Characterizing Misuse and Snooping in Home IoT Devices

Phoebe Moh
University of Maryland

Noel Warford
University of Maryland

Pubali Datta
University of Illinois

Nathan Malkin
University of Maryland

Adam Bates
University of Illinois

Michelle L. Mazurek
University of Maryland

Abstract

Internet of things (IoT) devices have become increasingly common in the home. While users have raised concerns about data collection and remote attackers, these devices are also potentially susceptible to misuse and snooping by others in the same physical space, such as housemates and visitors. There has been little work studying these insiders. To better understand what kinds of misuse and snooping IoT owners face in the physical space, we developed a characterization survey (n = 100) to broadly capture what kinds of misuse and snooping incidents participants have experienced or engaged in. Overall, 26 participants reported directly having either experienced or engaged in misuse or snooping within the past three years, and we observed a wide variety of misuse and snooping incidents. We plan to use the results from this survey to develop a second survey to assess – in a roughly representative sample of the U.S. population – the prevalence of the different classes of misuse and snooping incidents.

1 Introduction

Internet of Things (IoT) devices have seen widespread adoption in recent years. While home IoT devices benefit their users in many ways, the rapid adoption of IoT technology has also exposed new avenues that adversaries can take advantage of. Users have raised concerns about privacy and security in regards to the amount of data these devices collect from personal spaces, such as the home, and whether this data can be accessed by remote adversaries [5, 6, 9, 10].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

Although remote adversaries have the potential to inflict widespread damage, these attacks are relatively rare, and while data collection by distant parties such as manufacturers is fairly common, IoT devices are also susceptible to being accessed by others physically closer to the device, such as housemates or visitors. These insiders do not need the sophisticated skills and tools that remote adversaries employ and can instead act opportunistically to misuse these devices.

We broadly define misuse as when someone uses an IoT device in a way that the owner does not approve of, and we define snooping as when someone accesses private information or information that was not already known from an IoT device. While misuse and snooping have been well-studied in the context of mobile phones, there is little research in the space of IoT devices attempting to fully characterize the kinds of misuse or snooping users experience from insiders. In order to better understand the kinds of IoT snooping and misuse incidents that everyday users face, we ask the following research questions:

1. What kinds of snooping and misuse incidents do IoT device owners experience in the physical space? What devices do these incidents occur on?
2. What factors impact an IoT device owner or IoT device user's comfort (or lack thereof) with these incidents?

We explore these research questions through a primarily open-ended characterization survey. Using the observations from this survey, we are currently developing a second survey to measure the prevalence of these events in a representative sample of the population.

2 Related Works

Snooping in non-IoT contexts This study builds on previous works on snooping in the context of mobile phones. Muslukhov et al. investigated smart phone snooping by social insiders, such as friends and family. Specifically, 9% of participants reported accessing someone else's smart phone without

permission [8]. Marques et al. evaluated the prevalence of snooping in a larger population, with 31% of participants reported having looked through someone else's smart phone without permission in the past year [7]. Even when owners give permission to use their smart phones, unease around snooping persists [4]. Despite similarities in smart phones and IoT devices, there has been little work characterizing the range of snooping (and, more broadly, misuse) IoT owners experience.

Security and privacy concerns of IoT owners Home IoT devices have the potential to collect sensitive, personal information about the environment and its inhabitants. Naeini et al. found that individuals are less comfortable with IoT devices collecting data in a private setting, such as the home, versus a public setting, and 29% of participants stated that they did not want to share this data due to some perceived risk, such as identity theft or data misuse [9]. In a study on smart speakers, privacy concerns served as a deterrent to adoption among non-owners [5]. Owners and non-owners of smart TVs alike disapprove of manufacturers repurposing collected data for other uses, such as advertising [6]. While users have exhibited concern about what manufacturers and remote attackers can do with information collected by IoT devices, this information can be exposed to immediate parties through physical access.

IoT interactions in shared spaces Incidental users, who are exposed to but do not control smart devices, include housemates and visitors. Cobb et al. investigated the privacy concerns of incidental users, who can be unknowingly recorded by smart devices, and unearthed tensions between these users and device owners in regards to these privacy needs [1]. While incidental users and secondary users also have the potential to use and access the information stored these devices, works focusing on non-adversarial, multi-user smart homes have observed social norms as a powerful factor that inhibits bad behavior and decreases the need for access controls [2, 11]. However, Huang et al. found that while users have expressed concerns about smart speaker misuse by incidental users, they often adopted suboptimal risk management strategies [3]. Previous works have highlighted the potential for device misuse by incidental users or in shared spaces, and ours is the first to attempt to characterize these incidents.

3 Methodology

In order to better understand the characteristics of IoT misuse and snooping incidents, we created a primarily open-ended online survey (n = 100) to obtain a wide variety of responses on the the kinds of incidents that participants have experienced or engaged in, as well as what these participants considered to be acceptable or unacceptable in regards to their smart devices. Participants were recruited through Prolific and were required to reside within the U.S., be at least 18 years old, and fluent in English. Because we are interested in responses from both those who have experienced misuse or snooping on their own devices as well as those who have committed misuse or snooping on another person's device, survey participants were not required to own a home smart device. Participants were paid if they answered the attention check question correctly and their answers to the open-ended questions were on-topic. This study was approved by the UIUC Institutional Review Board (IRB).

We defined home smart devices as "internet-connected objects in your home, which can include lights, thermostats, smart assistants, and refrigerators. Oftentimes, these devices sense events in the home and change their behavior in response (for example, a doorbell camera that sends out an alert when it detects movement)." We excluded computers, laptops, tablets, cell phones, and cell phone assistants from this definition because these devices are inherently more personal than typical home smart devices and less likely to become shared devices when placed in the home.

The survey took an average of 12.4 mins (median 9.6 minutes). Participants were paid $5 each, which is well above the U.S. minimum wage and Prolific's suggested rates. The data collection took place in October and November of 2021, and we asked participants to recall events from the past three years. The survey consisted of 6 main sections:

1. **Instructions:** Participants were briefed about the study, presented with a consent form and definitions, and then asked about the smart devices in their home.

2. **Experiences:** Each participant was asked about whether they 1. noticed any unexpected changes or behaviors in one of their devices after someone used it, 2. had one of their devices used in a way that they did not expect, 3. were snooped on through one of their devices, 4. used someone else's device while the owner was not watching, or 5. used someone else's device to snoop, as well as which kinds of devices these incidents occurred on.

3. **Drill-down:** If the participant had experienced or engaged in at least one of the topics of interest above, we selected one of these reported topics at random to ask follow-up questions on what happened and how the participant felt about it.

4. **Secondhand stories:** If the participant had no experiences of interest, we asked if they had heard of an acquaintance experiencing something similar. If they did, we asked them to describe the event as best as they could.

5. **Privacy expectations of smart devices:** Participants were asked to describe the kinds of actions they were comfortable and uncomfortable with being performed on their own and others' devices, as well as their comfort with visitors using their devices.

6. **Demographics:** The survey concluded with demographics, a sample of which is shown in Table 2.

For open-ended answers, we performed qualitative analysis by developing a codebook to draw out common themes. Two researchers collaboratively and inductively coded 10% of the responses to develop an initial codebook. They then independently applied the codebook to an additional 10% of responses until strong reliability was reached at three rounds (average Cohen's kappa = 0.84). Afterwards, each coder independently coded about 65% of the remaining responses, and the overlapping responses (21) were used to re-evaluate reliability of the codebook. Inter-coder reliability on these 21 responses showed an average Cohen's kappa of 0.75 and an average Kupper-Hafner concordance of 0.82.

4 Limitations

Due to social desirability, participants may not disclose engaging in snooping. We attempted to mitigate this through assurances that responses would be kept anonymous. We asked participants to recall events from a relatively large timeframe (three years) to compensate for the COVID-19 pandemic limiting opportunities for interacting with home smart devices, which may have impacted recall accuracy. In addition, choosing one topic at random for participants to recall means that we could not capture every one of a participant's experiences, but this was deemed acceptable because we sought a broad range of misuse and snooping stories experiences rather than a precise estimate of prevalence. Finally, our small sample size makes it difficult to make conclusive claims on prevalence regarding home IoT misuse and snooping.

5 Results

The number of participants that reported having experienced each topic of interest, along with the types of devices, are shown in Table 1. Overall, smart TV's and smart speakers are the most commonly misused and snooped on devices, but they are also the most common devices owned by our sample, whose demographics are shown in Table 2.

Of our 100 participants, 44 elaborated on one of their experiences in the drill-down section. Not every response was directly related to misuse or snooping: 26 responses described events that qualified as misuse or snooping. In some cases, it was unclear if an incident counted as misuse due to not knowing the device owner's thoughts, so we opted not to include these in our count. Of the 56 participants that did not have a personal experience to report, 13 had a secondhand story of IoT misuse or snooping. Of those responses, seven fell under our definition of misuse and snooping.

We observed 14 broad categories of misuse and snooping incidents among respondents, shown in Table 3. These responses covered a wide range of severity, from simple pranks

		Count
Had a device used without supervision (84)	Smart TV	62
	Smart speaker	55
	Smart home management	22
	Smart camera	17
	Standalone smart appliance	10
	Smart security	7
	Other	3
Had a device used in an unexpected way (11)	Smart TV	8
	Smart speaker	5
	Smart home management	2
	Smart security	2
	Standalone smart appliance	1
	Smart camera	1
Noticed unexpected device changes after someone used it (8)	Smart home management	3
	Smart TV	3
	Smart speaker	3
	Smart camera	2
Experienced snooping on a devices (7)	Smart speaker	5
	Smart TV	2
	Smart camera	1
Used someone else's device without supervision (23)	Smart speaker	19
	Smart TV	14
	Smart home management	5
	Smart camera	3
	Standalone smart appliance	2
	Smart security	2
Snooped on someone else's smart device (13)	Smart speaker	6
	Smart TV	5
	Smart camera	4
	Smart security	2
	Smart home management	1
	Standalone smart appliance	1

Table 1: Reported experiences, with participant count in parentheses.

("I asked Alexa to add something silly in the shopping cart for the person's amazon account," P99) or long-terms spying ("My ex was able to extract sensitive personal information on me based upon the conversations i was having privately when she wasnt around," P65). Finally, we group the wide variety of factors that contributed to a participant's comfort or lack of comfort with an incident into 5 categories. We observed similar themes in the "Privacy expectations of smart devices" segment of our survey, which all participants responded to.

- **Owner/user relationship:** Some participants were comfortable with their devices being used without supervision because of trust with the other party, and some participants who engaged in misuse or snooping said they were comfortable because they were close with the owner and felt that they would not be upset.
- **Intent:** Some participants that engaged in snooping and misuse cited events being accidental or having no malicious intent behind their actions as reasons for their own

		Count
Gender	Women	51
	Men	48
	Nonbinary	1
Age	18-29	57
	30-39	27
	40-49	9
	50-59	6
	60+	1
Own at least one...	Smart TV	74
	Smart speaker	69
	Smart home management	42
	Smart camera	36
	Smart security	19
	Standalone smart appliance	12
	Other	5

Table 2: Participant demographics.

comfort with what happened.

- **Event perception:** Participants who experienced misuse or snooping listed events being unsurprising or easily reversed as reasons for comfort, whereas events being surprising were a reason for discomfort. Participants that engaged in misuse or snooping reported feeling comfortable because they perceived the event as funny.
- **Information sensitivity:** Both participants that experienced and participants that engaged in snooping expressed comfort with certain events because they did not consider the revealed information to be sensitive. Some participants expressed discomfort with seeing or having new, unexpected, or more personal information revealed.
- **Consequences:** Lack of long-term consequences was cited as a cause for comfort for both participants that experienced misuse and engaged in misuse. On the other hand, events that lead to a perceived violation of privacy was a reason for discomfort in both parties.

6 Discussion

Of note, 13 participants reported having engaged in snooping, whereas seven reported having experienced snooping. We hypothesize that device owners under-report incidents of being snooped on because these incidents go entirely unnoticed. While we cannot make conclusive claims about the prevalence of misuse or snooping incidents due to our small, non-representative sample, we do note that our observed proportion of participants with direct experience as reported by the drill-down section (26/100) is similar to the rate of phone snooping (31%) that Marques et al. reported [7].

Code	Description
Entertainment (7)	Accessed some form of entertainment media, such as games, music, videos, or streaming services.
Private information accessed (7)	Accessed private information stored on a device.
Prank (7)	Pulled a prank. *This code is used in conjunction with another code to describe the consequences of the prank.*
Access control change (3)	Changed access controls on the device, such as by adding an unauthorized user or changing pass codes.
Broken device (3)	Stopped working properly after use due to physical or software issues.
History accessed (3)	Accessed search, viewing, or action history on a device.
Spying (3)	Monitored someone without their knowledge, longer-term than "Eavesdropping".
Account logout (2)	Logged out of an account.
Add information (2)	Added non-personal information to the device, like items to a shopping cart.
Eavesdropping (2)	Learned the contents of an interaction (audio or rext), shorter-term than "Spying".
Accidental connection (1)	Accidentally connected to and used a device that does not belong to them.
Device shared (1)	Physically shared device without permission.
Environment change (1)	Changed physical environment with device.
Unexplained behavior (1)	Unexplained behavior triggered.
Not of interest/ambiguous (24)	Event is not directly/ambiguously related to misuse or snooping.

Table 3: Experiences from the drill-down and secondhand stories segments, with combined participant counts. Multiple codes are possible for a single incident.

7 Conclusion

Home IoT devices have the potential to be misused or snooped on, but it is unclear what kinds of misuse or snooping IoT owners experience or how they feel about it. In this study, we use survey methodology to broadly understand what the wide variety of incidents users experience, ranging from fairly innocuous events like accidentally connecting and using a speaker to graver events like long-term spying. We are currently using the results of this study to create and deploy a second survey to measure the prevalence of these incidents in a larger, more representative population sample.

Acknowledgments

This research is supported primarily by the National Science Foundation under NSF award numbers CNS-1955805, -1955172, -1955228, -1955231.

References

[1] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. "i

would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 2021(4):54–75, 2021.

[2] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[3] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. *Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks*, page 1–13. Association for Computing Machinery, New York, NY, USA, 2020.

[4] Amy K. Karlson, A.J. Bernheim Brush, and Stuart Schechter. Can i borrow your phone? understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, page 1647–1650, New York, NY, USA, 2009. Association for Computing Machinery.

[5] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), nov 2018.

[6] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "what can't data be used for?": Privacy expectations about smart tvs in the u.s. 01 2018.

[7] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 159–174, Denver, CO, June 2016. USENIX Association.

[8] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Know your enemy: The risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '13, page 271–280, New York, NY, USA, 2013. Association for Computing Machinery.

[9] 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 *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA, July 2017. USENIX Association.

[10] 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, Santa Clara, CA, July 2017. USENIX Association.

[11] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in Multi-User smart homes: A design exploration and In-Home user study. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 159–176, Santa Clara, CA, August 2019. USENIX Association.