Perceptions of Smart Home Privacy and Security Responsibility, Concerns, and Mitigations

Julie Haney
National Institute of Standards and Technology
julie.haney@nist.gov

Susanne Furman
National Institute of Standards and Technology
susanne.furman@nist.gov

Yasemin Acar
Leibniz University Hannover
acar@sec.uni-hannover.de

Mary Theofanos
National Institute of Standards and Technology
mary.theofanos@nist.gov

Poster presented at the 15th Symposium on Usable Privacy and Security (SOUPS 2019)

Abstract

Smart home devices are increasingly being used by non-technical users who have little understanding of the privacy and security implications of the technology. To better understand perceptions of smart home privacy and security, we are conducting an interview study of individuals living in smart homes. Preliminary analysis reveals potential relationships between perceptions of responsibility and privacy and security concerns and mitigation actions. Results can inform future efforts to educate users about their responsibility, advance the protection of user data, and protect the devices from unintended access.

Author Keywords

Internet of things; smart home; usable security; usable privacy

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction

The Internet of Things (IoT) market is exploding, with the number of IoT devices expected to grow from 26 billion in 2019 to 75 billion in 2025 [5]. With this growth, IoT technology is becoming more pervasive in the home environment, with 34% of broadband households forecasted to have

Privacy Concerns: *“If somebody has access to this cloud information and they’re actually able to associate when you’re home and when you’re not home based on the sensors and other things you have in your house, they could potentially target you.”* (P11_A)

Security Concerns: *“what if someone hacks into our phones and. . . with the Nest. . . they try to reconfigure it on their own or especially the alarm system.”* (P12_U)

Lack of Concern: *“I feel like you’ve got people who are pretty talented with computers and can get this stuff. But again, I’m of the mindset, have at it. We don’t do anything cool in my house, anyways.”* (P8_A)

Tradeoffs: *“I know that it’s collecting personal data. . . and I know there’s the potential of a security leak, but yet, I like having the convenience of having those things.”* (P1_A)

smart home systems by 2025 [1]. While early adopters of smart home technology have typically been more technically savvy, IoT smart home devices are increasingly being used by non-technical users who have little understanding of the technology or awareness of the implications of use. In particular, the impact of and interplay of factors such as usability, security, privacy, and trust have not been adequately explored within one comprehensive study. We address this gap with an in-progress qualitative interview study of individuals living in smart homes. Preliminary analysis focused on privacy and security reveals potential relationships between perceptions of responsibility, concerns, and mitigation actions. Results can inform future efforts to educate users about their privacy and security responsibility, advance the protection of user data via usable interfaces, and protect the devices from unintended access.

Related Work

Prior work has examined perceptions of smart home privacy and security. Parks Associates [2] and Worthy et al. [7] found that a lack of trust in vendors to properly safeguard personal data is a major obstacle to adoption of smart home technology. From a broader IoT perspective, Williams et al. [6] found that IoT is viewed as less privacy-respecting than non-IoT devices such as desktops, laptops, and tablets. However, users’ privacy concerns were not always translated into privacy-protecting actions. Interviews of people living in smart homes by Zeng et al. [8] and a PwC industry survey [4] revealed that, although users may be aware of security and privacy issues, these were often overlooked when a product proved otherwise valuable.

Methods

We conducted 15 semi-structured interviews, lasting on average 50 minutes, as part of an in-progress study to understand end users’ perceptions of and experiences with smart home devices. The study was approved by the NIST Human Subjects Protection Office. Prospective participants first completed an online screening survey about their smart home devices, their role with the devices (e.g., purchaser, administrator, user), and professional backgrounds. Participants were selected for interviews if they had multiple smart home devices for which they were an active user. Of the 15 participants, 12 had installed and administered the devices (indicated with an A after their participant ID) and three were non-administrative users of the devices (indicated with a U).

Interview questions addressed several areas: understanding of smart home terminology; purchase and general use; installation and troubleshooting; privacy; security; and safety. Interviews were audio recorded and transcribed. We then performed iterative coding and qualitative analysis on the data to identify core concepts [3]. In this poster, we report on a subset of our preliminary findings specific to privacy and security concerns, mitigations, and responsibility.

Preliminary Findings

Preliminary analysis reveals possible relationships between privacy and security concerns, enactment of mitigations to alleviate those concerns, and perceptions of responsibility for the privacy and security of smart home devices. Example quotes for each concept are provided in the side bars.

Concerns

Participants were asked if they had any hesitations or concerns about their smart home devices during which time many participants, unprompted, discussed privacy or security. They were later asked explicitly about their privacy and security concerns. All participants acknowledged privacy concerns (12 unprompted). Concerns were either personally held or those they had heard others express, with 11

Privacy Responsibility

Personal responsibility: *"if you want your information protected, don't bring a camera into your house. If you want your information not to be put on the cloud, don't give the opportunity. So, I think that you are ultimately accountable. It's your information."* (P8_A)

Manufacturer responsibility: *"[Those responsible are] really the people who write the software that interact with the devices, people that write the firmware for the devices, and then the software that essentially runs in the cloud services that aggregates all of this data, and then performs functions. So you're really at their mercy."* (P11_A)

Government responsibility: *"voluntary consensus on privacy issues is almost impossible to get from the commercial sector. . . I think they need privacy guidelines at least from the government in order to adhere to them."* (P13_A)

being personally concerned. Fourteen voiced security concerns (11 unprompted, 10 personally concerned).

Despite having concerns, participants were more than willing to bring devices into their homes. For example, one participant commented, *"it's not gonna stop me from living my life. . . But we do take it into consideration the privacy aspects of things, but it's not to any extreme" (P6_U).*

Mitigations

Concern often, but did not always, translate into action. During the privacy and security portions of the interviews, participants were asked if they performed any mitigations to alleviate their concerns. Of the 11 who were personally concerned about privacy, nine discussed implementing mitigations. The most commonly mentioned privacy mitigations were: configuring privacy-related options (e.g., not sending usage statistics, disabling ordering) (6 participants); covering/repositioning cameras (3); and not putting listening devices in rooms where sensitive conversations could occur (3). Not surprisingly, among those four who were not concerned about privacy, only one implemented a mitigation.

Eight of the 10 participants who were personally concerned about security mentioned mitigations. The most frequently mentioned security mitigations included: password management (e.g., strong passwords and changing passwords on apps) (7); home network security (e.g., secure WiFi, network segmentation) (6), configuring security options on the devices (4), choosing devices with strong security features (3), and physical security of devices (2).

Security mitigations in particular demonstrated lack of understanding of mitigation effectiveness as well as confusion about the relationship between smart home devices and other activities such as social media, web browsing, and email. For example, when asked what smart home device privacy mitigations he takes, P4_A mentioned that he does not go on Facebook and tries to clean up old emails.

Household members also influence mitigations as was the case for four participants not personally concerned about privacy or security. One participant said, *"My husband is more security minded. . . The Alexa device has a video camera that you can use, but he's taped it over" (P1_A).*

Responsibility for Privacy

Participants were asked who they thought was responsible for protecting the privacy of information collected by their smart home devices. Responses included three different entities: themselves, device manufacturers, and the government, with only one participant saying they did not know. Responsibility was often viewed as being shared.

Eight placed partial responsibility on themselves. Two of those eight put sole responsibility on themselves. One such participant did not trust device vendors since *"the manufacturers' desires are counter to the consumer" (P16_A).*

Eleven believed manufacturers share some responsibility, with four of those claiming manufacturers have sole responsibility. For example, one participant remarked *"They need to do everything [since they are] taking so much money for all that" (P9_A).* However, even while putting some responsibility on manufacturers, participants do not completely trust them. When asked if he ever reads any of the privacy agreements, P10_A said, *"I don't have much trust in what companies say they collect and don't collect. I think they collect what they can and use it" (P10_A).*

Four participants felt that the government had some responsibility to regulate smart home device privacy along with manufacturers and/or themselves. One mentioned the European Union's General Data Protection Regulation as a

Security Responsibility

Personal responsibility: *"I'd like to see the vendors take more responsibility and take more action to secure their own devices. But because they don't always do that and I don't always necessarily trust them to do that, I take it upon myself to be responsible for the security of these systems."* (P15_A)

Manufacturer responsibility: *"They are the prime people who are responsible for things they're making because we're not putting all the time, and energy, and money on building that stuff. So, we really don't know what is inside of this."* (P9_A)

Shared responsibility: *"If you have stronger security features that the device offers the user doesn't use, that's kind of the user's fault. If it doesn't offer certain level of security, that's the manufacturer's fault."* (P10_A)

model the U.S. might consider smart home devices.

We found disparities between privacy responsibility, concern, and mitigations. For example, P6_U and P8_A said they were at least partially responsible for the privacy of their devices but were not personally concerned. Not surprisingly, P6_U did not perform any privacy mitigations. While P8_A did cover the cameras on some of his devices, he did so only due to prompting by his wife.

Personal responsibility appears to be a differentiator when it comes to privacy concern and mitigation. Of the eight participants who said that they were at least partially responsible for privacy, seven mentioned at least one mitigation they perform. Of the six who claimed no personal responsibility, only three discussed performing a privacy mitigation.

Responsibility for Security

When asked about responsibility for the security of their smart home devices, similar to privacy, participants mentioned themselves and manufacturers, but only one said government. Eight viewed responsibility as being shared.

Nine claimed that they had at least partial responsibility, with three of those taking sole responsibility. One smart home owner remarked, *"I think we've realized, sooner or later, your stuff will get breached. It's on you to either put extra restrictions in place or just be okay with the fact that it's going to happen" (P8_A).*

Nine participants said manufacturers have at least some responsibility for security, with two of those claiming the manufacturer has sole responsibility and six believing that both the manufacturer and user hold responsibility. For example, one participant remarked, *"I consider myself to be responsible for doing the best I can security-wise, but really it's the manufacturers and the people who develop the software that ultimately hold the keys to the security" (P11_A).*

Seven of the nine claiming personal responsibility discussed some kind of security mitigation. A participant who did not implement mitigations was personally concerned, but not knowledgeable enough to take action: *"It could be fairly simple to do something and protect myself, but I have no idea. . . I'm not going to educate myself on network security. . . This stuff is not my forte. I'm very accepting to the fact that it is what it is" (P8_A).*

Two participants claimed responsibility but were not personally concerned about security. Those not claiming personal responsibility were also not personally concerned about security, with only one mentioning a rudimentary mitigation (occasionally changing passwords).

Future Work and Contributions

We plan to complete the interview study, with a goal of 40 interviews total. We would like to especially recruit more non-administrative users to explore potential differences between those who install and administer the devices and those who may only use the devices. With this larger dataset, we will also continue to investigate possible relationships between privacy and security concerns, mitigation actions, and perceptions of responsibility as well as how those perceptions and experiences interplay with usability.

Future results can inform efforts to foster a sense of personal responsibility for privacy and security among smart home end users or encourage more manufacturer or government accountability in areas for which smart home users tend not to claim responsibility. By examining the sophistication of mitigations, we can also start to uncover areas ripe for improved usable privacy and security features that manufacturers can build into their devices by default, thus alleviating the need for users to take protective action.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

REFERENCES

1. Bill Ablondi. 2019. Connected Consumer: Chairpersons Opening Remarks. Strategy Analytics. Presented at the 2019 Internet of Things World Conference, Santa Clara, CA.
2. Parks Associates. 2019. State of the Market> Smart Home and Connected Entertainment. (jan 2019). Retrieved May 29, 2019 from `http://www.parksassociates.com/bento/shop/whitepapers/files/ParksAssoc-OpenHouseOverview2018.pdf`
3. Barney G Glaser and Anselm L Strauss. 2017. *Discovery of grounded theory: Strategies for qualitative research*. Routledge.
4. PwC. 2017. Smart home, seamless life. (jan 2017). Retrieved May 29, 2019 from `https://www.pwc.fr/fr/assets/files/pdf/2017/01/pwc-consumer-intelligence-series-iot-connected-home.pdf`
5. Statista. 2019. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). (2019). Retrieved May 31, 2019 from `https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/`
6. Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2017. Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 181–18109.
7. Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust me: doubts and concerns living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, 427–434.
8. Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 65–80.