic devices, such as laptops [23, 24]. The most closely related study, conducted by He et al. [13], investigated users' preferences for access control policies for different *capabili-*

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

ties within a single IoT device. They examined how capability- and relationship-centric models influence user expectations concerning access control of the smart home. They discovered that the desired policies can vary widely within a *single* device based on the relationship and the context of access.

However, our previous work [15] indicates that smart device users have a tendency to share some types of information with their housemates and intentionally withhold other types of information due to privacy concerns. Therefore, we intend to conduct an exploratory study to investigate users' information-sharing behaviours and preferences within a multi-user smart home. In addition, we aim to explore how users' information sharing preferences differ based on device types and other factors. For example, our previous work [15] suggests that users of shared smart speakers have concerns about their housemates accessing their calendars. We, therefore, aim to discover whether users would have the same concerns regarding their calendars being accessed through shared PCs or other devices.

In summary, we investigate the following research questions:

- What are users' perceptions on how their smart device associated information is being shared?
- What are users' information-sharing preferences within a smart home?
- What methods do users employ to restrict others from accessing their information?
- What challenges do users encounter in terms of sharing information and devices in smart homes?

2 Related Work

Prior studies focused on understanding users' perceptions [28], privacy and security concerns [7, 30, 31], and mitigation strategies [1] in the context of home IoT devices. Tabassum et al. [28] report that users are highly uncertain about the data practice of their smart home device manufacturers. Zeng et al. [30] suggest that users' threat models have gaps that arise from a limited technical understanding of smart home technologies. Therefore, it is not surprising that participants in a study by Naeini et al. [6] were significantly more concerned with their biometric data being collected and used by companies. These limited concerns might be in part explained by the findings of Zheng et al. [31] that owners of IoT devices value the convenience and connectedness over their privacy. When Aleisa et al. [1] conducted a literature review of existing IoT privacy-preserving solutions, they concluded that most solution providers assume that the end users would be willing to expend effort to preserve their privacy, which may be unrealistic.

Other scholars have studied users' privacy preferences when using IoT devices. Lee et al. [20, 21] discovered that while participants were comfortable with device manufacturers' one-time monitoring of their activities, they were concerned about continuous monitoring. Regarding data access, participants were uncomfortable if their collected data were being monitored and shared with the government [21, 31]. He et al. studied participants' preferences for access control policies for different capabilities within a single IoT device. They discovered that the desired policies vary widely based on the relationship between the users and the context of access [14].

Security researchers have been actively investigating the vulnerabilities and security challenges in the IoT domain. Geneiatakis et al. [8] discovered vulnerabilities that enable impersonation, denial of service attacks, and eavesdropping on commands, while Bugeja et al. [4] identified possible vulnerabilities in services and communications of IoT devices. In addition, Bugeja et al. [4] reported four significant privacy and security challenges in the smart home domain, including identity management, risk assessment methods, information flow control approaches, and security management methods. All the identified risks emphasize on the situations where the adversary is an outside entity of the household. In such cases, the adversary may not be able to get access to the device directly and has limited information about the actual user. In contrast, the risks among different users in the same household could vary from identified risks in the previous research.

3 Methodology

3.1 Recruitment and Screening

In order to explore smart home users' information-sharing behaviours, preferences, and challenges, we conduct semi-structured interviews with smart home users. Participants are recruited by advertising on Facebook, Twitter, Instagram, and UBC's paid participants studies list. Potential participants are required to complete a survey to verify their eligibility for the study. The survey includes questions to identify whether participants are sharing any smart home device, and the relationship between them and the other users. The screening survey also ensures that the sample covered a wide range of relationships within a household, such as roommates, parent-child, siblings, and romantic relationships. Interviews were conducted through either Zoom or Skype. The participants were compensated with either $20 worth of Amazon gift card or through e-transfer. This study was reviewed and approved by the UBC Behavioural Research Ethics Board.

3.2 Interview Procedure

The interview questions focus on three segments.

Device-sharing management: Participants are asked to describe their shared smart devices, with whom they share the devices, and how and what rules they establish for the use of their shared devices. For instance, do users mutually agree that everyone has equal power over shared devices?

Perceptions of information sharing: In order to elicit participants' understanding about the information that is being shared through shared devices, we use a combination of three methods: a drawing exercise, a verbal explanation, and a card-sorting exercise. First, participants are asked to create a drawing to describe how the devices are shared within the household. After each drawing is completed, participants are asked to take a picture of their drawings and sent the pictures to us through email. After we get the email, participants are then asked to verbally describe their thought processes with reference to their drawings. Then, in the second step, participants are asked to conduct a card sorting exercise to describe the types of information that are being shared. Participants are asked to conduct the exercise through OptimalWorkshop, an online card-sorting exercise tool [1]. Participants are provided with a set of cards, with different types of information and the names of different housemates. They are then asked to move around the cards to explain what information is being shared and whom the information is being shared with through the shared smart device.

In addition, participants will be asked to indicate the types of information they prefer not to be shared and their reasons for this. More questions concerning private information being shared in other ways will be asked. Participants will also be asked to identify additional types of information they expect would be shared with other housemates and the reasons behind this. I will further ask participants to illustrate the factors that influence their decisions on information sharing.

Strategies to protect privacy: Participants will be asked about the strategies they use to protect their privacy in terms of sharing devices and information within their households. For example, participants will be asked about the methods they use to restrict others from accessing their information. They will also be asked about the efficiency of the methods they employed. Furthermore, participants will be asked about the challenges they deal with in terms of sharing their smart devices and information.

3.3 Data Analysis

The interview data are analyzed using Grounded Theory. After each interview, we transcribe and analyze the collected data. Based on the findings, the interview guide is modified before the next interview takes place. A model concerning how users of smart homes manage their information sharing behaviours is expected to be developed based on the collected data.

[1] shorturl.at/hlBS4

4 Current Process

This is an ongoing project. We have conducted two pilots and one more interview. The interview guide was modified based on the results of the pilots.

Device Purchase Decisions. Primary users usually conducted research on the smart home devices before purchased them. Some of them explicitly consulted with their co-occupants over which smart devices to get. One participant shared video reviews of certain smart devices to his housemates to help them learn about the shared devices.

Device-sharing management. Primary users often took the responsibility of setting up the devices and made the rules of sharing the devices. Participant one said her farther purchased the Google Home, created a family Google account, and asked all family members to use the shared the Google Home through the family Google account. P1 said: *" We don't like putting all our Google accounts in there. We just use one ... So we had like a family account, which was set up by my dad. So it's like only for like family issues ... so it's less of a privacy breach."*

Perceptions of information sharing. Participants have a limited understanding of how their devices are being shared. So far, two participants had an incomplete understanding of which features and data were shared and which were kept private through shared devices. For example, when Pilot participant one explained how the smart speaker was shared between her and her family members, she only drew and described the features that were mostly used by each user.

We are currently recruiting more participants. More results are expected to be provided in the later version of the manuscript.

References

[1] Noura Aleisa and Karen Renaud. Privacy of the internet of things: a systematic literature review. In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, 2018.

[3] IOT News Asia. Smart home devices forecast to deliver double-digit growth through 2022. https://iotnews.asia/1422/smart-homes/smart-home-devices-forecast-to-deliver-double-digit-g 2018. Last accessed: October 2, 2018.

[4] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. On privacy and security challenges in smart connected

homes. In *Intelligence and Security Informatics Conference (EISIC), 2016 European*, pages 172–175, Uppsala, Sweden, 2016. IEEE.

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

[6] 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, USA, 2017. USENIX Association.

[7] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 534:1–534:12, New York, NY, USA, 2019. ACM.

[8] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. Security and privacy issues for an iot based smart home. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on*, pages 1292–1297, Opatija, Croatia, 05 2017. IEEE.

[9] Marco Ghiglieri, Melanie Volkamer, and Karen Renaud. Exploring consumers' attitudes of smart tv related privacy risks. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 656–674. Springer, 2017.

[10] Google. How to use sightline and event history to watch your camera's video. https://support.google.com/googlenest/answer/9208447?hl=en, 2020.

[11] Google. Learn about family accounts and how to share access to your nest home. https://support.google.com/googlenest/answer/9304271?co=GENIE.Platform%3DiOS&hl=en, 2020.

[12] Google. Learn about notifications and how to change settings. https://support.google.com/googlenest/answer/9244826?hl=en&ref_topic=9346935, 2020.

[13] 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.

[14] 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 *Proceedings of the 27th USENIX Conference on Security Symposium*, SEC'18, pages 255–272, Berkeley, CA, USA, 2018. USENIX Association.

[15] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[16] IDC. Worldwide quarterly smart home device tracker. https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1781, 2019.

[17] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. Caring about sharing: Couples' practices in single user device access. In *Proceedings of the 19th International Conference on Supporting Group Work*, pages 235–243, 2016.

[18] Peter Klemperer, Yuan Liang, Michelle Mazurek, Manya Sleeper, Blase Ur, Lujo Bauer, Lorrie Faith Cranor, Nitin Gupta, and Michael Reiter. Tag, you can see it! using tags for access control in photo sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 377–386, 2012.

[19] Scott Lederer, Jennifer Mankoff, and Anind K Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*, pages 724–725, 2003.

[20] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. In *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*, pages 407–412, Reston, VA, 2016. IEEE.

[21] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide iot environment. In *Pervasive Computing and Communications (PerCom), 2017 IEEE International Conference on*, pages 276–285, Kona, HI, 2017. IEEE.

[22] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "what can't data be used for?" privacy expectations about smart tvs in the us. In *European Workshop on Usable Security (Euro USEC)*, 2018.

[23] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. " she'll just grab any device that's closer" a study of everyday

device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5921–5932, 2016.

[24] Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, et al. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 645–654, 2010.

[25] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. The contextual complexity of privacy in smart homes and smart buildings. In *International Conference on HCI in Business, Government, and Organizations*, pages 67–78. Springer, 2016.

[26] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? an exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 83–102, 2018.

[27] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 895–904, 2007.

[28] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. "i don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, pages 435–450, Berkeley, CA, USA, 2019. USENIX Association.

[29] Beth uel De La Cruz. August smart lock pro hands-on review. https://homealarmreport.com/smart-home/august-review/, 2019. Last accessed: Aug. 19, 2019.

[30] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, pages 65–80, Berkeley, CA, USA, 2017. USENIX Association.

[31] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW):200:1–200:20, November 2018.