Security and Privacy Perspectives of People Living in Shared Home Environments

NANDITA PATTNAIK, SHUJUN LI, and JASON R.C. NURSE, University of Kent, UK

Security and privacy (S&P) perspectives of people in a multi-user home are a growing area of research, with many researchers reflecting on the complicated power imbalance and challenging access control issues of the devices involved. However, these studies primarily focused on the multi-user scenarios in traditional family home settings, leaving other types of multi-user home environments, such as homes shared by co-habitants without a familial relationship, under-studied. This paper closes this research gap via quantitative and qualitative analysis of results from an online survey and qualitative content analysis of sampled online posts on Reddit. The study explores the complex roles of shared home users, which depend on various factors unique to the shared home environment, e.g., who owns what home devices, how home devices are used by multiple users, and more complicated relationships between the landlord and people in the shared home and among co-habitants. Half (50.7%) of our survey participants thought that devices in a shared home are less secure than in a traditional family home. This perception was found statistically significantly associated with factors such as the fear of devices being tampered with in their absence and (lack of) trust in other co-habitants and their visitors. We observed cyber-physical threats being a prominent topic discussed in Reddit posts. Our study revealed new user types and user relationships in a multi-user environment such as *ExternalPrimary-InternalPrimary* while analysing the landlord and shared home resident relationship with regard to shared home device use. Based on the results of the online survey and the Reddit data, we propose a threat actor model for shared home environments, which has a focus on possible malicious behaviours of current and past co-habitants of a shared home, as a special type of *insider threat* in a home environment. We also recommend further research to understand the complex roles co-habitants can play in navigating and adapting to a shared home environment's security and privacy landscape.

CCS Concepts: • **General and reference → Empirical studies**; • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**; • **Information systems → Social networks**.

Additional Key Words and Phrases: Privacy, Security, Multi-User, Shared home, Online social network, Threat Model, User behaviour, User perspectives, Empirical study, Rental home security, Bystander, Smart home, Smart device, Survey, Demographic analysis, Contextual analysis

ACM Reference Format:
Nandita Pattnaik, Shujun Li, and Jason R.C. Nurse. 2024. Security and Privacy Perspectives of People Living in Shared Home Environments. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW2, Article 368 (November 2024), 39 pages. https://doi.org/10.1145/3686907

1 Introduction

"*I have a smart house set up, Hue and Cync lights, Ring doorbell, myQ garage, Nest Thermostat and a Nest Hub Max in my room. One of my roommates moved out on bad terms and still has legal rights to access our shared property when I am not home. How can I control his access so that he can only have*

Authors' Contact Information: Nandita Pattnaik, np407@kent.ac.uk; Shujun Li, S.J.Li@kent.ac.uk; Jason R.C. Nurse, J.R.C.Nurse@kent.ac.uk, Institute of Cyber Security for Society (iCSS) & School of Computing, University of Kent, Canterbury, UK.

This work is licensed under a Creative Commons Attribution International 4.0 License.

© 2024 Copyright held by the owner/author(s).
ACM 2573-0142/2024/11-ART368
https://doi.org/10.1145/3686907

access to my smart light and nothing else when he enters my home in my absence? I don't want him spying on my stuff."[1] The scenario paints a typical privacy issue faced by a shared house resident posted on the social media platform Reddit. It depicts a picture of how the traditional notion of household life is changing fundamentally from a closed, physical and private space to a hybrid half-public and smart living place characterised by 'digitalization, connectedness, smartization and automation' [92]. This increasing digitisation is powered by the growing adoption of multiple smart and other traditional devices by household members [77]. For instance, a 2020 report from the British telecommunications operator BT [12] stated that an average UK household possesses 28 connected devices on average. This burgeoning use of computing devices by home users brings about various security & privacy (S&P) related challenges, which have been widely discussed in the research literature [1, 8, 41, 47, 49, 83, 90, 91, 93]. One of the primary factors contributing to the S&P challenges of this growing conglomeration of devices is the number of users that own/use/share those devices. According to a piece of research by the Pew Research Center in 2020 [40], the average household size was 4.9 around the world, although this varies sharply regionally. The issues and challenges of a multi-user modern smart home are a subject of active research. Studies have focused on different topics while exploring this subject, which includes topics on different types of multi-user relationships while using those devices [1, 17, 24, 53, 91], on the challenges and concerns they face [6–8, 24, 36], on user awareness and perceived norms [1, 50, 89] and on mitigation techniques [1, 18, 31, 41, 82, 89].

However, the **context of most of these discussions principally referred to traditional family home settings**, where household members mainly include family members, visitors such as friends and guests, and people providing on-site household services such as nannies. This leaves a whole range of different non-family contexts that have not been covered by past research. For example, *hybrid and extended homes* [92] where the definition of the home is more detached from a physical geo-location, *pseudo-homes* [67] covering people who split their stay between two or more regular sites (e.g., students who live in their parent's house during term breaks and at university accommodation during term time), and *shared homes* [45] where not all co-habitants are related by a familial bond, has not been addressed in past research as separate non-family contexts. These non-family home settings could lead to different types of S&P concerns of users in comparison with family settings. In most traditional family-home settings, we have observed that the primary users have more overall control of the home devices [24, 90] and, therefore, are the likely vulnerable points in home security. In a non-family home, each participating user is considered a primary user, and consequently, each of those primary users could expose the S&P vulnerability of the shared home. Moreover, with the presence of multiple primary users, the negotiation of S&P behaviours becomes trickier in a shared home environment. Additionally, each co-habitant might possess their own set of devices, such as a smart camera, adding not only to the number of devices and consequent S&P vulnerabilities of a multi-device context but also creating potential new S&P issues for other more passive users of such home devices. The S&P perspectives of home users in these settings, therefore, should be researched separately from the users who live in a family setting.

Past research [85] has commented on the passing about concerns of shared home residents on physical safety and reluctance to stay in shared housing due to privacy concerns. However, there is a lack of research to understand S&P-related multi-user issues and challenges that users of such houses might encounter as these types of households reflect a different way of living in contrast to the normativity of the nuclear family [46]. For example, the multi-user relationships concerning

[1]The message is rephrased to be different from the original message while keeping its essence. This is necessary to avoid re-identification of the author of the post via a simple online search as part of our research ethics application approved by our university.

user roles and power imbalances, i.e., between the primary and secondary users as defined in a traditional family unit [1, 17, 24, 53, 91] might not be applicable to a shared home owing to the existence of multiple primary users for common shared devices such as routers, smart locks or smart lights. The S&P issues and concerns of the users in a non-family setting are affected by the fact that each co-habitant in a shared home setting often presents a different circle of outsiders; hence, the possible S&P risks and threat actors in a non-family shared home setting are more likely higher than those in a family home setting. Furthermore, past research [60] has highlighted how shared home living requires more frequent and dynamic negotiations about privacy boundaries in terms of domestic space or practices, unlike users in a family home setting, which raises the question of how these negotiations could influence S&P behaviours of users in such non-family shared home settings. Approaches to S&P vary depending on the context where it is experienced [88]. Therefore, a thorough understanding of S&P perspectives in various contexts is important to derive a comprehensive S&P-related understanding regarding the users in multi-user homes.

This study, therefore, specifically focuses on the non-family S&P perspectives of shared home users, as this type of shared living are becoming more common in some parts of the modern society with more people living in for a longer period and across a widening age demographics [45]. Such shared homes offer social, economic, and environmental benefits to their co-habitants and society as a whole. Similar evidence has been reported by others, e.g., a 2023 research paper Ronald et al. [72] reported that housing options such as shared accommodation and commercial co-living are fast becoming popular and increasingly institutionalised in European cities [72] and the number of HMOs (houses in multiple occupations) increased by 22% in 2021 from 2020 in London [25]. This trend of increasing shared housing is seen globally in many countries and regions such as the UK [84], Europe [80], Japan [23], and New Zealand [16], especially in large cities. One interesting aspect of this type of household is the diversity of the household members. According to recent data from a popular room share website as reported in a 2022 article on the BBC Magazine [59], the number of people who preferred to live in shared homes increased across different age bands, e.g., as much as 239% for 55-64-year-olds, 114% for 45-54-year-olds, 161% for 65-year-olds, and 106% for 35-44-year-olds. S&P perspectives of people living in these homes, therefore, could help improve our understanding on cyber security and privacy aspects in such special types of home environments with multiple users from different backgrounds who often share many different devices. We therefore defined the following two research questions for our work.

- **RQ1**: What are the S&P awareness and behaviours of people living in a shared home?
- **RQ2**: What S&P concerns are experienced by shared home co-habitants, and which threat actors are the likely sources of these concerns?

The above research questions were studied using a mixed research method: an online survey and analysis of data collected from a popular online forum (Reddit). The main **findings and contributions** of the paper can be summarised as follows.

(1) The results of our online survey showed that most of the survey participants (85%) in a shared home reported trusting their co-habitants, but almost 50% of them felt that a shared home setting is less secure compared to a traditional family home.
(2) We found that the S&P behaviours, issues and corresponding S&P negotiations in a shared home setting could be very complex, with many primary users for the same shared home devices, possible security threats from visitors of each inhabitant and ownership of multiple computing devices by most shared home residents.
(3) The study also demonstrated the unique role of the landlord in most scenarios, where they are a primary user of some home devices from outside of the shared home. For instance, most people in a shared home equipped with shared smart devices owned by their landlords were

never provided with any details of the nature of data collection, storage, or sharing and never signed any agreement in relation to this.

(4) We found cyber-physical harm to be a frequent theme amongst those residents who were concerned about their co-habitants in many shared homes. These inhabitants were afraid of physical harm from their cohabitants, often exacerbated by the use of in-home smart devices, and were looking for a smart solution to the problem.

(5) The study highlighted different S&P perspectives of multiple device users in a shared home. For instance, it revealed the co-existsnce of different types of primary users of some devices, the balance of power between the co-habitants that exist in such a context, and the operational/usage problems that might arise due to the clash of multiple primary users.

(6) We proposed a customised threat actor model highlighting different insider threat actors in shared homes, including the landlords as a special type threat actor outside of the home and beyond home threat actors whose involvement is specific to shared home settings. The inhabitants' level of trust fluctuates depending on the known and unknown elements of the actors involved.

The rest of the paper is structured as follows. The next section further articulates the background and reviews related work. Section 3 discusses the methodology adopted, followed by results described in Section 4. The last section discusses our study's important takeaways and limitations and gives future research directions.

2 Related Work

There has been a robust growth of research interest in the area of multi-user smart homes focusing on different contexts, behavioural aspects, concerns, and challenges in relation to home users' S&P perspectives. This section highlights the focal points of related research where home users' S&P perspectives in a multi-user home were explored, primarily in traditional family home settings.

2.1 Awareness & Behaviours of Users

2.1.1 Focus on Different Types of Users: Several of the studies [31, 35, 41, 43, 47, 90] focused on the influence and impact of different types of users in a multi-user home environment. Depending on their ownership, control and use of the devices, different user types were defined. *Primary users* were defined as the user who owns/install/set up, and manage the computing devices at home. *Secondary users* came under the categories of users who do not possess ownership/configuration control on the devices, have either very little or no control over the management, but use the devices and/or are affected by the use of such devices by other users. Researchers used various different terms to describe such users, such as *bystanders* [1, 7, 17, 50, 52, 53, 87, 89], *incidental users* [17, 58, 90], and *passenger users* [38]. Some studies [15, 35, 41, 66] examined both primary and secondary users' points of view.

2.1.2 Power Dynamics between Different Types of Users: McKay and Miller [56] focused on the extreme cases of power imbalance in a multi-user home. They described how the abusers in an abusive relationship use different smart devices and try to control the home environment, i.e., temperature, hot water, and lighting, to exert their power on the other individual(s). They explained the monitoring behaviour of the abusers by using audio recording or camera surveillance and spoke about a 'technocratic attitude' of the abuser, who, according to their data, is predominantly male, ignores the victim's discomfort, and follows a pattern of increasing technology use.

Unlike studies on controlling abuser behaviour and that of controlled victims [42, 56, 75], most research [1, 24, 38, 47, 89] reflected on the power imbalances by exploring the positive negotiation of main users and passive acceptance of secondary users. Koshy et al. [38] used a theoretical framework

(domestication theory [30]) and stated this relationship as a spectrum where the pilot users try to accommodate the passenger users while at the same time giving priority to their own needs. Ahmad et al. [1] proposed a novel concept of 'tangible privacy', which is built around the framework of Altman's Privacy Regulation theory [5] and privacy as Contextual Integrity theory[62]. Ahmad et al. [1] observed that it is natural for bystanders to follow the familiar interpersonal boundary regulation mechanism to manage their privacy with IoT devices when with other people. However, in the absence of a tangible privacy mechanism from the devices, there is a mismatch between perceived privacy and actual privacy, creating uncertainty in the negotiation process. Geeng and Roesner [24] highlighted the role of smart home device drivers, presented an account of the power dynamics at play in a multi-user home while focusing on key topics of types of tensions, the reason for exacerbation of the tension and ways of mitigation techniques during different phases a smart device life and thus added temporal dimension to the analysis as well.

Bernd et al. [7] explained how the power dynamics between the bystanders (i.e., nannies) and owners motivate and constrain the privacy choices of the bystanders. They explained how the presence/absence of cameras at work could motivate acceptance/refusal of a job offer or sometimes constrain their choice of leaving a job, discussing/negotiating about their job. Bystanders and residents' behaviour, their different privacy perceptions, coping strategies to protect their environments, and the kind of information shared between them were all explored in a series of related papers [50, 51, 53, 54]. Marky et al. [51] found that residents have clearer knowledge about the data collection nature of the devices and fewer misconceptions compared to the bystanders.

2.1.3 Shared Devices & Consequential Actions: We noticed S&P discussions in a multi-user home were based primarily on two different types of smart devices, such as devices developed to be used by all members of a household, such as smart thermostats, smart cameras, smart bell or smart locks, and devices which are owned individually but can also be shared at times such as smart speakers/hubs. Although most studies focused on specific smart devices such as smart speakers [1, 27, 31, 35, 41, 89, 91], smart thermostats [17, 24, 38, 56] and smart cameras [7, 58] also had a fair share in the multi-user S&P research. Malkin et al. [47] mentioned how users in a multi-user home might inadvertently share search questions, listening preferences, or other personal data with others while using smart speakers. Lau et al. [41] recommended smart device companies to adopt multi-user-oriented user experience design interface. Moh et al. [58] reflected on the common S&P behaviour in a multi-user home by characterising the accidental or intentional unauthorised use of IoT devices by the residents while being shared.

Few of the past studies investigated the tensions or concerns of sharing traditional devices such as laptops and personal computers (PCs) [43, 87] along with smart devices. Among other studies, Lin and Parkin [43] explored the area of transferability of privacy behaviour between traditional computing devices and modern smart devices to find out how individuals with set privacy habits for traditional devices tend to adopt the same behaviours for smart devices as well. Several studies reflected on the nature of sharing traditional devices such as laptops and mobile phones in multi-user contexts. Matthews et al. [55] pointed out the messiness and varied ways of sharing a laptop or mobile phone, the commonness of sharing devices such as mobile phones and computers within family home environments, and the influence of trust and convenience. In their 2022 SoK (systematization of knowledge) paper, Wu et al. [88] mentioned 'access to shared resources' as one of the four key S&P behaviours in the social cyber security literature and reflected on the fact that the sharing percentage is higher for desktop computers than for laptops. Studies have explored the views of romantic partners [65] and cohabiting couples [33] in connection with account and device sharing. Several studies [14, 37, 68] investigated the intent behind device sharing to understand the underlying reason for sharing and the implications of sharing by individual users. However,

these studies lack a focus on examining users in a non-family shared home setting. Exploration of sharing habits includes strangers, acquaintances, colleagues [68], guest [14], and friends [37], mainly in a family home context. There is a lack of research focusing on S&P behaviours of shared home users concerning traditional computing devices. A specific research focus on understanding how home users behave in different non-family shared households is, therefore, an important topic.

2.1.4 Contextual Behaviours: The concept of contextual behaviour has been discussed in detail by many different researchers. Bernd et al. [7] as discussed above, has explained the privacy behaviour in a multi-user home from different contextual angles of the home, work, and a parental point of view and Yao et al. [89] observed that bystanders, as opposed to owners of smart devices, faced strong contextual variations as their interface with the devices varies quite prominently depending on places they visit (i.e., friends home as visitors, employees like nannies at their employer's house or even user in an Airbnb place) and the time period they spent time on such devices. Windl and Mayer [87] expressed similar views to Yao et al. [89] when they observed that bystanders privacy behaviour/concerns changed depending on the context of the device in use. Ahmad et al. [1] showed that contextual integrity shapes the privacy perception of the user about the devices in use and privacy violation occurs when there is a mismatch of expectation of device function/behaviour against the actual data collected by the device. He et al. [27] presented different contextual factors such as time of the day, location of a device, and age of the person, which decide the capabilities of a device being used.

2.2 Multi-user Home: Issues & Concerns

User behaviour and concerns are, to a certain extent, intertwined with each other in such a way that discussing one invariably refers to the other. While discussing the camera-related concerns for nannies about how the cameras spy on them or use illegitimately to record them, it was inevitable to discuss the S&P behaviour of the owners as well [7, 8] as it was the behaviour of the owner which bought on the said concerns. Bernd et al. [7] reflected on the complex contextual bases of home and workplace where the nannies have the challenges of balancing their own privacy expectations, their limited ability to make choices or express preference and that of the existing parental/employer/homeowner prerogatives. Other studies [18] have found that device owners are often willing to accommodate the incident users, but incidental users have varying degrees of concern and frustration depending on the type of devices.

Smart device-related concerns were very prominent amongst the IPA victims [42], who were concerned about the shared nature of smart devices, providing the possibilities of shared accounts, log views, and remote surveillance access by the abusers. As mentioned in the sub-section 2.1, Windl and Mayer [87] highlighted the concept of a 'skewed privacy concern' where the bystanders considered the laptops and personal computers significantly less privacy-concerning than the smart devices owned by the owners.

With the increasing facilities of sharing single, smart devices with multiple people, access control becomes one of the most important challenges in a multi-user home. Many of the multi-user studies [24, 27, 35, 91] have explored the area to discuss the level of granularity, the device-centric model, contextual dependencies, flexibility, user agency, balancing usability and complexities, etc. in relation to the topic of access control. Zeng and Roesner [91] proposed different types of access control systems such as role-based, location-based, supervisory, and reactive based on the device capabilities and other factors involved, whereas He et al. [27] added different contextual factors such as age, location of the device to the device capabilities and user relationship mix, suggesting these would better capture the user preferences and hence should guide the granular access control policy rather than the device itself. Jang et al. [35] used various scenarios to explain how access to

information in a smart device could be categorized as high/medium or low risk depending on the device and the user and recommended the need for fine-grained access control.

2.2.1 Insider Threats and Adversarial Settings: The intensity of the issues and concerns in a multi-user home is examined and reflected in a variety of spectra, starting from mild annoyance/conflict between the home users to the extremes of intimate partner violence (IPV) facilitated by smart devices and digital technologies. He et al. [27] pointed out the scarcity of research in identifying and discussing internal threats. Research on adversarial settings at home and *insider threats* has been touched upon by few studies to mainly point out the glaring absence of research in this area [74]. Many studies [42, 56, 75] have looked into how the smart devices facilitated homes, enabled the abusive behaviour inside the home, and discussed in detail the victims' concerns and the surrounding issues. On the other end of this spectrum, there lie several reasons, such as wilful disobedience [27] to exacerbation of existing power driver dynamics [24] or unintentional access denial [90], for the inhabitants of a household which might be exhibited in mild threat-like behaviour inside a smart home.

Our study endeavours to shed light on this area, keeping in mind that inter-user relationships in a shared home are different from those in a family home, and the power dynamics in such homes are not similar, affected by many different factors and contexts.

2.3 Multi-user Home: Coping Strategies

Several studies discussed the mitigation techniques either by reflecting on how users manage, protect, and prevent S&P violations in a multi-user home or by suggesting/recommending ways to protect. Huang et al. [31] discussed how the users follow either an 'Avoidance' or an 'Acceptance' strategy to cope with concerns from other members of the households or visitors. Various coping strategies were mentioned by Yao et al. [89] while they explored the concept in relation to both the bystanders and the owners. Potential techniques that the bystanders wanted to use included switching off the device, deleting/jamming the data collection, adapting to what is available, or no strategy at all. Owners, on the other hand, considered the placement of the device and selective assignment of information as their coping strategies. Conversation and negotiation as a strategy was mentioned in many different studies [1, 24, 89]. Ahmad et al. [1] study result on coping mechanism was reflected in line with the categorisation of Altman [5], i.e., 'filtering', 'ignoring', 'blocking', 'withdrawal', and 'aggression'. Privacy resignation is a common theme that appeared in many of the related studies [7, 41, 53].

The majority of the above discussions floated around the traditional family home settings, reflecting on the relationship between spouses, parents and children, friends and visitors to family, or employees working for the family. Some of these research data [1, 24, 31, 41, 91] did include shared home residents such as the roommates in their datasets, but none of the studies specifically focused on shared home settings to understand the S&P behaviour and attitude of the inhabitants that might be peculiar to the occupants in such environments. More often than not, the people living in shared homes are often not connected by familial bonds, and hence, the ties, trust, understanding, and obligations between the members of a shared home are different in comparison to a family home. Thus, it is important to study whether these differences are reflected in their S&P behaviour and attitude and whether they give rise to a different set of concerns and issues.

2.4 Research Gaps Identified

The above-summarised literature demonstrates a wide variety of research has been conducted on users in multi-user homes and their perception of S&P-related issues and concerns. However, the context of research, as seen, has primarily been on users of family homes. Several past studies [31,

35, 53, 91] did include users of non-family homes in their analysis to evidence the varied multi-user home settings. Focusing on access control issues in a multi-user home, Zeng and Roesner [91] commented on roommates' respect for each other's space. Huang et al. [31], as part of their discussions on users' concerns and coping strategies on shared smart speakers in multi-user homes, included some data from non-family households reflecting on trusting issues and how roommates in a multi-user scenario use shared smart speakers as coping strategies. While discussing the challenges of sharing smart devices in a multi-user household, Jang et al. [35] highlighted a typical non-family household scenario and the possibilities of having alternate primary users. Geeng and Roesner [24], who focused on understanding the tensions and cooperation among users of a multi-user home during different phases of smart device use, expressed their difficulties in being able to recruit a large number of non-family households.

Although some past studies considered non-family household scenarios, they were always researched and presented as '*part of*' a bigger picture, i.e., a multi-user household with family and non-family rather than studied '*holistically*' to understand the S&P nuances of the users living in these settings as a separate group. The specific S&P impact and implications that a non-family home context as a whole might exhibit are certainly worth more investigation. As mentioned in Section 1, this type of shared home would possibly always have multiple primary users for shared devices, several passive users of devices which might be bought by other users in the house, constant possibility of exposure of their devices to outsiders, i.e., friends of friends with whom they might not be familiar with and/or probable past/ex-users who might be privy to the detail S&P settings if appropriate care has not been taken. The current research aims to fill such research gaps.

3 Methodology

As reflected from the research questions described in the Introduction section, our study aims to understand the S&P perspectives, including awareness, behaviours, and concerns of co-habitants in shared home environments. We decided to collect our data from two different sources: data collected via an online survey and user-generated content (UGC) from an online platform. There were several reasons behind the decision to use the two different sources of data. First, usability security and privacy (USP) studies generally use traditional empirical methodologies, i.e., surveys and interviews. Since our study falls under such a category, we chose online surveys as our first choice of data collection. Second, we know that survey responses can be biased by the questions of the researchers and also by the survey respondents' desire to submit an answer that fits the norm. We, therefore, decided to collect additional data from a real-world online platform, which was collected in a passive manner so that there was no influence of the researchers [71, 76]. We wanted to find out whether there are any S&P-related online discussions with regard to the shared home environment and, if there are some, to investigate the nature of such discussions. Throughout this paper, whenever we use the term 'dataset', it will include both the survey data and the data collected from the online platform.

3.1 Collecting Online Data

Among multiple online platforms, we decided to choose Reddit. There were a few reasons behind this choice. 1) Reddit is a highly popular online forum with 52 million daily active users, active on over 3.5 million different communities called subreddits [10], each devoted to discussing a different subject. So, the probability of getting relevant data on our chosen topic was high. 2) Reddit is one of a few online platforms that have been actively studied [69] by many researchers due to the richness of UGC [64, 81]. 3) Past research [34] has shown that Reddit is a valuable platform for getting high-quality data from a diverse population with good measurement reliability inexpensively.

To collect online posts relevant to our research questions, we first needed to select one or more relevant subreddits related to S&P aspects of home users and then relevant Reddit posts on selected subreddits. To this end, we first searched on Reddit using the keyword "Home Security" to find relevant subreddits. Out of the 56 returned subreddits, we selected seven that meet the following criteria: 1) the description is pertinent to computing devices and/or networks used in a home setting, 2) there were at least more than 1,000 members, and 3) the topics covered are not very technical in nature, e.g., 'r/cybersecurity' focusing on technical security discussions was excluded. In addition, we decided to add three popular subreddits related to smart speakers (Google Home, Smart Things, and Amazon Echo), drawing on the evidence from past studies where we noticed many past studies [1, 24, 27, 31, 35, 41, 89, 91] that used one or more of the three types of smart speakers to demonstrate S&P perspectives of users in multi-user homes. The ten selected subreddits include 'r/technology', 'r/privacy', 'r/smarthome', 'r/homeassistant', 'r/homenetworking', 'r/homeautomation', 'r/homesecurity', 'r/googlehome', 'r/Smartthings', and 'r/amazonecho'.

In order to collect relevant Reddit posts, we designed a search query with a selection of keywords. Our keyword selection was guided by the research questions and the context of our study. The research questions focus on two main areas, i.e., S&P perspectives of home users and the shared home context. As mentioned above, the selection of subreddits focused on home security-related topics to satisfy the criteria of S&P perspectives of home users. Next, we needed to find relevant posts that reflect the shared home context. We, therefore, chose the following list of keywords that are synonymous with the meaning of shared home and might be used by Reddit users in such a context. These keywords were chosen after a detailed discussion between the authors of this paper. In the following search query, the character '|' represents the Boolean operator OR:

("shared apartment" | housemate | "shared accommodation" | "shared room" | "shared flat" | "Paying guest" | "Live-in landlord" | "Hospital accommodation" | "shared house" | communal | hostel | hospice | "communal home" | "student accommodation" | "staff accommodation" | flatmate | roommate).

We used the Pushshift API (https://github.com/pushshift/api) to search for and extract the relevant data dated between 1 May 2021 and 1 May 2023 from the selected subreddits, leading to 411 posts related to shared home environments. Pushshift API ingests Reddit data through its official API as per Reddit's data collection and maintenance terms of service [70] and makes it available for public use. We manually analysed each post to filter posts that are S&P related (58) and discarded posts that seemed, in our expert opinion, to be posts submitted by an expert user. We finally got 46 posts for further analysis.

3.2 The Online Survey

The survey included in the Appendix was used to understand the behaviours, attitudes and concerns of co-habitants in shared home environments. Some of the questions in the survey followed the topics we discovered earlier in Section 2 and were included to comprehend any pronounced similarities or differences in the S&P perspectives of the people in shared homes, as opposed to the traditional family homes. Although questions in the survey cover previously studied topics in past research, we constructed all our survey questions independently for our work.

The questions in the survey formed three different sections: collecting demographic data in a multi-user home, S&P behavioural data related to network and router use, and finally, the S&P behaviour and concerns with regard to devices and other users in the shared home environments. Two researchers rigorously examined and validated the survey questions in several sessions. A pilot survey was conducted with participants recruited using Prolific (https://www.prolific.co/), an online participant recruitment system used widely by many researchers [18, 49, 79, 87]. The survey questions were edited after reviewing the pilot survey data results. The final survey was

also conducted using Prolific. 174 people participated in the final survey, each taking an average of 8 minutes to complete the survey. Participants were rewarded for their time at a payment rate of £11.10 per hour. The authors' institution's research ethics committee gave a favourable opinion of the study. After carefully examining the data, we rejected 25 participants because of the incompleteness of data, leading to 149 valid participants.

Our survey questions were designed to understand several different concepts, including identifying peoples' device use, access and management of shared home networks, and residents' trust level towards their cohabitants' visitors and endeavoured to discern various threat actors specific to shared home users. We calculated the descriptive statistics of the survey data and conducted some inferential statistics to explore the associations between participants' perceived S&P risks in shared home environments and the factor that might be responsible for the perceived risks, such as potential malicious behaviours from other co-habitants and their visitors.

3.3 Analysis of data

We used both descriptive and inferential statistics to analyse the survey and online data quantitatively. All analyses were conducted using IBM SPSS Statistics (V.29.0). The descriptive statistics were primarily conducted to understand the frequencies of survey question responses. A series of chi-square tests were performed on the online survey data as part of the inferential statistics to understand whether responses to certain questions may be associated with other responses. Specifically, we wanted to find out whether the participants' S&P concerns are related to how their perception of S&P-related risks in the shared home environment and their understanding of S&P risks from sharing computing devices amongst the members of the shared home.

The Reddit data was also qualitatively analysed. We open-coded each of the Reddit posts to understand the different messages within them. Following the interpretative phenomenological analysis (IPA) approach [3], we decided on sub-themes for each post and then compared the individual sub-themes to decide on the high-level theme of all the Reddit posts. The first author performed open coding to develop a codebook capturing the main themes, while the second author of the study used that same codebook to code the Reddit posts independently, adding/modifying the codes as they felt fit. The second meeting decided on the axial codes, that is, the second level of codes, which identifies the emerging themes [86] and the possible final themes. Our main aim was not to see whether the same open codes were chosen for each post but whether both coders linked the same posts to the same axial codes. Subsequent meetings discussed any modifications and/or additions to the codebook and the major themes. The posts were coded with the new coding scheme. We aimed to achieve a richer interpretation rather than a consensus of meaning, as pointed out by Braun et al. [11]. We used a research software system called MAXQDA (http://www.MAXQDA.com/) to help our qualitative analysis. To maintain the anonymity of Reddit users, we have paraphrased all the quotes from the users throughout this article.

4 Results

This section begins by describing some descriptive statistics of our survey data. It then shows results from both the online survey and analyses of the Reddit data, organised around the two research questions.

4.1 Survey Participants

Table 1 shows the demographic details of our survey participants. The average size of the household is 4.27, with 25.3% living in a 4-person household, 24.7% in a 3-person household, and 11% in a 5-person household. For eight households, the number of co-habitants reaches up to 8, and for two

households, the number of co-habitants is 20 and 30, respectively. Nearly half (50.3%) of participants belong to the age group of 26–35, and the second largest age group is 18–25 (23.5%).

Table 1. Participant demographics (n = 149)

Demographic	Statistics
Gender	Male (54.4%); Female (45.6%); Others (0.0%)
Age range	18–25 (23.5%); 26–35 (50.3%); 36–45 (16.8%); 46–60 (9.4%); > 60 (0.0%)
Type of shared accommodation	Privately rented (88.0%); Student accommodation (8.7%); Staff accommodation (1.3%); Hostel (1.3%)
Student status	Yes (29.3%); No (70.7%)
Employement status	Full time (70.0%); Part time (20.0%); Unemployed (10.0%)
First degree or above (ICT-related)	Yes (26.1%); No (including education below the first degree) (73.9%)
ICT-related job	Yes (24.2%); No (including unemployed) (75.8%)

The following chart shows the number of people living at each participant's home. We assume people staying with more than 20 or more participants to be living in student/staff/hostel accommodation. We can deduce from this figure that more than 50% of households live with ≥ 4 inhabitants.

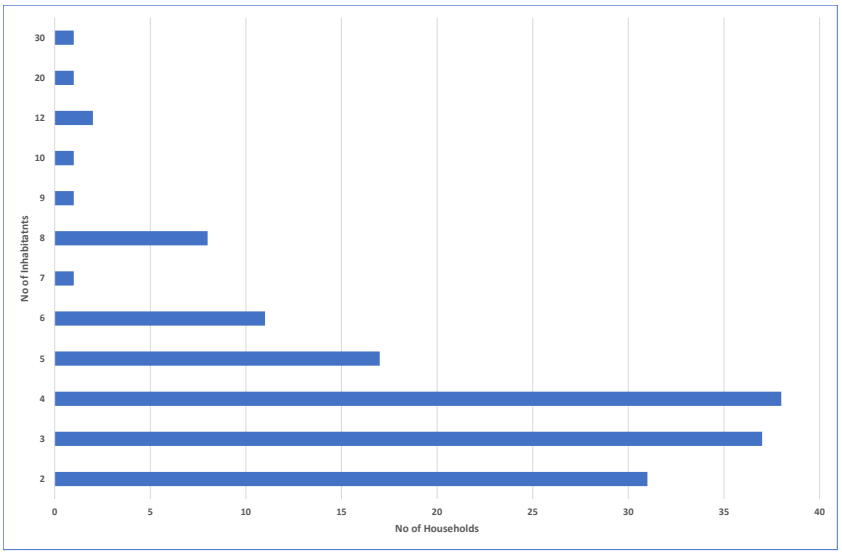

Fig. 1. The distribution of the number of inhabitants per household

4.2 Device Ownership & Sharing

In shared home environments, who own(s) and manage(s) what devices can be complicated due to the existence of multiple co-habitants without a familial bond. We observed some interesting points with regard to the spread of devices in our dataset. Table 2 denotes the number of homes

with a particular device and what percentage of those devices are owned or managed by landlords, individually owned by the participants as inhabitants of the shared home or by multiple occupants pf the said home. As highlighted in the Table 2, over half of most types of reported devices were owned/managed by the landlords. One possible explanation for such a phenomenon is that most shared homes are often fully or partially furnished; therefore, the landlord is the natural party who is expected to provide basic home appliances and computing devices. This is reflected in another observation that 89% of our survey participants lived in privately rented households. Note that the landlord-tenant relationships in terms of device ownership and management can also exist in more traditional family homes as long as the home is privately rented. However, as far as we know, this particular aspect in relation to multi-user S&P challenges has not been researched in past studies for any home environments, so our work is the first one exploring it. Considering the nature of most home devices, we can assume the actual residents are the frequent users of such landlord-provided devices; however, our survey data show that our participants were not provided much information on the extent of data collection/storage of these devices from their landlord: 52.3% of them did not receive any details regarding the devices, and only 22.1% received some functional and/or operational details such as WiFi password and how to use the smart thermostat. A survey question about the sharing habit of devices revealed that 27.5% of the residents shared their smart speakers. When asked about their behaviours on sharing traditional computing devices, a surprising 24.7% of the survey participants mentioned that they regularly shared their laptops/PCs/tablets with other co-habitants and 5.3% of the participants even shared their smartphones.

Most device-related posts on Reddit are about investigating secure ways of owning and/or sharing devices within a shared home. Sometimes, the poster wanted to have control of a device so that they could control the activities of the other co-habitants, and sometimes, the poster wanted to understand whether their co-habitants' devices were spying on them. There are five posts where the landlord-resident relationship was mentioned. In all of these cases, the router was owned by the landlord. Although the landlord was not involved in any of the S&P concerns mentioned in these posts, they had the controlling say in how these issues were managed (i.e., in four out of those five cases, the posters referred to the landlord to solve their problem).

4.3 RQ1: What are the S&P awareness and behaviours of the people living in a shared home setting?

4.3.1 ***Types of Users – Contextual Roles****:* As shown in the related work, there are different types of user relationships at play in a multi-user home environment, including primary and secondary users or pilot and passenger users [31, 38, 41, 43, 47, 66, 90], bystanders [1, 7, 52, 87, 89] and incidental users [18, 58]. We examined different scenarios in our Reddit data and the survey data to find out what user types existed in shared home settings. We observed that shared home users exhibit roles similar to those in traditional family homes. However, the nature of such user roles often differs, reflecting different associations amongst co-habitants, which are mostly horizontal in nature due to the lack of a hierarchical familial structure as in traditional family homes. For example, co-habitants in a shared home normally have an equal right to use landlord-provided devices, which results in a *primary-primary* user relationship rather than the more typical *primary-secondary* user relationship seen in a family home. A bystander in a family home is always portrayed to represent a temporary visitor, i.e., visitors coming over and domestic workers such as nannies working at home, as opposed to in a shared home where other co-habitants can become bystanders and they are not usually temporary visitors to the home. Both our survey data and the Reddit posts evidenced the existence of these above relationships. A detailed examination of our findings revealed four different types of users in addition to other types already described in past studies. The description below endeavours to define such users.

Table 2. Statistics of the device ownership and control

Type of Devices	Owned / Managed by			#(Homes) with said devices
	Landlord	Participant	Multiple Co-habitants	
Router	**50.7%**	27.7%	12.8%	148
Smart Thermostat	**75.0%**	7.9%	3.9%	76
Smart Lock	**61.1%**	11.1%	5.6%	36
Smart Speaker	12.0%	42.4%	21.7%	92
Security Camera (external)	**80.0%**	13.3%	6.7%	45
Security Camera (internal)	**41.7%**	22.2%	8.3%	36
Smart Bell	**48.8%**	14.0%	11.6%	43
Smart Fridge/Freezer	**30.0%**	10.0%	5.0%	20
Smart TV	15.7%	48.8%	15.7%	127
Smart Meter	**61.7%**	11.1%	11.1%	81

(1) **ExternalPrimary**: These users have primary ownership and control of the devices being used but do not reside inside the shared home. The main example of this kind of user is the landlord of a shared home who does not live in the home but controls one or more devices inside the home. For example, the landlord commonly owns and controls the router in a rented home, so they are the primary users, but in most cases, they do not live inside the shared home. Hence, we labelled them as ExternalPrimary.
(2) **InternalPrimary**: These are users who have their own devices and control them as administrators. For example, many shared home users would have their own smart speaker or security camera, which they own and control themselves. They are the primary users of these devices, and they live inside the shared home. These users are, therefore, termed as InternalPrimary users.
(3) **ActiveSecondary**: These are users who do not have primary control over one or more devices in a shared home but actively use them. For example, when some of the shared home users do actively use a smart speaker owned by another co-habitant, they are called secondary users as they do not have the primary ownership or admin rights over the device, but at the same time, they use the devices actively so are labelled as ActiveSecondary.
(4) **PassiveSecondary**: These users do not have primary ownership or admin control over one or more devices. Additionally, they do not actively use such devices, either, however, they can be affected by other co-habitant(s)'s use of such devices. For example, when a user of a shared home installs a security camera in front of their room in a common corridor, the movements of other co-habitants get recorded whenever they pass by the corridor or do any activity there. The latter users are not actively using the camera, but their privacy could be affected by the existence of such a camera. Such users are named in our study as 'PassiveSecondary' users. The nature of these users simulates the same features as a *bystander* as mentioned in past studies [8], with the only difference being the following: Bernd et al. [8]'s *bystanders* are users who temporarily visit the device owner(s)' home whereas our *PassiveSecondary* users live in the same home.

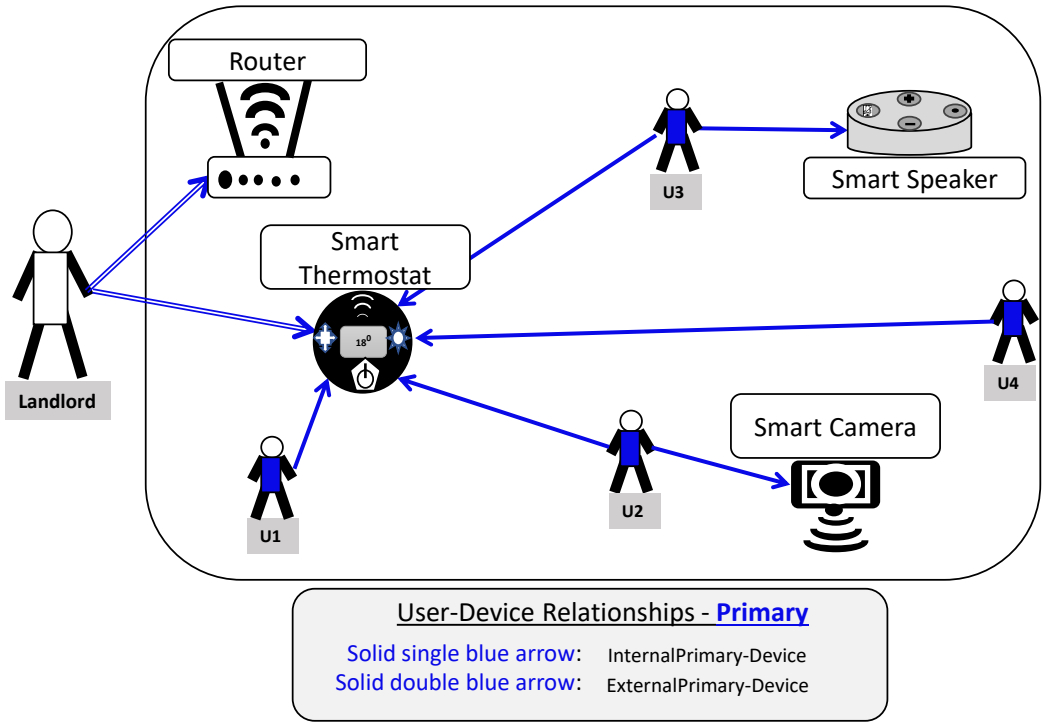

Fig. 2. A visual illustration of user roles within a shared home in terms of owning, managing, and using computing devices – Primary users

Figures 2 and 3 represent an imaginary example scenario of a shared home with four co-habitants (U1 – U4) and an externally living landlord (reflecting an average case according to our survey data) and the possible connections between these users and four home devices: 1) a router, 2) a smart thermostat, 3) a smart camera, and 4) a smart speaker. The example scenario involves four different types of users, which we describe below. To represent the different user-device relationships, we use different types of line styles and line colours in these figures, as explained below.

- A **solid single blue arrow** represents a relationship between an InternalPrimary user and a device.
- A **solid double blue arrow** represents a relationship between an ExternalPrimary user and a device.
- A **solid single red arrow** represents a relationship between a SecondaryActive user to a device.
- A **dashed red arrow** represents a relationship between a SecondaryPassive user and a device.

The **router** is owned and managed by the landlord, so they are the designated primary user of the device. Because, in this case, they live outside of the shared home, they are labelled as an **ExternalPrimary** user, and their relationship with the router is displayed with a solid double blue arrow in Figure 2. All other users, U1 – U4, use the router actively to connect to the internet. They, therefore, are labelled as **ActiveSecondary** users, and their relationship with the router is depicted in Figure 3 with solid red arrows.

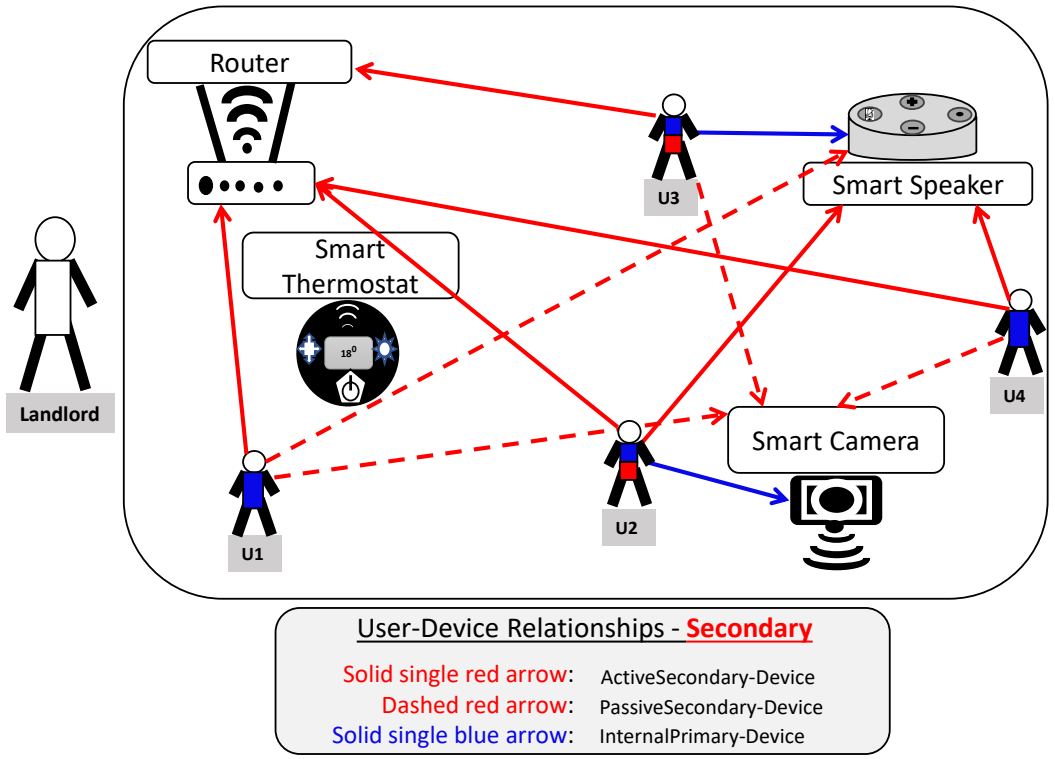

Fig. 3. A visual illustration of user roles within a shared home in terms of managing and using computing devices – Secondary users.

The landlord owns the **smart thermostat**, and they also have the administrative rights to control the device if they want to do so. They, therefore, are a primary user of the device. On account of his living outside of the house, they are labelled as an **ExternalPrimary**. His relationship to the thermostat is displayed as the solid double blue arrow in Figure 2. The administrative rights to control and manage the thermostat are also given to all the co-habitants U1 – U4. Hence, all of them are considered primary users who are internal to the home and labelled as **InternalPrimary**. Their relationship with the thermostat is displayed with a solid single blue arrow in Figure 3. This scenario, therefore, creates multiple primary users in the shared home context.

U3 owns and controls a **smart speaker** and, therefore, is the primary user of that speaker. This relationship is displayed in Figures 2 and 3 by the solid single blue arrow between U3 and the smart speaker. U3 allows U2 and U4 to use the smart speaker whenever they want. U2 and U4 are, therefore, designated as secondary users of the device who actively use the smart speaker and labelled as **ActiveSecondary**. Their relationship to the smart speaker is represented with a solid single red arrow. U1, on the other hand, could be playing the role of **PassiveSecondary** as the smart speaker might accidentally record U1's conversation as they participate in any common discussion.

U2 owns and manages an internal **smart camera** for their own use. They, therefore, are considered the primary users of that camera and designated as **InternalPrimary**. Their relationship with the camera is denoted by a solid single blue arrow. Other co-habitants are not given permission to use the camera, but the camera actively records all movements of anyone passing in front of it and

is placed near the front of U2's room door, which opens to the communal corridor of the shared home. The camera, therefore, quite possibly records the movements of the other co-habitants U1, U3 and U4 whenever they are in the corridor. These other users, therefore, are passively exposed to the camera all the time and labelled as **PassiveSecondary**. In Figure 3, this relationship is exhibited with a dashed red arrow.

The implications of these different relationships in a shared home and how they relate to a traditional family home are discussed further in Section 5.

4.3.2 ***S&P Awareness and Behaviours – Home Network****:* 38.3% (57/149) of survey participants thought the computing network in a shared home is less secure than that in a traditional family home. Two main reasons given for this perceived lower security include reduced trust in other co-habitants and their visitors and the constant exposure of the shared home to many strangers. A similar proportion of participants (60/149, 40.27%) thought that shared homes have a similar level of security to traditional family homes. 14.1% of the participants were not very sure about this, whereas 7.4% believed that shared homes are less secure when they moved in but felt secure after settling down. We observed that the landlord provided 51.0% of the households' routers, but 91.3% of the participants shared a WiFi password, using a router that was bought by themselves (30.9%) or another co-habitant (10.1%). 36.9% of the survey participants (55/149) had administrative rights on the router to change administrative settings; however, not everyone was engaged in administrative activities. From those participants who had administrative rights to make changes in the WiFi, we noticed that some co-habitants were familiar with changing the WiFi password (30.9, 17/55) or checking the status of devices connected to the WiFi network (40.0%, 22/55) and a few also ventured into setting up a guest network (9.0%, 5/55). Interestingly, 14.0% (21/149) of the survey participants did not know or care about the administrative rights of the routers they used. Posts in our Reddit data also demonstrated shared home users' understanding of the requirements of a secured home and their inclinations towards building more secure home networks. For example, one of the posts queried about the creation of a guest network purely to create a safe boundary between different co-habitants of a shared home so that their devices do not get infected in case of other co-habitants use a compromised device in the home.

Exploring some of the other S&P behaviours of shared home users, our survey discovered that 79.2% (118/149) of the participants shared their WiFi password with all visitors to their homes, and the shared password had never changed afterwards. 60.4% (90/149) of the participants reported that their router had been placed in a common area accessible to everyone who would visit the house. Although 53.6% (80/149) of the participants were aware of the fact that WiFi can be spied on, 28.2% (42/149) did not think about it, and 6.0% (9/149) did not care about it. Additionally, 12.1% (18/149) of the participants were unaware of it. In order to find out whether these behaviours have any statistically significant association with our survey participants' opinions about the lack of security in comparison to a traditional family home, we decided to perform a number of χ^2 tests. With $\alpha = .05$, our results indicated a statistically significant association ($\chi^2(1, n = 149) = 39.916, p = .002$) between our participants' perception of security in a shared home network and their awareness of being spied on in the network. We also found a strong association ($\chi^2(1, n = 149) = 50.634, p = .001$) between our participants' reported behaviours of sharing their WiFi password with visitors of other co-inhabitants and their perception of shared home security. Table 3 presented later in Section 4.4 reveals more associations on this above assertion.

We observed that some Reddit posters used terminologies such as *'extremely paranoid and worried to share the WiFi connection'* with their roommates or expressed the desire to learn to separate their network from their co-habitants so that they could protect their security and privacy better. There

were 32.6% (15/46) network security-related queries in our Reddit data, and almost all of them were posted regarding secure configurations and settings of the network.

4.3.3 ***S&P Awareness and Behaviours – Around Devices Users****:* As evident from the survey data, 75.8% (113/149) of our participants used and shared devices that were provided by the landlord or the property owner/manager. Apart from the landlord-provided devices, some participants also shared personal devices with other co-habitants in the shared home. 24.8% (37/149) shared their laptop/PC/tablet with other co-habitants. Only 12.8% (19/149) were concerned that co-habitants might spy on them using the shared computing devices, and only a small percentage of 4.7% (7/149) had some problems such as malware infection or illegal downloading after they shared their devices with their co-habitants. 38.23% (57/149) participants of our survey shared their smart speakers with other co-habitants, and only 5.4% (8/149) were concerned about any privacy violation from their co-habitants. 28.8% (43/149) mentioned that the smart speaker was kept in a publicly accessible place for anyone to access it, and only 8.7% (13/149) of the participants had set individual voice profiles on the hub so that sensitive data could not be easily accessible by untrusted persons. The above data give a slight indication that shared home users might be more concerned about sharing their traditional devices than their smart devices. We observed that more than half of the participants (56.9%, 84/149) actively tried to move their devices, such as smart speakers, laptops, PCs, and tablets, to a secure place before any parties and other get-together events happened in their shared homes. For 44.9% (67/149) of the participants, there was a smart camera or a smart doorbell in the shared home; however, 20.8% (14/67) of them were unaware of how and where the recordings from such a device are kept, and for 25.4% (17/67) the recordings were stored under the control of the landlord. Most participants exhibited good S&P behaviours around portable computing devices such as laptops by switching them off and keeping them in secure places when not used (57.7%, 86/149) and locking these devices when they leave the device temporarily (59.7%, 89/149). These statistics seemed to indicate that residents in shared homes are likely more aware of S&P issues with regard to traditional computing devices such as laptops.

Analysis of Reddit data exhibited different S&P characteristics of shared home users. At times, the poster wanted to learn whether sharing a particular smart device is secure, and at other times, the poster sought advice or information on specific security settings on devices or the purchase of specific smart devices to prevent privacy violations. For example, one of the Reddit posters wanted to connect a smart bulb with a motion detector so as to deter their roommates from accessing personal belongings and information, while another poster wanted to know the ways of restricting Amazon Alexa devices from sharing selected information. Out of the 46 Reddit S&P-related posts that we analysed in detail, 67.4% (31/46) are on smart devices. We noticed only two occurrences of posts with regard to traditional devices (PCs and laptops).

4.3.4 ***S&P Behaviours – Around Other Users****:* Researchers have observed that a social context should always be in the background when we analyze any S&P behaviours (similar to any other type of human behaviours) [20]. Past studies have looked into the social influence on S&P behaviours, attitudes, and practices [19, 82] to understand how specific S&P behaviours are triggered and the impacts thereof. While endeavouring to understand the nature of S&P social interactions between co-habitants, we found our survey participants had engaged in various S&P discussions such as placement of shared devices, sharing of passwords, creating separate guest networks with the most common form of discussion around sharing (47/149, 31.5%) of different devices such as routers, smart locks, and security cameras. Discussions also touched upon areas such as the placement of smart routers and smart speakers (25/149 16.7%), installing anti-virus/malware protection on personal devices to keep the network secure (25/149 16.7%), how to maintain security and privacy of devices (23/149 15.4%), and creating guest networks (19/149, 12.7%). Upon questioning whether

the co-habitants sought help from each other, 32.8% (49/149) mentioned affirmatively regarding S&P settings of various devices. There are also mentions of help in relation to S&P problems such as cleaning infected machines, phishing(38/149 25.5%) and other related configurations such as setting up VPNs, creating cloud-based backups, setting up MFA, and purchasing security software (34/149 22.8%).

We observed that Reddit posts are more in relation to seeking S&P-related help and advice. Some of the frequent help-seeking posts are in relation to the use and purchasing of security cameras (16/46, 34.8%), setting up secure networks (11/46, 23.9%), and privacy in communal areas (14/46, 30.4%). Note that there can be overlaps between the different topics, i.e., some of the security network-related posts contain messages about security cameras as well, and some posts about security cameras include privacy-related queries. In several of the posts (34/46, 73.9%), the poster was desperate to know ways to prevent privacy risks using smart devices, which arose from conflicts with roommates. Sometimes, the behaviour displayed is conciliatory in adapting to S&P actions of other co-habitants without any questions, and at times, the poster expressed frustration and sought ways to modify the situation. In one of the cases, the poster wanted to get advice on persuading their roommate not to buy a specific brand of vacuum cleaner that they believed was privacy-invasive. At times, tech-savvy residents undertook the responsibility of technical and S&P work inside the shared home but did not possess the patience to explain to other co-habitants. We noticed this happening in one of the messages where the user felt frustrated because their co-habitant disabled and modified advanced settings and did not explain the reasoning behind these actions. This left the poster annoyed and being less aware of the S&P situation of the shared home.

To summarise, we observed that the majority of shared home co-habitants consider a shared environment as less secure than a traditional family home, which could be because they felt they had to share their WiFi password with less trusted people and their fear of being spied upon by such people. We found that existing S&P-related relationships between co-habitants in a shared home could be very complicated depending on the devices used. This sometimes led to situations with multiple/all device users having primary access to the device, a situation that is not very common in traditional family homes. Our findings also revealed the unique S&P-related role the landlord plays in a shared home environment, where they can be considered outside "insiders". Note that such a role can also exist in traditional family homes when a whole family lives in a rented home from a landlord. This observation raises the point that any future research and discussions regarding S&P of the shared and traditional family home environments should seriously include landlords in its scope. We noticed that many participants endeavoured to behave securely by having various S&P discussions with other co-habitants within their shared homes and sought S&P-related advice when needed. However, their efforts to be secure in a multi-user shared home environment were limited by a lack of knowledge and skills and also by how cordially the other co-habitants behaved.

4.4 RQ2: What S&P concerns are experienced by shared home co-habitants, and which threat actors are the likely sources of these concerns?

This section analyses the S&P concerns that were expressed in the Reddit posts we collected and by the participants of our survey. We investigated the origin of the threats in our dataset and drew possible threat actors who might be responsible for the concerns of the co-habitants.

4.4.1 ***S&P Concerns: Network, Device, Co-habitants and landlords****:* As mentioned in Section 4.3, according to our survey data, 38.9% (58/149) of the participants believed the shared home network is less secure than a traditional family home, and 50.3% (75/149) thought that devices in a shared home are less secure than those in a family home. 88.6% (132/149) of our survey respondents were from privately rented flats with multiple tenants, which, as shown by our further examination,

is one of the reasons why users of these types of houses perceived a higher level of S&P risks than in a family home environment. We found that some participants were sometimes concerned about threats posed by their co-habitants (14.0%, 21/149) and more about visitors of their co-habitants (23.4%, 35/149).

There are two main questions in our survey, B7 and C11 (see the survey questionnaire in the Appendix), which asked the participants about their S&P concerns in living in a shared home network with shared devices compared to a traditional family home. Intending to find any possible associations between the S&P concerns of the participants with various factors such as the nature of the shared home, device ownership, S&P behaviours and perceived risks of co-habitants and the landlord, we performed a series of Pearson χ^2 tests ($n = 149, \alpha = .05$). Tables 3 (tests pertaining to co-habitants' concerns in a shared home network) and 4 (tests pertaining to devices used in a shared home) show the results of those tests. These results include only the reasons with a significant effect. As can be seen, users probably formed their perception of security in a shared home for many different reasons, ranging from threats posed by other co-habitants or visitors of other co-habitants to their fear of devices being tampered with when unattended. One important finding is about our survey participants' S&P concerns due to the fact that some devices used are owned and managed by the landlord and that the tenants did not receive any relevant documentary information about such devices. We have highlighted these associations in both tables with an asterisk at the beginning of relevant entries.

Table 3. Statistical results of Pearson χ^2 tests on probable reasons of shared home co-habitants' perceived higher S&P risks in a **shared home network/WiFi**

S&P Concern	χ^2 **Statistic**	**df**	p**-Value (2-sided)**
Fear that WiFi can be spied upon	40.743	21	.006
(*) Living in a shared student accommodation	19.115	7	.008
(*) Ownership of the router	68.705	35	$< .001$
Worry that the co-habitants or their visitor might spy using shared devices	22.039	7	.003
Probable S&P risks from the co-occupants	23.299	7	.002
Probable S&P risks from the co-occupant's visitors	14.629	7	.041
Probable risks of tampering with computing devices from the co-occupants when not at home	14.187	7	.048

Users we observed in our Reddit data were sometimes afraid of/concerned about their roommates as they could not convince them to adopt secure behaviours. We came across Reddit users expressing their concerns about their roommates who exhibited insecure behaviour by opening up random websites and installing software without checking their authenticity. Such posters were anxious and worried that they were unable to educate their roommate and that their roommates' devices would get infected by such insecure actions, and, consequently, they could get their own devices infected. At times, some posters feared that their co-habitants might hack their devices but were unsure how that might happen. They took to the Reddit platform to query about possible ways how they might be affected and likely devices that might be in use to gear such activities.

4.4.2 ***Cyber-Physical Threats and Concerns Thereof****:* We observed that users in a shared home displayed concerns such as power imbalance between users, direct conflicts between users of different shared devices, and complex trust relationships amongst co-habitants of the home, which are somewhat similar and prevalent in traditional family homes [7, 91], although the trust level of

Table 4. Statistical results of Pearson χ^2 tests on probable reasons of shared home co-habitants' perceived higher S&P risks **to their devices in shared home**

S&P Concern	χ^2 Statistic	df	p-Value (2-sided)
(*) Staying in a privately rented house with multiple tenants	14.217	3	.003
(*) Not receiving relevant information from the landlord-owned and controlled devices	13.935	6	.030
(*) landlord-owned and controlled devices	11.950	3	.008
Routers owned by landlords and cohabitants	17.446	8	.026
(*) Access to the recording of the smart camera(s)/video doorbell(s) by landlord and other cohabitants	170.600	18	< .001
Shared WiFi passwords between occupants	14.927	6	.021
Shared WiFi passwords with visitors of co-occupants	31.504	9	< .001
Exposed WiFi password by the common placement of router	152.474	9	< .001
Being spied upon when devices are shared	12.040	2	.002
Sharing of smart hubs between co-occupants	160.288	12	< .001
Sharing smartphone with other co-habitants	12.039	4	.017
The need to hide the devices when there is a party/get-together organised by other co-habitants	171.367	12	< .001
S&P is adversely affected by the negligence of co-occupants	154.754	6	< .001
Malware affected devices of co-occupants might affect other devices at home	159.407	12	< .001
S&P risks related to other co-habitants	10.911	2	.004
S&P risks related to other co-habitants' visitors	11.856	2	.003
Devices being tampered with when not at home	8.350	2	.015
The WiFi network is not secure in a shared home	5.535	21	< .001

participants is different. For example, the trust level between a resident and their co-habitants or their co-habitants' visitors is totally different from that between family members.

Our Reddit dataset includes several posts that discussed concerns about physical security. This echoes the findings of another paper [90], where physical security has also been recognised as the most common type of concern in a traditional family home setting. Our data show evidence of three different types of cyber-related threats described below: cyber threats, cyber-physical threats, and physical-cyber threats. For the latter two types of threats, we followed the *Cyber Physical Threat* taxonomy proposed by [29], who provided detailed examples of how security breaches in smart homes can affect both cyber and physical spaces.

Cyber threats: These refer to types of potential S&P attacks that might be happening in the cyber space [63]. These include, for example, the fear of a shared home user from other co-habitants or their visitors' accessing their private information by accessing shared computing devices.

Cyber-physical threats: These are threats where the physical safety of a shared home user is threatened by one or more smart devices that are affected by malicious cyber activities. We considered a *cyber-physical* threat in line with the definition of 'cyber-physical attack' by Loukas [44] as a security threat from the cyber space that threatens to adversely affect the physical space.

The affected people in the physical space are concerned about their physical privacy, safety, and well-being. For instance, in a Reddit post in our dataset, one shared home user complained about their roommate who supposedly violated the poster's privacy by hovering near their bedroom door. The poster enquired about how to install a motion detector to a smart bulb to automatically flash blind their roommate with bright light when they reach the bedroom door.

Physical-cyber threats: These are threats opposite to cyber-physical ones, where an attack performed in the physical space adversely affects the cyber space [44]. Some posts in our Reddit data are examples of one sub-type of such threats called 'Unauthorised actuation' reported by Heartfield et al. [29], where the user's roommate kept disconnecting their security camera in the common living room, an unauthorised physical action by the roommate that led to concerns over the proper working of a smart home device.

Several examples (11/46, 23.9%) touched upon the subject of privacy violation, where the poster's privacy was violated by the act of their co-habitants, but they were not sure of how to handle the situation (e.g., whether to contact the police and what are the grounds of such calls) or did not have the means to do so (e.g., lack of finance to access legal help). Other examples present evidence of privacy concerns and impact on domestic life, including 'loss of control', 'inconvenience' and 'invasion of privacy' (terminology used by Heartfield et al. [29]).

4.4.3 ***S&P Concerns and Threat Actors in a Shared Home****:* Threat models in multi-user home security have been studied by many researchers [27, 74, 75, 82, 90]. Threat modelling in smart homes generally espouses two main classes of adversaries, i.e., external parties who can cause damage to the system, data, and/or platforms, and internal adversaries, including household members who have physical access to the home and can pose a threat to all assets. Some researchers, such as Slupska [74], focused on the extreme end of the concept of 'insider threat' in smart homes while researching intimate partner abuse (IPV). At the same time, others [91] discussed non-adversarial threats in a family home setting involving conflicts between different users. However, apart from He et al. [28], who developed a threat model on non-technical adversaries who have legitimate access to the home, no other prominent studies have looked into this area.

Exploring both the survey data and the Reddit posts, we discovered different threat actors specific to shared home settings who might pose S&P concerns for shared home users. Based on the data we collected and the information on related cases discussed in Section 2, we constructed a model representing possible threat actors which the shared home user might face internally under the umbrella of 'insider threat.' The model is presented in Figure 4. The model does not consider any outsider threat actors, e.g., hackers trying to sniff the house data, but focuses mainly on people who might be present in a shared home due to either being a resident or visiting the shared home or having a chance to visit the shared home legally/illegally due to their earlier connection with the shared home. We categorized the threat actors in the model into three categories, I, II, and III, according to the trust level that was revealed in our dataset and our analysis of it. As the scope of the threat actors broadens (this is represented with the grey ellipses in Figure 4) to include the co-habitants and the shared home users' own visitors first, then the visitors of the co-habitants, the trust from these actors decreases, and correspondingly the security concern increases. We can see a reflection of this in our survey data where in answer to the question on whether users were concerned about S&P risks, 5.3% of the users showed concerns about their own visitors, 11.5% were concerned about their co-occupants, and 16% were concerned about the visitors of their co-occupants. Figure 4, shows different threat actors in a shared home environment organized around a specific user in the shared home, who is shown in the middle of the diagram as 'Me'. Each threat actor in the diagram is placed in a different category depending on to what extent the specific user trusts the threat actor. Other co-habitants and visitors of the specific user are placed

in Category I (the most trusted people by the specific user 'Me'). Visitors of other co-habitants and the 'beyond home users' are placed in Category II (the group of people less trusted than Category I people). The 'beyond home users' are people who had access to the same shared home in the past as a former co-habitant or due to other reasons (e.g., a frequent visitor to the shared home in the past due to a close tie with a former co-habitant). The landlord is assigned a different category III owing to their special status in the shared home context.[2]

Some of our Reddit posts (7/46, 15.2%) exhibit characteristics of what we have termed as the 'beyond home' threat actors. These are people other than the landlord who do not live in the home but could visit and control one or more home devices in some way. For example, some posters expressed their concerns and frustration when their home devices were controlled and managed by their co-habitant's friends, whom the co-habitant trusted with the device management permission, without consulting everyone in the house. The 'friend', in this case, was outside of the shared home but still controlled devices inside the home. In other cases, such posters were anxious about their security and privacy from their ex-roommates, who still had legal access to their shared home. Threats such as these cause concerns for people and still happen within the home boundary but are caused by actors beyond the home.

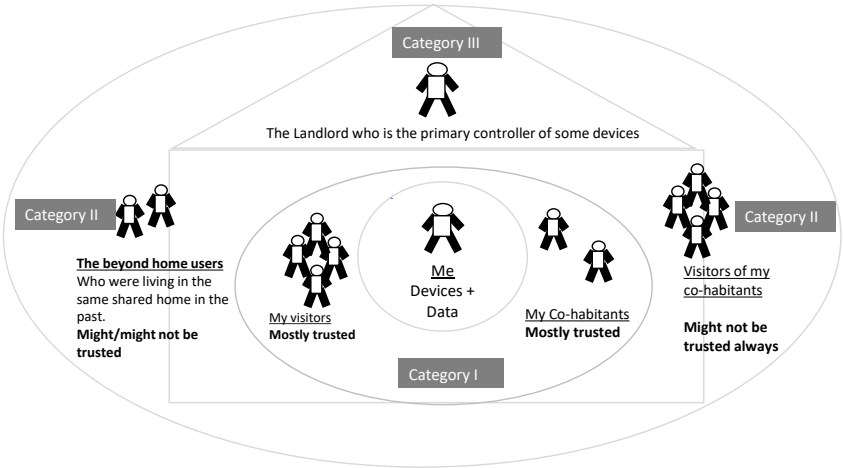

Fig. 4. Different threat actors in a shared home setting

In summary, our observation of shared home privacy and security concerns evidenced that residents in a shared home environment face different threat actors due to the nature of their relationships with other co-habitants, which affect their trust level to a certain extent. The concepts of 'insider threat' and 'beyond home threat actors' in relation to shared homes are important subjects of further discussion and should be paid more attention to in future research. We also noticed that cyber-physical threats are a big concern for the residents of a shared home. Multi-user relationships emerging from the way devices are used, such as *Primary-Primary*, *ExternalPrimary-Secondary* and *Primary-Bystander*, are some of the areas where we need to look at more closely to understand how such relationships impact the S&P behaviours and actions of the residents as well as the landlords. Another intriguing point is that, although shared home users exhibit similar roles as bystanders and primary users, the contextual variations, in this case, can let people have different

[2]Note that some landlords may rent one or more rooms in their home to others so they can also be co-habitants of the same shared home. For this paper, we did not consider such complicated scenarios.

perspectives as bystanders. More specifically, in past studies [9, 52], bystanders considered are mostly visitors whose exposure to home devices as bystanders is accidental and infrequent, which is substantially different from exposure of shared home residents who have to face the situation on a daily basis. Research in this area would shed light on different factors that might influence or impact users' S&P perspectives as a whole.

5 Further Discussions, Limitations & Future Work

Our focused investigation in this specific area of multi-user relationships in a shared home setting revealed a unique contextual disposition of user-to-user and user-to-device relationships regarding cyber security and privacy of the home. It uncovered some ignored or insufficiently studied aspects in past research on home S&P, such as the landlords as ***ExternalPrimary*** users, S&P nuances of multiple primary users, 'bystander' users beyond one-off or less frequent visitors, ex-inhabitants' ability and probability to access household data and/or the home, and consideration of various threat actors in multi-user settings. In addition, our research also led to a number of recommended future research directions, such as more research on specific demographic factors within the shared home population, more empirical studies broadening the scope of online sourced data our study used, and development of a fuller threat model for the multi-user environments. The above aspects and recommendations are discussed below in detail.

5.1 Shared Home S&P: Differences in User Perspectives

Careful consideration of different user roles that we observed in our data demonstrated many similarities of user roles and relationships between traditional family homes and shared home users, such as primary, secondary users and bystanders. We highlighted the case of ***multiple primary users*** in the shared home situation, which has been mentioned in some previous studies [35] specifically focusing on houses where the primary/administrative permissions might be with more than one person. The main difference we noticed in the case of a shared home environment is that if the landlord, as a primary user, shares the administrative permissions of a home device such as a router with their tenants in a shared home, they are expected to share such permissions with each of the tenants by default, as everyone has an equal right to such permissions as a resident. In a traditional family home, these permissions might be shared only if the need arises to share, and there is no compulsion to share such permissions amongst all members. However, these types of shared administrative permissions in shared homes may give rise to a number of problems in terms of S&P, such as who would be held responsible if the lack of security of one administrative user created an S&P problem for all users and how a consensus could be decided in relation to the S&P of a device managed by multiple primary users. For instance, an erroneous administrative setting in a smart camera by one careless or less skilled user might affect the privacy of every member of a shared home. As we noticed in our survey data, only 33% of participants discussed any kind of S&P configuration issues with their co-habitants.

This difference in the contextual balance of power in different types of multi-user homes merits further investigation in future research.

Another interesting point to mention here is the context in which ***PassiveSecondary*** or *bystanders* are verbalised in the existing literature. This user type is primarily looked into as non-household users, such as visitors, neighbours, and household workers [9, 18, 78], who have no or less access to the home devices in question. In a shared home, all co-habitants could be considered '*PassiveSecondary*' when they do not own a device but are exposed to its use on a daily basis. Therefore, **the location of a bystander in a shared home is not necessarily external to the home.**

This leads to two relevant points that are of interest for future research: 1) the internality of the problem requires looking at ***trust in a shared home and its significance in maintaining the social bond between co-habitants***, and 2) the fact that shared home users are staying at home more on a daily basis justifies the consideration of the ***topic of temporality***.

The concept of trust in multi-user homes has been discussed by other researchers from the point of view of users' trust as providers of computing devices in a multi-user home [1, 57, 87], trust between the Airbnb host and guests [22, 48], trust relationships between family members [2, 24, 27, 39, 42, 55], and trust between the employer and employees in a home context [7]. However, shared home users could have specific trust issues. For example, trusting other users with private resources when using the same WiFi, trust implications when device ownership/use of individual members could affect the daily activities of other users, i.e., keeping a camera to record the movements of other users, and trust between users when each one could possess primary user rights are some of the topics that need exploring further.

In considering trust between individuals and their co-habitants in a shared home, Altman's [4] concept of 'interpersonal boundary' is important. Altman discusses the dynamic negotiation process by the individuals to maintain their private space. This process is more challenging when we consider the use of smart devices as well at home. As Ahmad [1] points out, the 'software-controlled and display-limited' nature of smart devices creates a level of mismatch between the *perceived* and *actual* level of privacy for the users at home. So, considering from the 'boundary regulation' perspective, we not only have to attend to the interpersonal relationship between individuals within the shared home but also address the trust and privacy expectations of the shared home users (or non-users in case of *PassiveSecondary* residents) of the different computing devices present within that environment. The entanglement and complexities of these factors increase due to different types of users in a shared home environment, i.e. **multiple primary users**. Understanding the nuances involved in trust between the *user – user* and *user – smart device* in a shared home with multiple devices and their implications needs further research.

For the second point, which is the topic of temporality, discussions on *bystanders* in the existing literature always have the flavour of a user who spends time with a certain device for a set temporary time period and gets exposed to the device. However, shared home residents are not temporary visitors, and they normally stay at home much longer than visitors. Therefore, they should be more concerned according to research of Yao et al. [89], which showed that *bystanders* are more concerned about their privacy when the 'length of stay' is longer. Hence, further research is definitely needed for a better understanding of shared home users as different types of bystander users or what we termed as *PassiveSecondary* users, which have not been studied in the past. This temporality issue is further convoluted by the ex-inhabitants' ability and probability to access household data. According to the English housing survey from 2021 – 2022[3], 88% of the rental properties are rented as shorthold tenancy, i.e., 12 or 6 months. This is just evidence of the frequency with which the tenants in some of the regions might move. In these cases, there is always an increasing possibility of an S&P breach from the ex-tenants, e.g., accessing the house wifi if the shared password is not changed or accessing the house physically if the smart lock password remains the same. Further research in this area is needed to understand and establish clear policies with regard to the changeover of tenants.

[3]https://www.gov.uk/government/statistics/english-housing-survey-2021-to-2022-private-rented-sector/english-housing-survey-2021-to-2022-private-rented-sector#housing-history-and-future-housing-aspirations

5.2 S&P Issues in Rental Homes

The ***landlord-tenant relationship*** highlighted in our study has not appeared in detail in past studies. Studies that looked into S&P aspects of landlords and tenants focused on corporate landlords and broader technological facilitation on increasing rent revenues, such as management of the maintenance of the properties using smart apps or finding viable renters using *"data-enabled disciplinary capabilities*" [61][4]. Researchers such as Hulse and Milligan [32] and Byrne and McArdle [13], who did look into rental security, explored the concept of rental tenure security and rental occupancy security on account of factors such as legislative, public policy, market force and cultural dimension. We did not notice any past studies that addressed S&P aspects in the context of shared rental homes, considering the use of multiple computing devices by multiple users. We discussed the *ExternalPrimary* user type in connection to the landlord, which might introduce a very different dimension to the existing multi-user relationships.

We also noted that, despite owning some devices in these premises, landlords hardly inform their tenants or sign any formal agreements with them concerning the use of home devices and the collection of related data (if any). An examination of the UK Government's landlord legal requirements [21] revealed that landlords are not legally required to provide any such information to their tenants. We observed in our survey results that 30% of the participants' data in the form of recording was collected by the landlord (for cases where a smart camera and/or video doorbell existed). The other important point that we would like to mention is that, although we investigated the landlord-tenant relationship in the context of non-family shared homes, a similar relationship is equally possible in the context of traditional family homes that are rented from a landlord.

Hence, we believe that the S&P implications of the landlord-tenant relationship in both shared and traditional family homes need further research. This could include topics from the technical point of view, such as to what extent the landlord can exert their administrative power in configuring and setting the devices, legal obligations and rights the landlord has to store/use the tenants' data, and to what extent the tenants could protect their rights to privacy in terms of smart device data usage.

5.3 Insufficient research on smart home threat modelling

We observed from our literature review that past research has not covered the different threat actors in multi-user homes, such as shared homes, focused in our study. He et al. [28] proposed a threat model focusing on non-expert adversaries in home settings, added on top of expert adversaries commonly considered in the past. However, their work focuses on contextual detection of access control in home IoT sensors. Our current study endeavours to consider all types of computing devices at home, including smart and non-smart devices, while building the threat model. Discussing their proposed threat model for smart home environments, Zeng et al. [90] reflected on the fact that threat models often depend on the 'sophistication' of the mental model of the users, and they stated that the interaction between the primary and other users could be more positive if they share the same threat model. Huang et al. [31] observed how concerns about visitors and other users based on conjectures can lead to inaccurate or incorrect threat models. In her 2019 paper, Slupska [74] raised concerns about the fact that how domestic technology abuse has been conspicuously absent from the general security threat models. They advocated for the same level of policies and protections for domestic abuse victims as happens at an organisational level and pointed out that such steps would only be possible when the 'insider threats' model is considered seriously for intimate partner victims (IPVs) as an extreme type of adversarial settings in a home. Our work further advances our understanding of threat models for multi-user homes by focusing on shared home environments, a very specific area of multi-user homes that have not been studied before,

[4]This is a method whereby the corporate landlords use the rental data at their disposal to screen their prospective renters.

and analysing the threat actors in such environments in detail. The results of our examination and previous studies both evidenced that threat modelling of multi-user home environments needs more attention from the research community as well as from smart home device designers and vendors.

One of the major contributions of our study is the identification of the *insider threat actors* in a shared home environment. However, these threat actors are only part of the whole threat model, and our study examined only people who have access to computing devices at home. We acknowledge that there are some other threat actors our study did not consider, e.g., hackers who never stayed at a shared home but can still access some home devices illegally, vendors and other third parties who might also access some home devices in certain circumstances. These actors do not fall into the scope of our study as we primarily looked into users who are currently staying at a shared home, stayed previously, visited the house or have constant access to the home, such as the landlords. Our future avenue for research is to build a fuller threat model for the shared home environment and extend it to understand the threat model for the multi-user home environment. This would enable us to develop a more comprehensive threat outlook of the multi-user home and provide us with richer insights into multi-user S&P perspectives.

5.4 Limitations and Future Research Directions

A majority of our survey data (64%) was collected from UK participants, and hence, the data may lack the perception of people from non-UK residents. Prior research [26] has evidenced how different cultural dimensions, such as masculinism and uncertainty avoidance, influence individual intentions to participate in a shared economy. Further research should incorporate participants from different geographical areas and culturally varied populations, which might reveal how cultural factors are important to understanding shared home users' S&P behaviours. Further studies focusing on more specific demographic factors within the shared home population may reveal interesting details on various aspects, e.g., whether the age or gender of cohabitants in a non-family household has any specific impact on their S&P behaviours and/or concerns in general.

Additionally, our online data analysis specifically focused on Reddit. This choice has its limitations. Research has shown that different online platforms attract varying populations to their sites, leading to platform coverage error where the platform base is not aligned with the target population [73]. For Reddit, its population has been identified as primarily male and belongs to the younger generation[5]. Although we used relevant keywords to identify a sub-population on Reddit that had relevant discussions, we acknowledge that such a sub-population may be a biased representation of the whole target population of our study (all people living in a shared home environment). This limitation is, however, largely unavoidable because all online platforms have the same problem, and there are no obvious alternative channels for us to reach the target population directly. In our future work, we plan to consider other online platforms in order to cross-validate the Reddit-based results reported in this paper. We also plan to run some empirical studies such as surveys and interviews to overcome the problem of relying on online platform data and to identify other ways to reach out to more people in the target population.

Due to the relatively small size of our dataset, our study might not be very representative of the perception of shared home users, but it raises important points on S&P behaviours of rented shared home users, including the landlord-tenant relationship and possible threat actors inside a shared home. Additionally, it would be interesting to extend the participants to include multi-user views from traditional family settings as well to get an overall S&P perception of multi-user residents in rented accommodations. Furthermore, the current work specifically focuses on privately

[5] https://www.socialchamp.io/blog/reddit-demographics/

rented homes, as more than 80% of our participants lived in such homes. It would be interesting to explore specific communal living, such as student or staff accommodations and/or hostels, to understand whether the S&P perspectives of these places differ from the current study as the control of devices and resources in these kinds of homes are even more centralised; the WiFi is shared with a comparatively larger group of people than a privately rented shared accommodation, which may increase S&P vulnerabilities of shared home users.

6 Conclusion

Understanding the perspectives of shared home users is an important part of understanding the multi-user perspectives in a smart home. Using a survey and analysis of posts from the online forum Reddit, this study identified several relevant S&P behaviours and concerns of residents of shared homes, such as the prevalence of multiple primary users and concerns due to cyber-physical threats. The research reflected on threat actors and analysed the 'insider threats' in connection to a smart home, which are specific to a shared home setting, while commenting on specific user roles, their contextual variations, and the unique S&P role held by the landlords. The study suggested further research into insider threats specific to shared homes and exploring the varying roles of shared home users, considering the burgeoning interest in the area.

References

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2, Article 116 (2020), 28 pages. https://doi.org/10.1145/3415187

[2] Mahdi Nasrullah Al-Ameen, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna. 2021. "We, three brothers have always known everything of each other"": A Cross-cultural Study of Sharing Digital Devices and Online Accounts. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 203–224. https://doi.org/10.2478/popets-2021-0067

[3] Abayomi Alase. 2017. The Interpretative Phenomenological Analysis (IPA): A Guide to a Good Qualitative Research Approach. *International Journal of Education and Literacy Studies* 5, 2 (2017), 9–19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

[4] Irwin Altman. 1975. *The environment and social behavior: privacy, personal space, territory, and crowding.* ERIC.

[5] Irwin Altman. 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues* 33, 3 (1977), 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

[6] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2022. You, Me, and IoT: How Internet-connected Consumer Devices Affect Interpersonal Relationships. *ACM Transactions on Internet of Things* 3 (2022). Issue 4. https://doi.org/10.1145/3539737

[7] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. In *Proceedings of the 18th Symposium on Usable Privacy and Security*. USENIX Association. https://www.usenix.org/conference/soups2022/presentation/bernd

[8] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet*. USENIX Association, 14 pages. https://www.usenix.org/conference/foci20/presentation/bernd

[9] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. 2019. Smart Home Bystanders: Further Complexifying a Complex Context. In *Proceedings of CI Symposium 2019*. PrivaCI, 6 pages. https://privaci.info/symposium2/papers_and_slides/Sub_Bernd_et_al_Bystanders_CI_2019.pdf

[10] Nicola Bleu. 2023. 23+ Reddit Statistics For 2023: Users, Revenue, And Growth. https://startupbonsai.com/reddit-statistics/

[11] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2019. Thematic Analysis 48. *Handbook of research methods in health social sciences* (2019), 843–860. https://doi.org/10.1007/978-981-10-5251-4_103

[12] BT. 2020. 83% of UK consumers are planning to gift a connected device as families get set for Christmas, according to study by BT Full Fibre. https://newsroom.bt.com/83-of-uk-consumers-are-planning-to-gift-a-connected-device-as-families-get-set-for-christmas-according-to-study-by-bt-full-fibre/

[13] Michael Byrne and Rachel McArdle. 2022. Secure occupancy, power and the landlord-tenant relation: a qualitative exploration of the Irish private rental sector. *Housing Studies* 37, 1 (2022), 124–142. https://doi.org/10.1080/02673037.

2020.1803801

[14] Jiayi Chen, Urs Hengartner, and Hassan Khan. 2022. Sharing without Scaring: Enabling Smartphones to Become Aware of Temporary Sharing. In *Proceedings of the 18th Symposium on Usable Privacy and Security*. USENIX Association, 671–685. https://www.usenix.org/conference/soups2022/presentation/chen

[15] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating Receptiveness to Sensing and Inference in the Home Using Sensor Proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 61–70. https://doi.org/10.1145/2370216.2370226

[16] Vicky Clark, Keith Tuffin, Natilene Bowker, and Karen Frewin. 2019. Rosters: Freedom, responsibility, and co-operation in young adult shared households. *Australian Journal of Psychology* 71, 3 (2019), 232–240. https://doi.org/10.1111/ajpy.12238

[17] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections"": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 54–75. https://doi.org/10.2478/popets-2021-0060

[18] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 54–75. https://doi.org/10.2478/popets-2021-0060

[19] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proceedings of the 15th Symposium on Usable Privacy and Security*. USENIX Association, 97–115. https://www.usenix.org/conference/soups2019/presentation/das

[20] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *Proceedings of the 10th Symposium On Usable Privacy and Security*. USENIX Association, 143–157. https://www.usenix.org/conference/soups2014/proceedings/presentation/das

[21] Department for Levelling Up, Housing and Communities and Ministry of Housing, Communities & Local Government, UK Government. 2019. Guidance Landlord and tenant rights and responsibilities in the private rented sector. https://www.gov.uk/government/publications/landlord-and-tenant-rights-and-responsibilities-in-the-private-rented-sector/landlord-and-tenant-rights-and-responsibilities-in-the-private-rented-sector#landlords-rights-responsibilities-and-advice

[22] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J Wisniewski. 2020. Exploring smart home device use by airbnb hosts. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article LBW082, 8 pages. https://doi.org/10.1145/3334480.3382900

[23] Oana Druta and Richard Ronald. 2021. Living alone together in Tokyo share houses. *Social & Cultural Geography* 22, 9 (2021), 1223–1240. https://doi.org/10.1080/14649365.2020.1744704

[24] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 13 pages. https://doi.org/10.1145/3290605.3300498

[25] Greater London Authority. 2022. Housing in London 2022. https://data.london.gov.uk/housing/housing-in-london/

[26] Manjul Gupta, Pouyan Esmaeilzadeh, Irem Uz, and Vanesa M. Tennant. 2019. The effects of national cultural values on individuals' intention to participate in peer-to-peer sharing economy. *Journal of Business Research* 97 (2019), 20–29. https://doi.org/10.1016/j.jbusres.2018.12.018

[27] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *Proceedings of the 27th USENIX Security Symposium*. USENIX Assocaition, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[28] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. 2021. SoK: Context Sensing for Access Control in the Adversarial Home IoT. In *Proceedings of the 2021 IEEE European Symposium on Security and Privacy*. IEEE, 37–53. https://doi.org/10.1109/EUROSP51992.2021.00014

[29] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428. https://doi.org/10.1016/j.cose.2018.07.011

[30] Eric Hirsch and Roger Silverstone. 2003. Information and communication technologies and the moral economy of the household. In *Consuming Technologies*. Routledge, 25–40.

[31] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. 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*. ACM, Article 402, 13 pages. https://doi.org/10.1145/3313831.3376529

[32] Kath Hulse and Vivienne Milligan. 2014. Secure occupancy: A new framework for analysing security in rental housing. *Housing Studies* 29, 5 (2014), 638–656. https://doi.org/10.1080/02673037.2013.873116

[33] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing: Couples' Practices in Single User Device Access. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work*. ACM, 235–243. https://doi.org/10.1145/2957276.2957296

[34] Matthew R. Jamnik and David J. Lane. 2019. The use of Reddit as an inexpensive source for high-quality data. *Practical Assessment, Research, and Evaluation* 22, 1, Article 5 (2019), 10 pages. https://doi.org/10.7275/j18t-c009

[35] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling Multi-User Controls in Smart Home Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, 49–54. https://doi.org/10.1145/3139937.3139941

[36] Shravya Kanchi and Kamalakar Karlapalem. 2021. A Multi Perspective Access Control in a Smart Home. In *Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*. ACM, 321–323. https://doi.org/10.1145/3422337.3450324

[37] Leah Komen. 2016. "Here you can use it": Understanding mobile phone sharing and the concerns it elicits in rural Kenya. *for(e)dialogue* 1, 1 (2016), 52–65. https://doi.org/10.29311/for(e)dialogue.v1i1.532

[38] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598

[39] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598

[40] Stephanie Kramer. 2020. With billions confined to their homes worldwide, which living arrangements are most common? https://www.pewresearch.org/short-reads/2020/03/31/with-billions-confined-to-their-homes-worldwide-which-living-arrangements-are-most-common/

[41] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 102 (2018), 31 pages. https://doi.org/10.1145/3274371

[42] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *Proceedings of the 2019 ACM Designing Interactive Systems Conference*. ACM, 527–539. https://doi.org/10.1145/3322276.3322366

[43] Vanessa Z. Lin and Simon Parkin. 2020. Transferability of privacy-related behaviours to shared smart home assistant devices. In *Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security*. IEEE, 8 pages. https://doi.org/10.1109/IOTSMS52051.2020.9340199

[44] George Loukas. 2015. *Cyber-Physical Attacks: A Growing Invisible Threat*. Butterworth-Heinemann.

[45] Sophia Maalsen. 2020. 'Generation Share': digitalized geographies of shared housing. *Social & Cultural Geography* 21, 1 (2020), 105–113. https://doi.org/10.1080/14649365.2018.1466355

[46] Sophia Maalsen. 2023. 'We're the cheap smart home': the actually existing smart home as rented and shared. *Social & Cultural Geography* 24, 8 (2023), 1383–1402. https://doi.org/10.1080/14649365.2022.2065693

[47] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271. https://doi.org/10.2478/popets-2019-0068

[48] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2000, 2 (2020), 436–458. https://doi.org/10.2478/popets-2020-0035

[49] Karola Marky, Paul Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. 2022. "You offer privacy like you offer tea"": Investigating Mechanisms for Improving Guest Privacy in IoT-Equipped Households. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022), 400–420. https://doi.org/10.56553/popets-2022-0115

[50] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 83–95. https://doi.org/10.1145/3428361.3428464

[51] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles matter! Understanding differences in the privacy mental models of smart home visitors and residents. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 108–122. https://doi.org/10.1145/3490632.3490664

[52] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2022. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 108–122. https://doi.org/10.1145/3490632.3490664

[53] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences,*

Shaping Society. ACM, Article 4, 11 pages. https://doi.org/10.1145/3419249.3420164
[54] Karola Marky, Verena Zimmermann, Alina Stöver, Philipp Hoffmann, Kai Kunze, and Max Mühlhäuser. 2020. All in One! User Perceptions on Centralized IoT Privacy Settings. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article LBW071, 8 pages. https://doi.org/10.1145/3334480.3383016
[55] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "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*. ACM, 5921–5932. https://doi.org/10.1145/2858036.2858051
[56] Dana McKay and Charlynn Miller. 2021. Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Article 332, 14 pages. https://doi.org/10.1145/3411764.3445114
[57] Nicole Meng. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1, Article 45 (2021), 29 pages. https://doi.org/10.1145/3449119
[58] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L. Mazurek. 2022. Characterizing Everyday Misuse of Smart Home Devices. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy*. IEEE, 1558–1572. https://doi.org/10.1109/SP46215.2023.00089
[59] Becky Mortan. 2022. Over-50s turn to house-shares to beat rising rents. https://www.bbc.co.uk/news/business-62344571
[60] Megan Nethercote. 2019. Caring households: The social ties that house. *Housing, Theory and Society* 36, 3 (2019), 257–273. https://doi.org/10.1080/14036096.2018.1465994
[61] Megan Nethercote. 2023. Platform landlords: Renters, personal data and new digital footholds of urban control. *Digital Geography and Society* 5, Article 100060 (2023), 15 pages. https://doi.org/10.1016/j.diggeo.2023.100060
[62] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (2004), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10
[63] Tushar P Parikh and Ashok R Patel. 2017. Cyber security: Study on attack, threat, vulnerability. *2017 International Journal of Research in Modern Engineering and Emerging Technology* 5, 6 (2017).
[64] Albert Park, Mike Conway, and Annie T. Chen. 2018. Examining thematic similarity, difference, and membership in three online mental health communities from reddit: A text mining and visualization approach. *Computers in Human Behavior* 78 (2018), 98–112. https://doi.org/10.1016/j.chb.2017.09.001
[65] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proceedings of the 14th Symposium on Usable Privacy and Security*. USENIX Association, 83–102. https://www.usenix.org/conference/soups2018/presentation/park
[66] Sunjeong Park and Youn-kyung Lim. 2020. Investigating User Expectations on the Roles of Family-Shared AI Speakers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article 323, 13 pages. https://doi.org/10.1145/3313831.3376450
[67] Nandita Pattnaik, Shujun Li, and Jason R. C. Nurse. 2023. A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. *Comput. Surveys* 55, 9, Article 180 (2023), 38 pages.
[68] Rizu Paudel, Prakriti Dumaru, Ankit Shrestha, Huzeyfe Kocabas, and Mahdi Nasrullah Al-Ameen. 2023. A Deep Dive into User's Preferences and Behavior around Mobile Phone Sharing. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1, Article 119 (2023), 22 pages. https://doi.org/10.1145/3579595
[69] Nicholas Proferes, Naiyan Jones, Sarah Gilbert, Casey Fiesler, and Michael Zimmer. 2021. Studying Reddit: A Systematic Overview of Disciplines, Approaches, Methods, and Ethics. *Social Media + Society* 7, 2 (2021), 14 pages. https://doi.org/10.1177/2056305121101900
[70] Reddit. 2023. Data API Terms. https://www.redditinc.com/policies/data-api-terms
[71] Tiago Rocha-Silva, Conceição Nogueira, and Liliana Rodrigues. 2023. Passive data collection on Reddit: a practical approach. *Research Ethics*, Article 17470161231210542 (2023), 18 pages. https://doi.org/10.1177/17470161231210542
[72] Richard Ronald, Pauline Schijf, and Kelly Donovan. 2023. The institutionalization of shared rental housing and commercial co-living. *Housing Studies* (2023), 1–25. https://doi.org/10.1080/02673037.2023.2176830
[73] Indira Sen, Fabian Flöck, Katrin Weller, Bernd Weiß, and Claudia Wagner. 2021. A total error framework for digital traces of human behavior on online platforms. *Public Opinion Quarterly* 85, S1 (2021), 399–422.
[74] Julia Slupska. 2019. Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review* 15, 1 (2019), 83–100. https://www.jstor.org/stable/27027755
[75] Julia Slupska and Leonie Maria Tanczer. 2021. Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald. https://doi.org/10.1108/978-1-83982-848-520211049
[76] Julia Muller Spiti, Ellen Davies, Paul McLiesh, and Janet Kelly. 2022. How social media data are being used to research the experience of mourning: A scoping review. *PLOS ONE* 17, 7, Article e0271034 (2022), 25 pages. https://doi.org/10.1371/journal.pone.0271034

[77] Statista. 2021. Average number of devices residents have access to in UK households in 2020, by device. https://www.statista.com/study/41673/connected-devices-in-the-united-kingdom-uk/

[78] Madiha Tabassum and Heather Lipford. 2023. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 571–588. https://doi.org/10.56553/popets-2023-0033

[79] Sarah Turner, Nandita Pattnaik, Jason R.C. Nurse, and Shujun Li. 2022. "You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2, Article 269 (2022), 34 pages. https://doi.org/10.1145/3555159

[80] Constance Uyttebrouck, Ellen Van Bueren, and Jacques Teller. 2020. Shared housing for students and young professionals: evolution of a market in need of regulation. *Journal of Housing and the Built Environment* 35, 4 (2020), 1017–1035. https://doi.org/10.1007/s10901-020-09778-w

[81] Juite Wang and Y.-L. Liu. 2023. Deep learning-based social media mining for user experience analysis: A case study of smart home products. *Technology in Society* 73, Article 102220 (2023), 18 pages. https://doi.org/10.1016/j.techsoc.2023.102220

[82] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable"": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article 478, 12 pages. https://doi.org/10.1145/3313831.3376605

[83] Chathurangi Ishara Wickramasinghe and Delphine Reinhardt. 2019. A Survey-Based Exploration of Users' Awareness and Their Willingness to Protect Their Data with Smart Objects. In *Privacy and Identity Management. Data for Better Living: AI and Privacy – 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*. Springer, 427–446. https://doi.org/10.1007/978-3-030-42504-3_27

[84] Eleanor Wilkinson. 2014. Single people's geographies of home: intimacy and friendship beyond 'the family'. *Environment and Planning A* 46, 10 (2014), 2452–2468. https://doi.org/10.1068/a130069p

[85] Eleanor Wilkinson and Iliana Ortega-Alcázar. 2019. Stranger danger? The intersectional impacts of shared housing on young people's health & wellbeing. *Health & Place* 60, Article 102191 (2019), 7 pages. https://doi.org/10.1016/j.healthplace.2019.102191

[86] Michael Williams and Tami Moser. 2019. The art of coding and thematic exploration in qualitative research. *International management review* 15, 1 (2019), 45–55.

[87] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI, Article 184 (2022), 21 pages. https://doi.org/10.1145/3546719

[88] Yuxi Wu, W. Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. In *Proceedings of the 2022 IEEE Symposium on Security and Privacy*. IEEE, 1863–1879. https://doi.org/10.1109/SP46214.2022.9833757

[89] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 59 (2019), 24 pages. https://doi.org/10.1145/3359161

[90] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security*. USENIX Association, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[91] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *Proceedings of the 28th USENIX Security Symposium*. USENIX Association, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[92] Bo Zhao. 2020. Unraveling Home Protection in the IoT Age: Living, Mixed Reality, and Home 2.0. *Science and Technology Law Review* 21, 1 (2020), 43–80. https://doi.org/10.7916/stlr.v21i1.5763

[93] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216. https://doi.org/10.1515/icom-2019-0015

Appendix: Survey Questionnaire

Investigating users' security and privacy perspectives in a shared home environment

Section A: Demographic

A2. What is your age?

A3. Do you hold a degree (Bachelor's or above) or above in an ICT-related subject? A4. Do/Did you have an ICT-related job?

A5. What type of shared house do/did you live in?

A6. How many total residents are in your current or last shared home including you?

A7. Do you have one or more computing devices in your shared home provided and/or maintained by your landlords or the property owner/manager, such as routers, smart security cameras, smart thermostats or smart locks?

A8. Did you receive any relevant document(s) from your landlord or the property owner/manager which gives information regarding the provided device(s)?

Section B: Use of Network

B1. Who owns your router?

I don't have a router inside my shared home, but I got the WiFi connection from a central network (e.g., access points provided by a university or a hospital).

I bought my router when I started sharing the home, and all occupants share(d) it. Another occupant of the shared home bought a router, which is/was shared with me and other occupants.

Each occupant has their own router.

There is a shared router, but some occupants also have a personal one. Other

B2. Do you all share one WiFi password?

B3. Do / Did any of you in the shared home have admin right on the router (i.e., you and/or one or more other occupants can change the router settings)?

B3a. What router settings did you try to change? Please choose all that apply:

Changing the router's admin password. Changing the WiFi access password. Setting up a guest network.

Checking devices connected to the router. I don't know how to make any change. I never thought about it. Other:

B4.Do/Did you share the WiFi access password you and other occupants use with visitors to your shared home?

Yes, and we didn't change the password after the visitors left. Yes, and we

changed the password after the visitors left.

No, we set up a separate network with a different password for the visitors. Other

B5. Is / Was your WiFi access password commonly accessible by anyone visiting your shared home, e.g., is / was the router placed in a common area and the

password is/was visible to everyone)?

Yes, the password is attached to the router placed in a common area.

Yes, the password is not attached to the router but is shown in a common area (i.e., on a noticeboard

or a fridge door).

No, the WiFi access password is/was not made visible to anyone. Other

B6. Are you aware that your WiFi can be spied on, and anyone might steal your information if you don't have a secure network?

Yes

No

I don't care

I didn't think about it Other

B7. Do you think the WiFi network is less secure when you live(d) in a shared home than in a traditional family home?

Yes, mostly because I don't fully trust other co-occupant(s).

I thought that when I just moved in, but now/later I trust(ed) other co-occupant(s). Yes, although I

trust other co-occupant(s), I don't/didn't trust their guests.

Yes, the shared home is/was constantly exposed to strangers, so I feel/felt worried. No, both are

similar in terms of security. I trust(ed) other co-occupant(s).

I am not sure about this.

I never thought about this. Other

Section C. Use of Devices

C1. Did you or your co-occupant(s) share any of your/their computing devices at any point in time? Please choose all that apply:

Yes, I shared my laptop, PC and/or tablets with other co-occupant(s). Yes, other co-occupant(s) shared their laptop, PC and/or tablets with me. Yes, I shared my smart phones with other co-occupant(s).

Yes, other co-occupant(s) shared their smart phones with me. Yes, I shared my router with other co-occupant(s).

Yes, other co-occupant(s) shared their router(s) with me. Yes, we shared some smart home devices.

No, neither I nor other co-occupant(s) shared any of my/their devices.

I don't remember I or other co-occupant(s) shared any of my/their devices, but I cannot be sure.

Other:

C2. Do/Did you get worried sometimes that your co-occupant(s) or their guests might spy on you using shared computing devices?

Yes

No

Other

C3. Have you ever had any security or privacy problems after sharing your computing device, such as malware infection, illegal download, data loss, etc.? If yes, please specify the nature of such problem(s).

Yes (please specify) No

Other (please specify)

C4. If you have any of the following devices at home, please specify who owns/manages them. Click all that apply.

	Landlord / Property owner /Manager	My co-occupants	Myself	Multiple people own this device	We don't have this device	I am not sure
Router	◯	◯	◯	◯	◯	◯
Smart thermostat	◯	◯	◯	◯	◯	◯
Smart Lock	◯	◯	◯	◯	◯	◯
Smart Speaker (Amazon Echo, Samsung SmartThings, Apple HomeKit etc)	◯	◯	◯	◯	◯	◯
Smart security camera - External	◯	◯	◯	◯	◯	◯
Smart security camera - Internal	◯	◯	◯	◯	◯	◯
Smart door bell (such as Amazon Ring / Google Nest)	◯	◯	◯	◯	◯	◯
Smart freeze	◯	◯	◯	◯	◯	◯
Smart TV	◯	◯	◯	◯	◯	◯

C5. Do you / your housemate share any smart hub such as Amazon Echo/ Samsung SmartThings / Philip Hue / Apple HomeKit?

Yes

We don't have any smart hub

We have more than 1 smart hub and some are shared Other

C5a. Is your or your housemate's smart hub kept in a common area and accessible by all of your housemate/guests/friends?

Yes

No

Other

C5b. Have you / your housemate set an individual voice profile for your smart hub ?

Yes No

I am not aware about this

Other

C5c. Is your smart hub kept in a publicly accessible area i.e. Living room/Kitchen

Yes

No

Other

C5d. Are you concerned about your privacy while sharing your smart hub with your co- occupant(s)?

Yes

No

Other

C7. If your house has a smart security camera or Smart Video Doorbell, then who could access the camera recordings?

All housemates

The Landlord

I am not sure

I never thought about it

We don't have any of the above

Other

C6. You might want to buy a smart hub or not. But please choose 'other' for this question and write the word "SmartHub"? This question is for attention check.

Yes, No, Other

C8. Did you keep your smart speaker and/or other computing devices, such as laptops/tablets, in a secure place when you had a party/get-together event where you expected people other than your co- occupant(s)?
If this never happened, tell us what you would have done if it did happen

Yes

No

Never thought about it Other

C9. Are/Were you concerned about any privacy and security risks from your co-occupant(s) and/or your/their visitors? Please choose **all** that apply:

No, not from my co-occupant(s)

No, not from my co-occupant(s)' visitors No,
not from my visitors

Yes, from my co-occupant(s) (sometimes)

Yes, from my co-occupant(s) (always)

Yes, from my co-occupant(s)' visitors (sometimes)

Yes, from my co-occupant(s)' visitors (always) Yes,
from my visitors (sometimes)

Yes, from my visitors (always) Other:

C10. Are/Were you concerned about your computing devices being tampered with and the data being stolen when you are/were not at the shared home but your co- occupant(s) or their visitors are/were present? Please choose **all** that apply:

Yes, from my co-occupant(s)

Yes, from my co-occupant(s)'s visitors

No, neither from my co-occupant(s) nor from their visitors I don't care about this I
never thought about it

Other:

C11. Do you think your devices (both traditional computing and smart) are less secure in a shared home than in a traditional family home?

Yes

No

Not sure

Other

C12. Do you think that if your co-occupant(s)'s computing devices are compromised by malware, your devices might also get affected?

Yes

No

I don't think so

I don't have the right knowledge to make a judgment. Other

C13. Have you ever faced a situation where your security and/or privacy were adversely affected due to the negligence of yourself or your co-occupant(s)?

Yes

No

Other

C14. Have you ever discussed how to maintain the privacy and security of computing (traditional and smart) devices with your co-occupant(s)? Please choose **all** that apply:

Yes, on placement of routers/smart speakers

Yes, on (not) sharing passwords of routers/smart locks/security cameras Yes,

on creating a guest network

Yes, on not allowing people to use their laptops/PCs in the network unless appropriate antivirus/malware protection is taken.

Yes, other privacy or security-related topics concerning your home

Other:

C15. Have you ever sought/provided help from/to your housemate in relation to the privacy and security problems/configurations? Please choose **all** that apply:

Yes, on configuring security or privacy settings of devices (traditional computing devices or smart devices)

Yes, to solve a security/privacy problem (i.e. clean virus infected laptops, decide what to do on a phishing message etc.)

Yes, to ask advice on security or privacy (i.e. how to setup a VPN, how to create cloud backup of your data, how to buy a security software, to set up MFA etc.)

Other:

C16. The following is a list of common security precautions. Please tick option(s) which you think is/are important in a shared home setting. Please choose **all** that apply:

Installing anti-malware (anti-virus, anti-spyware) Backing up my data regularly

Using a VPN

Updating software on my devices (both computing and smart devices) regularly Keeping important documents protected by password and/or encryption

Using a password manager Using strong complex passwords

Using Multi-Factor Authentication (MFA) when it is available Being more aware of phishing

Being more aware of phishing

Not sharing my passwords with others

Setting up and reviewing privacy and security settings of my devices regularly All of them

Other:

C17. Which of the following options do/have you take/taken to protect your privacy & security in the shared home? Please choose all that apply:

I don't use smart speaker to call anyone when other people are around.

I keep my smart speaker in my own room away from open access area such as a living room or Kitchen. I switch off my laptop/tablets and keep them in a secure place when I am not using them.

I have created voice profiles for myself to use my smart speaker.

I lock my laptop/PC or put it into sleeping/hibernation mode when I leave them temporarily. I usually don't think about such problems so don't take precaution.

I can't be bothered to deal with all the complicated problems and precaution. Other:

Received July 2023; revised April 2024; accepted July 2024