

Characterizing Misuse and Snooping in Home IoT Devices

Phoebe Moh (UMD), Noel Warford (UMD), Pubali Datta (UIUC), Nathan Malkin (UMD), Adam Bates (UIUC), Michelle L. Mazurek (UMD)



Motivation

IoT devices are vulnerable to misuse and snooping by housemates and visitors, but little research has been done to assess what **kinds** of incidents happen or how **often** this happens.

Research Questions

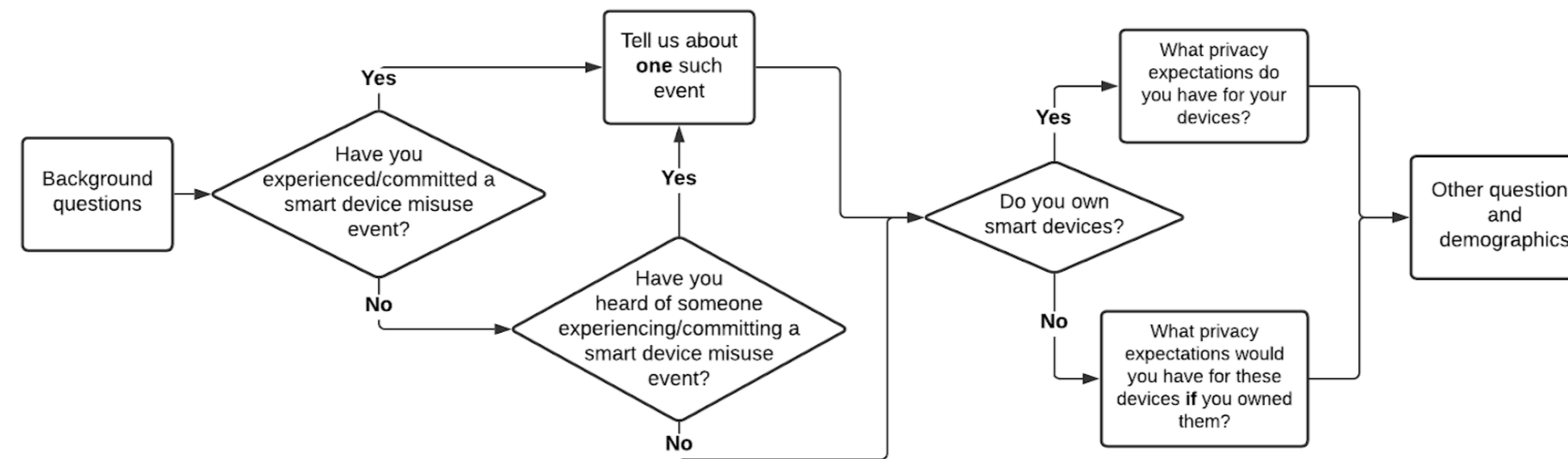
RQ1: What kinds of misuse and snooping incidents do IoT owners and users experience?

RQ2: What factors impact an IoT owner or user's comfort (or lack thereof) with these misuse and snooping incidents?

Methods

Developed a primarily open-ended survey

Recruited 100 participants for an online survey through Prolific



Used inductive qualitative coding to identify themes in responses to open-ended questions.

Results

44 participants elaborated on an incident, 33 (26 direct experiences, 7 secondhand experiences) were categorized as misuse or snooping:

Entertainment (7)	Private info accessed (7)	Prank (7)
Access control change (3)	Broken device (3)	Device history accessed (3)
Spying (3)	Account logout (2)	Add information (2)
Eavesdropping (2)	Accidental connection (1)	Device shared (1)
Environment change (1)	Unexplained behavior (1)	Not of interest (24)

What made participants (un)comfortable with misuse/snooping?

Factor	Example
Owner/user relationship	Device owner was a friend vs a stranger
Intent	Misuse was accidental vs purposeful
Event perception	Event was expected vs surprising
Information sensitivity	Information was not considered sensitive vs deeply personal
Consequences	Event was easy to undo vs irreversible

Discussion

- We observe a wide variety of misuse and snooping across many devices.
- Can't make conclusive prevalence claims, but incidence of misuse/snooping events (26/100) is similar to estimates of phone snooping (31%) by Marques et al.
- Asking participants to recall experiences through open-ended questions may have impacted response rate.
- More participants reported engaging in snooping (13) than experienced snooping (7), suggesting that snooping is unidentified by victims.

Next Steps

Use observed experiences to develop a second survey and assess the prevalence of home IoT misuse and snooping incidents in a representative population sample