Location, Location, Security? Exploring Location-Based Smart Device Security Concerns and Mitigations within Low-Rent Homes

Laura Benton
UCL Knowledge Lab, University College London
l.benton@ucl.ac.uk

Asimina Vasalou
UCL Knowledge Lab, University College London
a.vasalou@ucl.ac.uk

Sarah Turner
School of Computing, University of Kent
slt41@kent.ac.uk

ABSTRACT

The increasing adoption of smart devices in the home introduce new security implications for tenants, with previous research showing the significance of where the devices are placed. This paper examines the relationship between device location and security: we ask how users' security concerns shape where they place their smart devices and how they attempt to mitigate their concerns. The research focuses on an underrepresented group, those people living in social (low-rent) housing, motivated by the growing interest of housing providers to install smart devices within tenants' homes. Using speculative design as a probe followed by interviews with eleven tenants, we find that security concerns are centred around 'intimate places', 'social responsibility' and 'surveillance' with users combining social practices and technical security features to mitigate these. Our research contributes new ethical implications for deploying and designing smart home devices addressed to social housing providers and smart device designers.

CCS CONCEPTS

• **Human-centered computing**; • **Human computer interaction (HCI)**; • **Empirical studies in HCI**;

KEYWORDS

Security, Privacy, Smart devices, Speculative design, Social housing

ACM Reference Format:
Laura Benton, Asimina Vasalou, and Sarah Turner. 2023. Location, Location, Security? Exploring Location-Based Smart Device Security Concerns and Mitigations within Low-Rent Homes. In *Designing Interactive Systems Conference (DIS '23), July 10–14, 2023, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3563657.3596077

1 INTRODUCTION

For many people our homes are the places that we feel (or seek to feel) most secure and in control [38]. However, in recent years the increasing number and variety of smart devices that are being designed for, and introduced into, the domestic environment to improve people's wellbeing and comfort have also raised new security concerns. These concerns are important to understand, particularly in cases where the devices are introduced by external parties, such as landlords or housing providers, whereby the occupants may have less control over the choice and use of the smart device. Recent research has thus begun to consider the impact of smart devices on other householders and visitors [51], people staying in different forms of rental accommodation [52], domestic cleaners [39], and nannies [4]. Geeng and Roesner [23] recommend that smart device designers consider the relationships between "*smart home installers or drivers and other occupants, or in non-traditional home units, including partners, roommates, children and parents, older adults, landlords and tenants, people in potentially abusive relationships*". They highlight the example of landlords installing smart devices in a renter's home, suggesting that tenants should have control about how the devices are used and the data they collect. [33]

Contextualised in these socio-technical trends, our research is concerned with the introduction and use of smart devices in the UK's social housing sector. The social housing sector provides housing at more affordable rents for those living on low incomes, with around 4 million households living in social housing in England alone. A quarter of this population are aged over 65, a third have dependent children and over half of the households include someone with a long-term illness or disability. As a whole, this is a group that includes some of the most vulnerable people in society experiencing inequalities due to intersectional factors [13]. Social housing providers are legally obliged to monitor and maintain their housing stock to an adequate living standard [54], though the age of their properties and the lack of funding for refurbishment can often result in properties being damp and mouldy [29]. Stemming from the economic inequalities they experience tenants can struggle to heat their homes which aggravates this problem [29]. Many industry experts propose that smart devices – and in particular, smart energy devices such as thermostats – offer a cost-effective way for housing providers to meet expected housing standards (e.g., by identifying potential disrepair issues earlier) [24]. This is expected to lead to significant efficiencies in the resolution of issues that are so prevalent in the current system that secondary legislation exists to reimburse tenants that have to carry out their own repairs as a result of their landlord's inaction [24]. It is likely that, in addition to these obligations, social housing providers will have to meet higher standards to meet governmentally-set Net Zero targets [34]. There is the expectation that the introduction of such devices will confer benefits on tenants as well, crucially avoiding the degradation of their living space that has profound consequences on their life expectancy, health, and wellbeing [7] whilst increasing their empowerment and equality [24]. This is recognised by current providers of devices aimed at the social housing market: those devices that are marketed

DIS '23, July 10–14, 2023, Pittsburgh, PA, USA

ACM ISBN 978-1-4503-9893-0/23/07.
https://doi.org/10.1145/3563657.3596077

to landlords for property maintenance purposes, are also marketed to tenants in social housing as a means of reducing energy bills and heating their homes more efficiently [42]. Both can be true at the same time, as issues like damp and mould in a property could be considered to be exacerbated by currently inefficient heating. Whilst most social housing providers are yet to proceed with widespread rollouts of these devices, some providers have been piloting smart devices (for example smart smoke alarms, sensors, and thermostats) in a small number of their tenants' homes and are now beginning to proceed with more significant installation projects [22].

Alongside their potential benefits, little attention has been given to the views of social housing tenants as they relate to the *near-future use* of smart devices and the security risks they may introduce in their homes. Addressing this gap, we report on a critical inquiry involving 11 tenants in social housing in the UK. Prior research on smart devices has shown that the particular placement of smart devices within different locations in the home can interact with their risks [9, 28, 37, 43, 52]. A situated lens that considers the social practices in the home context is thus necessary to theorise the complex set of trade-offs involved when balancing benefits and risks, or tenants' technical knowledge about how smart devices may operate. Informed by this perspective, we seek to contribute a critical understanding of how tenants living in social housing in the UK consider, negotiate, and balance benefits and security concerns in relation to a set of smart devices proposed to save costs on their heating. In taking a material speculative approach, we invited tenants to interact with three physical smart device probes to explore the use of a range of technical security features and social practices to mitigate their varied concerns. To prompt discussions around potential future domestic smart technology scenarios [17] these smart devices were chosen to embody existing functionality based on smart energy technologies already being used in social housing (e.g. a motion sensor monitoring typical home occupancy as found in the Switchee smart thermostat [15]) that would facilitate the consideration of *probable* futures. Additionally the devices embodied functionalities that were more controversial within the home and often raise security concerns [28, 43] (e.g. listening and recording conversations to provide relevant advice), as well as those that stretch the limits of current technical possibilities of commercial smart devices (e.g. visually identifying specific activities being undertaken in the home) to initiate reflections on *plausible* or *possible* futures.

Our research offers three key contributions. Firstly, it provides a theoretical account of social housing tenants' particular security concerns in relation to smart devices being introduced within their homes. Secondly, it informs the situated understanding of how people imagine living with smart devices and the impact of where different devices are located within their home. Finally, addressed to smart device designers and housing providers, it provides a range of social practices and technical security features informing ethical implications for future interventions.

2 BACKGROUND

2.1 Use and benefits of smart devices within rented homes

Despite being a widely used term across the academic literature, exactly what constitutes a 'smart' device is quite broad and loosely defined [38]. It is typically used to refer to devices, such as cameras and speakers, which are connected to the internet and provide users with a service that is automated as well as being context aware [9]. Smart home devices are marketed as improving domestic life in some way, for instance by providing additional comfort, an increased sense of security, the ability to schedule/automate tasks to achieve convenience, improving energy management as well as supporting health/everyday living and enabling independent living for disabled or elderly residents [41, 49]. Although the majority of research in this area has tended to focus on private or family homes [19, 27], researchers have started to explore the use of smart devices within different rental contexts, identifying benefits for both the tenants and landlords.

Mare et al. [32] explored the use of different smart devices in short-term AirBnB rental accommodation, with guests appreciating that these devices provided them with entertainment, convenience, additional comfort or luxury, as well as safety and security. Hosts also benefited in feeling that the smart devices provided them with better protection against property damage, or theft, as well as the ability to ensure house rules were followed. In a slightly different context, Denefleh et al. [12] focused on the relationship between tenants living in shared apartments and highlighted the benefits that smart devices might have in this case, for instance by creating positive connections between housemates or supporting positive pro-social behaviour changes, such as contributing to house chores. Additionally, Kozubaev et al. [27] considered the implications of smart technologies in public housing in the US. Tenants recognised the value of the devices particularly for their health, wellness, as well as personal safety, whereas housing administrators believed they could benefit in a variety of ways from the aggregation of the data collected by the smart devices.

2.2 Placement of smart devices within the home

Seeking to inform HCI research in the home, Coughlan et al. [44] have highlighted the importance of considering digital technology use in different spaces, since particular rooms/areas may be perceived as being more private than others. As smart devices operate by collecting data from the surrounding environment, *where* these devices are located within the home, in combination with the specific functionality embedded within the device, can impact both the potential usage scenarios and the extent of data that can be collected and stored. Tan et al. [43] refer to these physical types of smart devices (such as smart cameras) as 'spatially sensitive and perceptually powerful' due to their ability to track and record a range of data from extensive areas of the home. This enables them to generate broader and deeper insights about activity in the home, which could significantly impact householders' security practices and experiences.

Previous research in this area has mainly been undertaken within the context of smart speakers and cameras [9, 28, 37, 43, 52]. Lau et

al. [28] identified important criteria users took into consideration to determine where to place their smart device. These included choosing a location that was *central* within the home, or *frequently used* (often in the case of having multiple devices), as well as *closeness to other electronics/entertainment systems* to increase their ability to pick up as much voice audio as possible and maximise the utility of the device. Common rooms that these devices were placed within included the kitchen, living room and bedroom, with Sciuto et al. [37] suggesting that the choice of a specific room such as a bedroom tended to indicate the use of the smart device for a specific task (e.g. setting a wake-up alarm) whereas the placement in a shared area allows the device to be used for more open-ended purposes (e.g. listening to music). Security was not generally highlighted as a specific consideration by the smart device users in this decision-making process, however one participant interviewed by Zeng et al. [52] did mention how they ensured the smart camera was not placed pointing towards the interior of their house when they were at home due to security concerns.

2.3 Security and smart home devices

Dourish and Anderson [16] define security as "the state of being free from danger" and Coles-Kemp [30] highlights how people often consider the security risks arising from using a technology in relation to the benefit they gain from it. Acquisti et al. [2] elaborate on this suggesting that trade-offs associated with security decisions are "often complex and nuanced", exacerbated by uncertainty and ambiguity around the available choices and the extent to which tighter security controls could lead to restrictions on the functionality and subsequent value of using the technology. Furthermore, in reference to IoT devices, Emami-Naeini et al. [20] highlight that even if users want to find out more about device security they typically struggle to find relevant information.

Due to this complexity, security-related issues are often seen as secondary [18] compared to the actual utility of the technology [48], or the price/convenience of the device [46]. This can result in a lack of motivation to evaluate the risk-benefit trade-offs, also reflected within the context of smart home devices [43] where it has been found that users who do value security often choose simply not to have the devices at all [49]. Tan et al. [43] summarise six potential reasons behind users who exhibit apathy around smart device security: (i) having nothing to hide; (ii) low risk (e.g. of being hacked), (iii) benefits outweigh the risks, (iv) sufficient control over use; (v) not thought about, (vi) can't see the threats. Zeng et al. [52] highlight that the gaps in smart device users' understanding of the potential security threats, due to incomplete knowledge about the technical functioning of the smart devices, lead them to transfer best practices from other technologies or use ad-hoc strategies with no real benefits. This gap in knowledge also makes it difficult to make informed security decisions [1].

Security researchers acknowledge that smart devices within the home have the potential to introduce a number of significant risks, including "privacy risks as well as vulnerable and unreliable devices" [52]. However, security is not just a technical, but also a social phenomenon (encompassing privacy concerns) [16], which is especially important within the physical and intimate space of the home. Therefore, in line with Dourish and Anderson [16], we propose that a more holistic approach needs to be taken to look at both technical and social aspects in tandem ensuring people recognise and appreciate various trade-offs between functionality and security in relation to the introduction of smart devices within the home. Given the varied ways in which we live in our homes, the specific location of the smart device is interconnected with the surrounding social processes, and, as highlighted by Yao et al. [51], it is vital to understand the particular trade-off between security risks and device utility and how this changes based on the device's location within the home.

In this paper we therefore specifically consider the following research questions within the context of social housing tenants: (RQ1) *What benefits do tenants anticipate in smart devices that have been introduced into their living space and how do they choose to integrate them into their homes?* (RQ2) *What security implications do location choices for smart devices raise and how do tenants envision mitigating these?*

3 METHODOLOGY

3.1 Participants

Prior to recruiting for the study, an ethics application was evaluated by the University ethics board and ethics approval was granted. In keeping with this, participant names have been replaced with pseudonyms. We recruited participants via our existing networks as well as using the website 'Call for Participants'. Our selection criteria required participants to be 18+ and living in social housing within the UK. In total 11 people completed the full study spread across different regions in the UK (see Table 1). Participant ages ranged from 18 to 65. Out of the 11 participants, two of them were South Asian (the rest of the participants were white British) and two were male. Participants lived in a variety of social housing settings: six lived alone, four shared their house with family, and one lived in shared accommodation with flatmates. Four participants also had disabilities or health conditions that shaped how they lived, which aligns with the characteristics of this population [13]. Caitlin had a hearing impairment which required the use of a loudspeaker when on the phone. Grace's mild autism and past experiences with an eating disorder were supported by a social worker. Noah had cerebral palsy, requiring a wheelchair and walking sticks, and was reliant on his parents to help him daily. Zoe reported a rare brain condition, which nonetheless did not impact on her everyday life in relation to her technology use. Looking into participants' previous experiences with technology, there was a mix of technology expertise and experiences with smart devices, although all the participants regularly accessed the internet, and all had smartphones. In terms of their security concerns related to smart devices, whereas some participants had not considered these or were not concerned (Grace, Farah, Jatinder, Zoe), others were reluctant to introduce smart technologies into their houses due to the concerns they raised (Sharon, Agnes, Catilin, Helena, Eve, Mario, Noah).

3.2 Speculative design methods

Speculative design aims to explore and question "possible, plausible, probable and preferable futures" [47] and researchers have now begun to engage marginalised and underrepresented groups using

Table 1: Summary of Participant Information

Pseudonym	Age	Location	Technology confidence	Smart device experience	Living situation	Additional info
Sharon	55	Town in SE England	Quite confident	None reported	Alone	White
Agnes	65	Village in SE England	Quite confident	None reported	Dog	White
Caitlin	50	City in W Scotland	Not so confident	None reported	Alone	White; Hearing Impairment
Grace	26	City in SE England	Quite confident	Smart voice assistant	Dog	White; Autism, History of eating disorders
Helena	38	City in SE England	Quite confident	None reported	Alone	White
Farah	18	City in SE England	Very confident	Smart voice assistant, smart washing machine	Parents + 2 younger siblings	South Asian
Jatinder	23	City in SE England	Very confident	Smart voice assistant	3 x flatmates	South Asian
Eve	44	Town in mid-Scotland	Quite confident	Smart voice assistant	3 x children	White
Zoe	31	City in SW England	Quite confident	Smart doorbell	Partner	White; Rare brain disorder
Mario	39	City in SE England	Quite confident	None reported	Partner	White
Noah	28	City in NW England	Very confident	Smart toothbrush, thermostat and vacuum cleaner	Parents	White; Cerebral palsy, wheelchair user

these speculative-based methods [6, 26]. In our work, we wanted to arouse participants' imagination of what it might be like to live with a smart device in their home considering housing providers' exploration of this technology and the near-future possibilities of its introduction in tenants' homes. The methods used in our study to foster speculation around this theme consisted of three physical smart device probes and situated speculation booklets accompanying the devices (see Figure 1).

Physical smart device probes: One approach to triggering speculation is by creating an imagined near-future through extrapolating aspects of existing technology [14]. Informed by this, we focused on functionalities related to three common smart devices: a motion sensor, security camera and voice assistant The devices collected different but familiar data types (movement, voice, video). We hoped that through the combination and application of these to a smart energy scenario we would expand participants' imagined experiences with smart technology and security beyond existing lived experiences into the realm of the plausible and the possible. Furthermore, the selection of these devices was intended to support a deeper exploration of different smart technology functionalities and associated security concerns, and enable our findings to be applicable to the broader area of the smart home. We drew on the concept of material speculations proposed by Wakkary et al. [47] that use "actual and situated artifacts as knowledge and speculative materiality of everyday practices". In comparison to other envisioning methods, this work proposes that the physical artefact can foster lived experiences that are vital to elicit critical speculations. This lens informed our decision to create lifelike physical versions of the three smart devices (using 3D printing). In placing the physical probes in people's homes, we hoped to elicit embodied actions within their physical environment (e.g., through encouraging participants to move the probe in different spaces) arousing more authentic experiences of what it means to experience in/security with smart devices.

While the materiality of the physical probe communicated some technology affordances, we wanted to further develop these 'extrapolations'. This was done through two sets of customized stickers: stickers representing *core device* features, and stickers reflecting technical *security* features. Both feature sets were split into three categories, which for the core features were: setting up (the data the device could collect/store e.g., people in the house, temperature preferences), monitoring (the kinds of activities the device could track e.g., changing facial expressions, patterns of movement) and acting (the actions the device could take e.g., automatic heating adjustments, making heating recommendations). For the technical security features the categories were: monitoring (allow users to monitor what the device is doing e.g., using lights, covers), limiting (additional restrictions on more risky actions and/or data storage e.g., not sharing data with technology provider) and protecting (additional protective features e.g., passwords, security updates).

Representations of technology are a key consideration in speculative design methods and related research has explored ways to anchor speculation beyond functional features toward exploring issues [14]. Informed by past work [3], the core features were designed to be both *familiar* through their use in existing smart technology (e.g., tracking which room(s) there has been movement and when), as well as more *provocative* (e.g., monitoring individual facial expressions and body postures to look for signs of feeling too warm) in order to break away from participants' existing ways of thinking about smart devices [14]. In contrast to the core features, technical security features were inspired/adapted from existing

Figure 1: – Physical smart device probes (from left: camera, voice assistant and motion sensor)

technical security functionalities available in current smart technologies. In summary, the features presented were designed to invite reflections around the benefits and concerns of smart home technology at large, as opposed to informing functionally feasible features (i.e., we did not provide specific technical details about how these features would be implemented and interact with one another).

Situated speculation booklets: The application of the stickers was guided through a new booklet designed for the research. Desjardins et al. [14, 15] previously introduced *bespoke booklets* as a way to support speculative exploration around IoT devices within the home by (1) "situating speculation in real world situations" and (2) facilitating co-speculation between researchers and participants. In representing people's living spaces through photographs embedded in the booklet's pages, the booklets invited them to layer sketches and written reflections that expressed their future visions of living with IoT. The booklets were thus designed to contextualise participants' speculations in their own physical spaces, and to also generate situated speculations whilst in their home. Inspired by this approach, we designed three new 'situated speculation' booklets to accompany each of the smart device probes directing our participants to speculate in their home. Each booklet situated the speculative smart energy scenario within the social housing context, as well as introduced the focal physical smart devices, an elaborated explanation of technology features and the customized sticker sets (Figure 2 illustrates the elaborated core and technical security features presented within one of the situated speculation booklets for the smart voice assistant; see Appendix A.1 and A.2 for a complete list of features presented for the three smart devices). These stickers were intended to support co-speculation with participants by prompting them to imagine possible future smart energy systems through customising the functionality and security features of each device, which they subsequently envisioned in their everyday life. Given participants' variable prior experiences with smart devices, six criteria were presented alongside the features to support their decisions:

- How much time you would want to spend giving direct instructions to your smart device
- What and how much personal information you would be happy for your smart device to know about you
- To what extent you would trust the smart device to make appropriate decisions about your heating on its own, without your input
- How the security features would impact the way the device would function
- If the security feature would protect against a risk you are actually worried about
- If the security feature is easy to turn on or would it require additional time to set up

Once the features had been chosen and physically attached to the smart device probe through the stickers, the booklet instructed participants to place the corresponding device probe in the most appropriate room of their home. To gauge participants' acceptance of the smart devices across different home spaces, using the booklet, participants indicated which other rooms they would allow the device to work in. After using the booklet to register the smart device features and room location selections, in alignment with Desjardins et al. [14], the booklet presented a series of reflective prompts inviting participants' to reflect on their experiences living with the smart device probe. The questions centred on heating and other benefits (i.e., whether they thought the smart device would benefit them and make appropriate heating decisions), security concerns (i.e., if the smart device might present a security threat to them, or other people in their household), and location preferences (i.e., whether the smart device location had any impact on their security concerns while living with the device). Given the extended

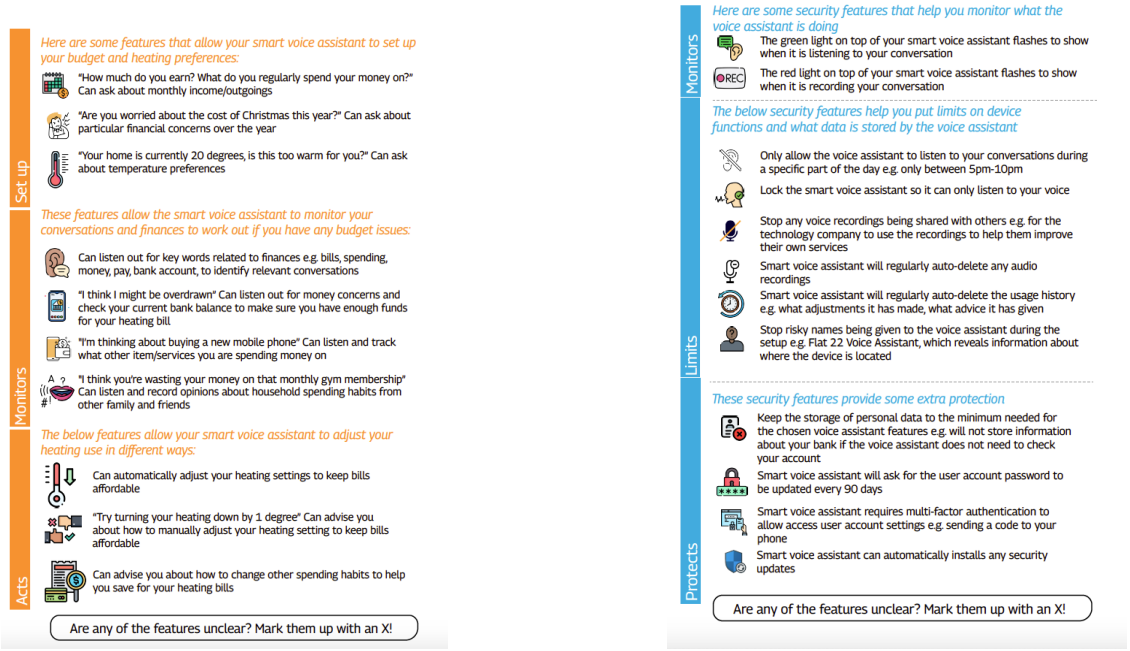

Figure 2: Core features (left) and Technical security features (right) from the Smart Voice Assistant situated speculation booklet. Image icons made by Freepik, Eucalyp, Flat Icons, Smashicons and Pixel perfect from www.flaticon.com.

timeframe between using the first smart device and the final interview, these written reflections also offered a way to capture critical reflections.

3.3 Context and procedure

The study took place in participants' homes during winter 2021/22. An introductory discussion was firstly arranged with the participant. All of the participants were competent using video conferencing, and we provided them with the choice to conduct the initial discussion either face-to-face (2 participants) or remotely i.e. phone or video conferencing (3 and 6 participants respectively). This discussion aimed to present the goals of the research, obtain ethical consent, and explain the timeline as well as the nature of the participation. It also provided an opportunity to explore the participant's current living circumstances, their use of technology at home, their previous direct or indirect experience of security breaches, their awareness and use of smart technologies for the home, as well as their concern around using these. The discussion was audio-recorded, informing a deeper understanding of each participant's living situation (see 3.1), and providing crucial context to later interpret the ways they made sense of smart technology in their homes.

To situate the smart device probes in tenants' relations with their landlord, participants were instructed to imagine that their housing provider had decided to install a smart heating system in their property, and they had the opportunity to customize the functionality and technical security features of three smart energy devices. As described in the introduction, smart energy is area of joint interest between housing providers and tenants, given policy targets in relation to Net Zero and increasing energy prices [35, 36] and the possibilities these devices afford for supporting repair. The researcher introduced the broad relationship between the device's 'smart' functionality, energy conservation and cost savings, leaving the space open for participants to bring their own interpretations for how the technology could work and readings about the potential benefits of this technology. A 'Context and Activities' information sheet was designed to introduce the study's imaginary scenario:

> *"Imagine your housing provider has recently installed a smart heating system in your property. During the cold winter days, it can be challenging to keep your home heated comfortably and affordably. The smart energy system could be the answer – it can work within any budget to ensure that your home is heated consistently, and you are not paying more that you need to heat your home comfortably. The smart energy system includes 3 smart devices. Over the next week you have been asked to review the core features and security features of each smart device and to customise these to your own personal preferences. How would you like this technology to work within your home? You have been provided with a 'smart energy system' kit. It contains a (non-functioning) 3D model of each device, a set of core feature stickers and a set of security features stickers. The devices are:*
>
> ***A Smart Voice Assistant:** monitors conversations to flag up money worries before they become a big problem. It adjusts your heating to ensure bills are within budget.*

> ***A Smart Motion Sensor:*** *looks out for who is in the house, what they are doing and how warm they might be feeling. It will turn your heating down or off completely to reduce your costs.*

> ***A Smart Camera****: looks out for behaviours that show you might be feeling too warm when the heating is on e.g. removing layers of clothing, fanning yourself, sweating. It will turn the heating down or off completely to reduce your costs.*

Through these initial instructions we introduced the participants to the three design tasks involving the technology probes and the situated speculation booklets. Participants received three packs, each containing one of the smart device probes and its associated situated speculation booklet. They interacted with each device (in a randomized order) guided by the corresponding booklet over a two-day period. During the first day, participants were asked to 'set up' their device probe using the two sets of stickers. This involved selecting a set of desirable features and physically attaching them on each smart device probe. Guided by the booklet, participants were then instructed to place the corresponding device probe in the most appropriate room of their home. On the second day participants were invited to experience and reflect on what it was like to live with the device probe documenting their reflections in the booklet. In keeping with our aim to situate participants' speculation in the material and everyday experiences with the smart devices (see 3.2), we asked them to engage with all three tasks, and thus there was no option given to reject using the probes. Each participant repeated the same task for each of their smart energy devices, following an order specified by the researcher to ensure that this varied between participants. Overall, the whole activity took participants around six days to complete.

3.3.1 Reflective Interview. Following the completion of the tasks, a reflective exit interview with the researcher was arranged. The interviews lasted on average 37 minutes [SD: 12.459] and were held either face to face, on the phone, or online mirroring participants' preferences from the entry interview. Participants were asked to share their completed situated speculation booklet which was used as a reference point during the interview. Upon inspection of the core features and technical security features attached to each smart device, participants were asked to share their reasoning for making these selections, including why they discarded other options presented to them in the situated speculation booklet. As part of this discussion, participants tended to volunteer security concerns connecting them to the smart device features they had chosen. This provided opportunities for further elaboration whereby participants often directed the conversation to the types of data each smart device collected. We also discussed the locations participants chose for each smart device, probing whether the participant believed the device fulfilled its objective to reduce their energy costs, and what security risks could be introduced or mitigated given where the device was placed. The discussion was facilitated to support participants' interpretations of the smart devices and foreground their distinctive concerns.

3.4 Data Analysis

The dataset consisted of transcriptions of the audio-recorded introductory and final interviews as well as the tenants' situated speculation booklet choices reflecting their choices of core/technical security features alongside the smart device locations they had selected. We also documented the reflective notes they wrote in each situated speculation booklet. Qualitative thematic analysis was carried out in line with [5]. The analysis primarily focused on the second interview, which was triangulated with the other data collected to enrich the interpretive process. For example, we compared tenants' verbal accounts of the features they had chosen with their responses in the booklets to ensure rigour in our analysis. Codes were generated through an inductive reading of the data to identify discrete concepts and patterns. These were iteratively reviewed by two of the authors and collated into themes. The next section reports the five main themes identified in our interviews with tenants aligned to our two overarching research questions.

4 FINDINGS

4.1 What benefits do tenants anticipate in smart devices that have been *introduced into their living space* and how do they choose to integrate them into their homes? (RQ1)

4.1.1 Identified benefits. Tenants recognised the potential benefits that the smart heating system, and its three devices, may provide in terms of **saving them money** from the expected reduction in heating bills. Caitlin highlighted the importance of this in terms of her current financial concerns: *"When you live on a low budget, energy always features, you know, really important. It's always been at the forefront of my mind. So yes, I would have it"*. Tenants also highlighted the convenience of being able to manage smart devices away from home, which would reduce the likelihood of the heating being left on unnecessarily for extended periods. Eve stated: *"In terms of going out the house and sometimes forgetting to turn the heating off that would automatically do it for me. That would be quite good"*.

Some tenants, however, were less convinced about the ability of the smart devices to make a tangible difference to their energy use, in the short term, at least: *"I think that benefit would obviously help like financial benefit, but I don't know how much of a difference it would actually make. Like I guess maybe, over time it would help, but not like any immediate difference, personally"* [Farah]. Other tenants, too, raised questions as to whether all devices would be needed to save money. Zoe, for instance, focused on the benefit that she felt the smart motion sensor would provide in particular: *"Yeah, I think definitely the motion sensor. So the lights and heating gets sort of reduced. It's kind of as a backup reminder."*

The promise of saving money is, of course, inextricably linked with **more efficient use of energy**. As well as saving money, this would allow them to be more environmentally friendly:

> *"I would choose to have it installed in my home, because I'm very keen. I do have a personal interest in, you know, energy use and trying to be as I suppose, efficient as possible."* [Caitlin]

Table 2: Overview of smart device location choices (by room)

	Kitchen [N=5]	Bedroom [N=6]	Bathroom [N=3]	Hallway [N=7]	Living Room [N=11]
Motion sensor	4	8	3	3	9
Voice assistant	2	1	0	4	7
Camera	4	2	0	4	8

> *"One more thing as it would, it could, prove to be like environment friendly, which is a responsible thing."* [Jatinder]

The ability to use the smart devices to explore the status of the heating, and be provided with potential actions, led tenants to suggest that this additional level of information could help them **make better choices**. Eve reflected: *"I can only think that it would make me more aware, it would maybe bring to my attention how much I was spending on heating"*. Caitlin envisaged how this could lead to positive behaviour changes: *"people don't really seem to think or know, that they can turn heating down [. . .] because I just think people get really stuck in a set way of doing it. So I think things like this that would encourage people to think about it. I think it's an excellent idea"*.

Aside from economic reasons for their use, tenants identified the **additional comfort** the smart devices could bring in terms of heating the different spaces in their homes to more ideal temperatures. For example, Grace considered how it could be used to increase her productivity when working from home: *"I think it would quite helpful if it kept the ideal temperature needed for like productivity. If you have different temperatures for if you're working from home, what's the minimum temperature needed to kind of think"*.

Moreover, several tenants found **additional uses** for the smart camera, moving away from its original design to a focus on 'home security, 'pet monitoring', or 'safety of others inside their house' widening the beneficial impact that such a system could have on their lives: *"It's handy as well [in the living room] because it could see what my dog's doing when I work. And making sure everyone's alright, because [neighbour] comes to let my dog out and she falls over sometimes so to check everything"* [Agnes]

4.1.2 Location choice criteria. An examination of tenants' location choices (as summarized in Table 2 and illustrated in Figure 3) showed that across the three smart devices most tenants chose to place their devices in the *living room*. There was also a preference for the *hallway* (seven tenants) followed by the *bedroom* (six tenants) and *kitchen* (five tenants). The least preferred room was the *bathroom* with only three tenants envisioning their smart device in that room. Looking at whether tenants preferred certain locations for a given device, the bedroom and bathroom were mostly selected to host the smart motion sensor, whereas tenants placed a mix of the smart devices in the other locations. Against this context, we now explore the criteria and security concerns that informed tenants to make their location choices.

Tenants who selected a central commonly shared area, such as the living room or the kitchen, to host the smart device did so by reflecting on their **lifestyle patterns**. A key concern was to ensure the smart device would be accessible, and thus regularly used. Agnes, for instance, chose the living room since her other digital devices were concentrated and used in the same room: "*I think because I've got the TV and other stuff in here really. I did wonder about the hallway, but yeah, I thought the front room*". Echoing several others, Jatinder explained that placing the smart devices in her living room, which was frequently used by herself and others, increased access and thus the technology's utility: "*I put it in the living room because I thought that that's like someplace where I spend quite a bit of time when there are more people in the house, it's just easy access to everyone. Yeah, it's more convenient I put it there.*"

In addition to the holistic approach described above, tenants selected rooms by focusing on the smart device's **design intention** to save money on their heating bills**,** choosing rooms that allowed them to monitor the spaces that they considered would have the most impact on their ability to conserve energy. This was most prominent in the case of the smart motion sensor: a popular feature was to monitor the usage of different rooms and turn down the heating in less used rooms:

> *"For the motion sensor I decided to put it in like places where in the home that you're not usually in. For example, the bathroom was like the main one I think 'cause it's not like you're chilling in the bathroom all the time, you occasionally go there. So like it would make sense for it to pick up your movement when someone's going in and out of the bathroom."* [Farah]

As mentioned in the previous section, however, where tenants found more than one use for the smart device, the design intentions they ascribed to the technology in turn shaped where they chose to place the device, such as Agnes' camera in the living room, which allowed for monitoring of her dog and her neighbour, or Noah who chose to place his in the hallway, which provided security around who was coming in and out of his house.

4.2 What security implications do location choices for smart devices raise and how do tenants envision mitigating these? (RQ2)

We now discuss three interconnected themes centred on tenants' security concerns. Each theme describes a distinctive concern arising from tenants' choice of placing the smart devices in their home in the event of an inadvertent or malicious system breach. We identify concerns associated with a specific smart device, with the smart voice assistant and smart camera perceived to be the most intrusive. We present how tenants regulated these concerns either using the focal technical security features explored in the study or social practices employed/envisioned. During the interviews it became evident that tenants used the placement of the device to regulate location-triggered security risks with this social practice featuring across all themes.

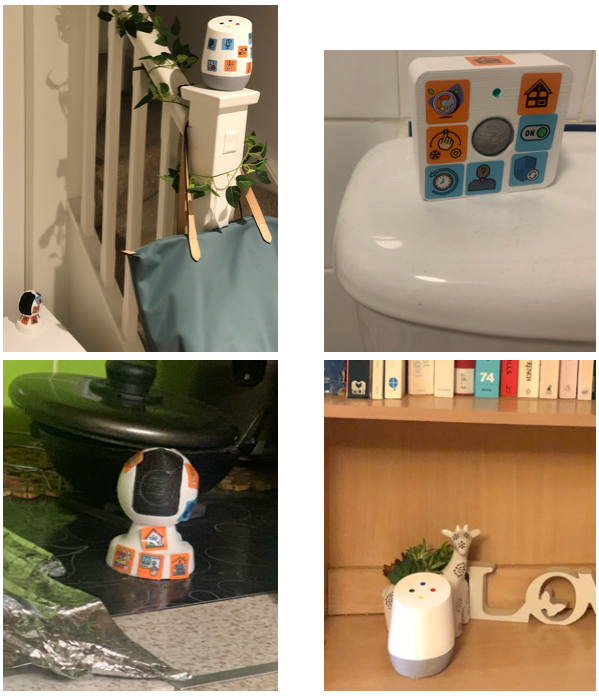

Figure 3: Smart device probes placed in tenant homes

4.2.1 Intimate Spaces. Tenants imagined the types of audio/video/motion data recorded by the smart devices within the different rooms in their home. This sparked **new worries about placing the smart devices in 'intimate spaces'**, such as the bedroom and bathroom, given the activities taking place within e.g., dressing/undressing, more personal conversations. In Helena's words: *"I didn't want it in intimate spaces, like the bathroom or the bedroom just obvious reasons, just having privacy. And yeah, when you're dressing and things, and you know. I wouldn't want that anywhere near those places."*

Tenants regulated the security breaches they anticipated by **placing the smart devices away from these intimate spaces**. This was most common for the smart camera and voice assistant, as they had the capabilities to capture voice or video data while placed in the intimate space. However, some tenants explicitly chose to exclude all three devices from these spaces. For instance, Jatinder explained *"I wouldn't specifically like in my room is you know. . .. Just felt like this is a little bit unnecessary. I don't need that much you know, you know, heating device probably"*. She went on to explain that even the addition of the proposed technical security features (see A.2) would not be enough to mitigate the concerns of having smart devices in the bedroom *". . .private conversation or something like that. . . I'd rather not have it in the bedroom and I don't want to keep looking over to see or what is being recorded and is this being tracked or something"*.

4.2.2 Social Responsibility. In addition to focusing on where the smart device was placed, tenants paid close attention to **whose data could be collected** by the device across the different spaces within their homes. One tenant, Eve, worried about her autistic son interacting with the smart devices on his own and therefore avoided placing them in his bedroom. Another tenant, Helena, anticipated the possibility of having private conversations in her home. Having placed the smart device in the living room, Helena renegotiated the communication norms within that room to afford her with some control over the sensitivity of data the devices collected: *"And because with the conversations in the living room, it's not necessarily things that you don't know. . .I can limit conversations in the living room much more easily"*. Placing the smart device in a communal space was also done to make it visible, allowing tenants to remember that it was there and operating, thus affording more control:

> *"I think to have it in other rooms, I think I would forget it was there or it wouldn't have all the information at its disposal to help me, so that's how I think it would be beneficial in the living room and I'm sure I could minimise the potential harm it could do."* [Eve]

Contrasting with tenants who increased their sense of control through placing the smart device in a communal space, such as the living room, others perceived communal spaces to afford less control owing to the collective and thus unpredictable conversations that took place. This led them to select more private rooms to limit the conversations the smart voice assistant could hear.

Tenants also discussed their use of the proposed smart device technical security features, which included **putting restrictions on the capture of other people's data** when they had chosen the devices to be located in communal spaces within the home. Sharon explained why she chose to incorporate particular technical security features (i.e., multi-factor authentication (see A.2: C10-SP; M7-SP; V11-SP) and locking the device to only listen to her voice (see A.2: V7-SL)): *"so I tried to think of the things that I would need like putting a code in, it's only me that could do that.My voice, I'm the only one that could activate it.I don't want it picking up anyone else's because it's a security risk to everybody else"*. Zoe also talked about adding particular technical security features to the smart devices to ensure her visitors would feel more comfortable to visit her with the devices operating in her home. Consequently, she selected a security feature which prevented the user from naming devices in such a way that their location was identifiable (e.g., by including part of home address – see A.2: C6-SL; M3-SL; V6-SL). Zoe envisaged this to prevent hackers from tracking her visitors' movements and knowing they had been to her home. In contrast to Zoe who used the technical security features to mitigate her concerns, Mario felt that none of the proposed security features on the smart voice assistant could protect his visitors and that some features could even **introduce the possibility for social tensions**. In reference to the warning lights, which indicate when a smart device is recording (allows users to monitor when the smart device is operating – A.2: C1-SM, V1-SM), Mario explained: *"I would never ask my friends or guest if I am allowed to record them, will feel very uncomfortable"*.

4.2.3 Surveillance . Most tenants reported **surveillance risks resulting from the use of the smart devices**, thus feeling watched and tracked within their home. Surveillance was expressed most vividly in relation to the smart camera device, which we focus on to illustrate the concerns. Mario, for instance, had experimented

with the three smart devices' locations within his home throughout the study, but was not able to place the smart camera in a room that mitigated the sense of surveillance. He explained: *"With the camera is different because when I had the camera even in my living room because I have only one bedroom.I just feel like all the time I was like being watched, if you know what I mean."*. In alignment with tenants' concerns over whose data was collected (see 4.2.2) Mario also highlighted the smart device owner's responsibility to make this covert surveillance visible in the presence of others.

Unlike Mario, whose concerns with the smart camera remained unresolved, Grace **strategically used the location of the smart camera to regulate her security** placing it in the hallway which she re-defined as a public space: *"So, the camera in the hallway, because if I open the door I'm willing for the world to see me. I'm willing for the camera to see me. I'm going to treat any information as [in the public domain] I know it's probably not, but you know that like when I was a teenager, people say on social media like what you post on social media has to be what you'd be happy with your parents reading. And if you're not happy with don't post it. So yeah, that's why I put that there."*

A further strategy was to **remove the more concerning functions** of the smart camera (such as facial recognition – see A.1: C3-CSU, C6-CM). Zoe, for example, removed core device features to alleviate the surveillance concerns of some visitors allowing her to use this smart device in a communal space: *"my mum for instance, she's very anti-technology and comes from a generation where they are kind of scared and she seems to think these devices can do more than they can do, like listen. Even if I reassured her, I think it would put her off coming to the house, she knew that was like that."* Eve applied the same approach to the smart motion sensor by limiting the extent of the data that could be tracked, choosing to exclude the detection of movement in particular rooms (see A.1: M4-CM).

Many tenants chose to utilise technical security features, which allowed them to **increase their ability to monitor the smart device's operation** and thus to manage their concerns. Examples included a green light being displayed when a device was detecting data (i.e., motion/voice/image – see A.2: C1-SM, M1-SM, V2-SM), a red light being displayed when a device was recording data (see A.2: V1-SM) and also a cover being closed when the smart camera was not in use (see A.2: C2-SM). These technical security features helped tenants to deal with feelings of being constantly surveilled, with Eve explaining *"And the red light was a good idea, to show when it's listening in on conversations, so I had a say over that. I knew what was being recorded, what wasn't. I liked that."*. In addition to monitoring, tenants such as Helena chose to regulate the smart device's data collection by using a security feature which restricted the times at which the smart voice assistant could listen to conversations (see A2: V8-SL): *"I don't want it to listen, like passively listen at any time, so I think has want to be in control of that all the time. Just because it just freaks me out the idea of this device in your home absorbing things about you"*. Finally, even though tenants applied a range of technical security features to their smart device, Farah highlighted that these features were more important when the device was first introduced with users likely to accept the smart camera with less security features over time: *"Uhm with the camera, when you know it's on or it has a cover when it's not in use, I guess it makes it feel a bit better, but I feel like it's something like when you first get it, you feel a bit-, but it's really, it takes getting used to it."*.

5 DISCUSSION

Our study shows that tenants, overall, believed that the smart energy system could personally offer them a range of potential benefits and were able to relate the imagined benefits of the different smart energy technologies directly to their life circumstances. This is in broad alignment with previous research by [32], and most notably Kozubaev et al. [27] whose study with a similar group of tenants in public housing in the US also showed that tenants appreciated the possibilities introduced by smart technology in their home. Tenants' shared vision to save costs with smart energy technology mirrors findings from past research [40]. However, considered in the context of the economic, and more broadly intersectional, inequalities social housing tenants can experience [13], we argue that security breaches could incur more profound financial and emotional harms on a group experiencing hardship, and thus the concerns of this group are of critical importance to understand.

To this effect, despite their positive readings of smart technology, tenants raised security concerns. Contrasting with the previously widespread apathy reported in relation to smart device security [43], we found that *all* the tenants were concerned about security risks. This may have been due to the fact that the devices would mean a certain level of acquiescence to sharing personal data, and the implications that that may bring, with their landlords. It could have also been because of the focus on security within the study. Nonetheless, inspecting how each of the tenants regulated their security suggests they were willing to accept different levels of risk. Tenants' security concerns in relation to smart devices used in the home context broadly fell into three themes: intimate spaces (not wanting to be recorded in the bedroom, for instance); social responsibility (not wanting to record visitors, or particular household members) and surveillance concerns (not wanting to feel watched at all times). These concerns were in turn regulated in the following distinct ways that combined technical and social resources: *utilising device-specific technical security features* in combination with *adopting particular social practices*.

Our findings underscore the idea that security is a situated practice [16]: it is not an abstract notion, but indeed one that – in the case of physical devices in the home – involves a consideration of place along with any connected domestic activities and routines. It is also a stark reminder that these considerations emerge through people's embodied experiences of living with the technology. Our study thus highlights the importance of employing material speculation to gain critical insights into the introduction of near-future technology for the home, providing an important consideration for smart device designers and housing providers working in the social housing sector. In what follows, we elaborate on some of the prominent themes arising from our findings to propose new ethical implications for *social housing providers* and smart device *designers*.

5.1 Malleable and regulated use of smart devices in intimate spaces

Seeking to maximise the benefits of their smart energy system, some tenants experimented with how they might use the technology and

what it was designed for, with this impacting in unexpected ways on where they placed the individual devices. Specifically, different tenants showed a range of ideas around how to use the technology to benefit their energy efficiency by using different rooms – for example, the use of the motion sensor in the bathroom being perceived as a cost-saving measure by some, but unnecessary by others. Tenants also realised that devices could be subverted to perform more than one task for them: this too may find the same device being placed in several potentially different locations, based upon the ways in which the user decides to use them. Scuito et al. [37] suggest that smart devices in more private rooms are most likely used to support specific tasks, whereas those in common areas are used in more open-ended ways. Taken together, our findings support a more complex account in the 'specific task' of managing energy use indicating that the placement of smart devices could greatly vary based on how tenants interpret the goals of the smart device, the convenience of its placement, and the tenant's inclination to creatively appropriate it. With regards to appropriation, the degradation of properties observed in the UK housing sector [29] could also direct tenants to use smart technology for the purposes of diagnosing or problem-solving room-specific concerns e.g., related to energy conservation or other consequences of disrepair. Our findings highlight the need for housing providers to follow *transparent smart device procurement processes* that involve tenants from the very start to identify how smart technology could equally benefit their lives through a better understanding of their personal living circumstances.

Despite the malleable practices with smart devices we report in this section, our study shows that there were also social norms that limited the use of smart technology in certain spaces. Owing to their audio and video recording capabilities, most of our tenants avoided placing their smart camera and voice assistant in the bedroom and bathroom considering the intimate activities taking place therein, reflecting similar findings reported by [43]. Conversely, the type of device placed the most in intimate spaces was the motion sensor showing a recognition that this device and the data it collected could still be helpfully used in these rooms to increase energy efficiency [50]. Therefore, tenants made balanced judgments about the data collected by the smart device and the security implications potentially arising in the location it was placed in. Contrasting with Tan et al. [43] who propose that smart devices can track data from wide-ranging areas in the home to expand the scope and severity of security risks, our study shows that people can also possess social norms that lead them to limit the use of smart devices across certain rooms of their home.

Alongside these shared norms and established ways of regulating security, we also found that social norms were transformed through the imagined use of different smart devices, with some tenants renegotiating their norms to make way for the benefits of smart technology. For instance, tenants reframed the hallway as a semi-public space used prior to stepping outside into the world, or that would be the primary entry-point of burglars. Lastly, our findings indicated the potential that these norms could evolve after the tenant has lived with the technology for a period of time, which could lessen the need for particular security features as a user becomes accustomed to the device in their home. This mirrors the wider finding that novel technologies in the home can quickly become a routine part of our domestic lives as well as how comfort with particular functionalities can evolve over time [9, 11]. Our study thus demonstrates the importance of *undertaking new smart device pilots* in-situ within tenant homes over an extended period of time as a route to provide opportunities for tenants to critically reflect on the social implications these devices may pose. Moreover, it will be equally vital for housing providers to allow for the agency of tenants who may remain concerned, for example, by critically evaluating and mitigating the potential inequalities that opting out of such devices may introduce.

5.2 Balancing smart device access with the security of others within communal spaces

Previous work has shown that smart technology users tend to place their devices in central or frequently used rooms within the home [28]. Our study provides support to this finding: tenants also placed the three devices in communal spaces, such as the living room, kitchen, and hallway. Crucially, the living room was chosen by most. Placing a smart device in a common room has been found to maximise the utility of the device by ensuring its use by the whole household and connectedness to other devices [28]. In line with this, our tenants perceived the smart device to be more visible and accessible to all household members in these communal spaces, which also indicates their desire to actively interact with it and benefit from its use. While the smart energy system in this study were imaginary, depending on how they are designed, many smart technologies depend on collecting data frequently, and thus communal spaces could be a critical factor to how well they work.

Although tenants agreed about the importance of device visibility and access, those who lived with others or had frequent visitors, experienced significant security concerns relating to their social responsibility toward those who didn't own the smart device. Placing the smart device in a communal area was almost certain to record, analyse and store others' data. Tenants imagined the people who would use the room using the placement of the smart device to regulate the security concern. Some tenants felt that having the smart device in the living room afforded them control to adjust their social interactions in that room, introducing trade-offs with their autonomy and freedom of expression within their home. In direct contrast, others removed the smart devices from communal spaces given the unpredictable conversations likely to arise with other family members and visitors, as a result limiting the direct benefits of interacting with the smart devices more frequently. Therefore, whereas tenants all shared the same social norms, the ways they used location to regulate these varied and always presented a trade-off. In addition, although both tenant and housing provider may agree that there are benefits conferred in the use of these devices, in the situation where the housing provider requires the use of such devices, tenants could find that they have little autonomy beyond where to place them. It is here where innovative *security feature design* could provide ways to better mitigate tenants' particular concerns around what and how much data is collected, for instance through informing tenants via their phone if they are being recorded when near a smart device [52] or sending them periodic summary reports of the data that has been collected and who has access to it, with recommendations to increase security

based on their specified risk level and/or particular vulnerabilities. Since most of the concerns we found stemmed from the type of data collected by the device, housing providers should select and ensure that on setup *data collection is minimised* as much as possible and directly connected to the purpose of the device.

5.3 Social and technical approaches for using security features in the home context

Our study shows that tenants chose to apply a range of technical security features to the smart energy system. This included features that allowed tenants to monitor what the different devices were doing, limit the data that was stored and shared, as well as provide additional access protections. Their active engagement with these features corroborated their concerns while showing an appreciation of the technical means available to regulate security in the home context. Yet, for those concerned about the security of their family and friends in communal spaces (see 5.1), technical security features also introduced the potential for social turbulence in these relationships. For example, cues highlighting the smart devices' data collection, such as a light to signal recording, indicated to visitors that they were being covertly recorded. One preferred solution to this issue was to place restrictions on the capture of voice/video recordings of visitors. This indicates a need to think more holistically about the *security feature design* to consider the social norms within the environment in which the device will be used. This could incorporate norm violation nudges [53] which ask users questions such as "Do you have family members or visitors who would be uncomfortable with being audio recorded?" as well as user agency nudges which prompt users to involve family members and/or frequent visitors in the security setup of devices placed in communal rooms.

In selecting these technical security features, tenants demonstrated a varied understanding of how these existing common security protections typically worked in practice and often appropriated the proposed security features in different ways, aligning with [52]. We draw on the tenant who wanted to protect visitors by only allowing the devices to respond to her own voice to illustrate this point. While this tenant used this feature to exclude the voices of others, visitors' voices would still require processing to determine whether they should be responded to or not. This suggests that even with the best intentions, users may fail to appropriately balance their security risks based on a poor technical understanding of the smart device. In addition to poor mental models around how the device works, so too may users struggle to conceptualise the risks of using such devices without appropriate guidance, specified to their needs. Therefore there is a broader need to *offer specific security training* that is accessible and appropriate to both tenants and housing providers around the function and limitations of technical security features within smart devices, which is in agreement with recommendations from [31, 45].

5.4 Ethical implications for smart technology design and use

Tenants' low socio-economic status as well as additional vulnerabilities, such as disability or other support needs means that they typically have little choice but to rent their home long-term from a social housing provider, increasingly under insecure tenure conditions [21]. Consequently, the power relations between tenants and their landlords are significantly imbalanced, with housing providers having control over several aspects of their tenants' lives. Furthermore, social housing is often viewed as a site for improvement and intervention [8, 25] and the introduction of new smart technologies is one such example. Social housing provides significant opportunities to undertake widespread home pilots of these technologies, allowing housing providers even greater control over their tenants.

Our findings indicate that housing providers as well as smart device designers (who cater to this market) could potentially be shaping tenants' future lives in profound ways through their choice and installation locations of this technology. This can introduce opportunities for increased surveillance, exploitation of personal data, losing freedom of expression and disruption of existing social equilibria within the home, that add to tenant vulnerability. This existing power imbalance highlights the importance that both housing providers and smart device designers ensure they are acting in ethical ways when embedding such technology into tenants' homes.

The initial choice of smart device made by housing providers can have implications for the areas in the home which may need to be monitored and have data captured from. Giving tenants agency during the procurement stage can help to identify devices that offer the benefits for both parties as well as ensure tenant feel comfortable having in their home. However, once tenants have agreed to installation, they may then feel powerless to change their mind after they understand the reality of living with the device in a particular location within the home. Furthermore, after a device has been installed into a tenant home our findings highlight that they may quickly become accustomed to it, especially if it is located in a less visible place. Devices may have capabilities to collect data beyond what has been consented for, and given the interventions that are often initiated within the social housing sector this raises the temptation that existing smart devices could be exploited to provide housing providers insight into new areas for future interventions. Housing providers thus need to maintain a duty of care, ensuring these devices are used in alignment with their tenants' consent on a continuing basis.

While the design and usability of security features is important for all users, it is even more critical for social housing tenants whose lives are often under scrutiny, thus posing the risk of technology being used for increased surveillance. When designing technology to function within a particular location in the home which may allow landlords (or other nefarious actors) access to sensitive information smart device designers should thus integrate appropriate security controls that can be used by the tenants whose digital literacies may vary. Due to lack of knowledge tenants may circumvent important security controls or conversely implement specific controls that impact the function of smart devices, which have implications for their vulnerability or potential to benefit from the device. Smart device designers should educate and support tenants to ensure that they understand the functionality and limitations of the device security, particularly in relation to mitigating risks arising from where the device is located in the home.

Table 3 summarises these ethical implications for both housing providers and smart device designers within the housing sector

Table 3: Summary of ethical implications for housing providers and smart device designers

	Security Strategy	Stakeholder	Implication
1	Practice: *Transparent device procurement*	Housing providers	Involve tenants in smart device procurement consultations to identify devices that offer flexible solutions to the needs of both parties, and provide equitable solutions for those wishing to opt-out due to security concerns (available before, or after the smart device is introduced)
2	Practice: *Undertake device pilots*	Housing providers	Provide opportunities to discuss and pilot with tenants the placement of smart devices prior to installation ensuring they understand the potential implications. Additionally, offer a trial period to allow tenants time to experiment and critically reflect on placing new smart devices in different locations within their home
3	Device: *Holistic security feature design*	Smart device designers	Engage with tenants to better understand their security needs and intentions in relation to smart devices, extending or reimagining how technical security features can consider the location of devices within the home
4	Device: *Minimise data collection*	Housing providers	Ensure devices are set up in such a way that the minimum possible data is collected for the stated purposes of the devices in line with tenants' consent
5	Device: *Offer specific security training*	Smart device designers	Provide training to tenants on the function and limitations of device-specific technical security features. The training can also highlight the impact of specific technical security features on the overall functionality of the device

who aim to integrate smart technology into future social housing interventions.

5.5 Reflections on the speculative approach

Having explored tenants' speculations of a future smart energy system and the connected security implications, we now reflect on our distinctive application of speculative design. We explicitly told participants that this was a fictional system containing a combination of real and imagined features, and chose to use 3D-printed probes of existing smart devices to represent the different components of this imaginary system alongside physical stickers for their features. Our literal use of the probes meant that some aspects of our approach were more closed than other speculative design methods and may have limited participants' speculations around future smart technologies. However, it also helped to ground the discussions in a scenario that connected with the real world and participants' lived experiences in a more tangible way. Our choice of probes, as opposed to using the real devices, also meant that we could focus on wider concerns rather being limited by tenants' prior experience (i.e. 5/11 participants had no prior experience using smart technologies) or their ability to fully grasp the more technical functionalities of smart devices. Furthermore, our focus on the imagined integration of the three distinct smart devices enabling the collection of different data types (i.e. voice, video and movement) allowed us to probe concerns relating to data sensitivity, which resulted in a set of ethical implications that are transferable to other areas of smart home technology within social housing.

Accessible methods are a particularly important consideration when seeking to involve traditionally marginalized and underrepresented communities in envisioning our digital futures. During this study we found the use of speculative design methods lowered the bar for participation. There was no requirement to own a particular device, have sufficient internet connectivity or technical knowledge to engage in the study. The methods also provided more freedom to explore the smart devices and associated security concerns in engaging and creative ways. For instance, using the combination of probes and stickers (rather than being limited to the current functionalities of an existing device) afforded participants with the agency to combine existing and imagined smart functionalities, broadening the speculative discussion into the realms of the plausible and possible. This customisation of the probes was also intended to enable a more participatory approach to speculative design [10] through allowing opportunities for tenants to adapt the initial technological future proposed by the research team and then subsequently speculate about how this imagined future might manifest within their own domestic lives. Further research could look to extend this participation through involving participants in collectively defining the initial smart technology scenario and identifying meaningful ways to connect it with the lived experience of social housing tenants through sustained engagement with diverse multi-generational groups.

6 CONCLUSION

The aim of this research was to explore social (low rent) housing tenants' speculations in relation to the near-future introduction of a smart energy system, comprising three devices (a motion sensor, smart speaker and camera) in their home. Social housing tenants are important to consider since they typically encompass vulnerable sections of society (e.g., low-economic status, retired, disabled). Manufacturers of smart energy devices aimed at the social housing

sector underline that there are cost and energy efficiency savings to be made for the tenant when using their devices. However, these devices will be installed in the property by the housing provider, who will use the same device to monitor the use and condition of the tenant's home. This means that, despite the promise of energy efficiency and cost savings, social housing tenants' ability to control their home environment could be limited with respect to these devices. We recruited 11 tenants from within this group, and despite the majority of the tenants in the study being White females, our sample reflected diversity in other ways, including in terms of age range, geographical locations around the UK, experiences with disability as well as co-living arrangements. Given these tenants self-selected it also provided an interesting contrast to the prevalence of male tenants within many other smart home studies as well as the default smart device settings being typically designed for the able-bodied man [41].

Within this context we wished to understand how tenants perceive the benefits of smart energy devices, alongside the security concerns this technology triggers. We took a situated lens that recognised tenants' agency in placing these devices in different locations within their home. To foster tenants' speculations around the themes of benefits and security concerns, we provided physical models of the three smart devices prompting our tenants to consider the possible money savings on their heating bills. Using the physical models along with situated speculation booklets, our participants 'customized' each smart device by incorporating core energy saving features and technical security features, placed these devices within their home, and lived with them for a period of a week. In follow-up reflective discussions participants were invited to share their individual interpretations of the smart energy system within their homes and share any related concerns that arose during this process.

Our empirical work offered three main contributions to the domestic smart device security literature: a greater insight into social housing tenants' particular and varied security concerns around the imposition of smart technology within their homes; a situated understanding of how people place and imagine living with smart devices in their homes; and a set of ethical implications targeted at smart device designers and housing providers looking to utilise smart technology within tenant homes. In light of the potential for future widespread imposition of smart devices within social housing we hope that this work provides a first step in examining one key aspect of the associated security concerns, highlighting the particular support needs of this underrepresented group to the security and privacy research community, and beyond.

ACKNOWLEDGMENTS

This work was funded by EPSRC grant EP/T026812/1. We are grateful to George Loukas, Etienne Roesch and Simon Busch-Moreno for their feedback on the study design. We would also like to thank all of the study participants for their engagement in this research.

REFERENCES

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security*, 451–466.

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2018. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys* 50, 3: 1–41. https://doi.org/10.1145/3054926

[3] James Auger. 2013. Speculative design: crafting the speculation. *Digital Creativity* 24, 1: 11–35. https://doi.org/10.1080/14626268.2013.767276

[4] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet*, 14.

[5] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2: 77–101. https://doi.org/10.1191/1478088706qp063oa

[6] Kirsten Bray and Christina Harrington. 2021. Speculative Blackness: Considering Afrofuturism in the Creation of Inclusive Speculative Design Probes. In *Designing Interactive Systems Conference 2021*, 1793–1806. https://doi.org/10.1145/3461778.3462002

[7] Mark Brown and Robert Booth. 2022. Death of two-year-old from mould in flat a 'defining moment', says coroner. *The Guardian Newspaper*. Retrieved November 15, 2022 from https://www.theguardian.com/uk-news/2022/nov/15/death-of-two-year-old-awaab-ishak-chronic-mould-in-flat-a-defining-moment-says-coroner

[8] Adorkor Bruce-Konuah, Rory V. Jones, Alba Fuertes, Leonardo Messi, and Alberto Giretti. 2018. The role of thermostatic radiator valves for the control of space heating in UK social-rented households. *Energy and Buildings* 173: 206–220. https://doi.org/10.1016/j.enbuild.2018.05.023

[9] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–16. https://doi.org/10/gksmtt

[10] Simran Chopra, Rachel E Clarke, Adrian K Clear, Sara Heitlinger, Ozge Dilaver, and Christina Vasiliou. 2022. Negotiating sustainable futures in communities through participatory speculative design and experiments in living. In *CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3491102.3501929

[11] Andy Crabtree, Richard Mortier, Tom Rodden, and Peter Tolmie. 2012. Unremarkable networking: the home network as a part of everyday life. In *Proceedings of the Designing Interactive Systems Conference on - DIS '12*, 554–563. https://doi.org/10.1145/2317956.2318039

[12] Teresa Denefleh, Arne Berger, Albrecht Kurze, Andreas Bischof, and Christopher Frauenberger. 2019. Sensorstation: Exploring Simple Sensor Data in the Context of a Shared Apartment. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, 683–695. https://doi.org/10.1145/3322276.3322309

[13] Department for Levelling Up, Housing and Communities. 2020. *English Housing Survey: headline report*. Retrieved September 12, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060141/2020-21_EHS_Headline_Report_revised.pdf

[14] Audrey Desjardins, Cayla Key, Heidi R. Biggs, and Kelsey Aschenbeck. 2019. Bespoke Booklets: A Method for Situated Co-Speculation. In *Proceedings of the 2019 on Designing Interactive Systems Conference*, 697–709. https://doi.org/10/gjx298

[15] Audrey Desjardins, Jeremy E. Viny, Cayla Key, and Nouela Johnston. 2019. Alternative Avenues for IoT: Designing with Non-Stereotypical Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3290605.3300581

[16] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21, 3: 319–342. https://doi.org/10.1207/s15327051hci2103_2

[17] Dunne, Anthony and Raby, Fiona. 2013. *Speculative everything: design, fiction, and social dreaming*. MIT Press.

[18] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the Experience-Centeredness of Privacy and Security Technologies. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop - NSPW '14*, 83–94. https://doi.org/10/gh2qtt

[19] Nils Ehrenberg and Turkka Keinonen. 2021. Co-Living as a Rental Home Experience: Smart Home Technologies and Autonomy. *Interaction Design and Architecture* 50: 82–101. https://doi.org/10.55612/s-5002-050-005

[20] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. https://doi.org/10.1145/3290605.3300764

[21] Suzanne Fitzpatrick and Hal Pawson. 2014. Ending Security of Tenure for Social Renters: Transitioning to 'Ambulance Service' Social Housing? *Housing Studies* 29, 5: 597–615. https://doi.org/10.1080/02673037.2013.803043

[22] Flagship Group. 2021. 20,000 Flagship properties in Switchee IOT deal. *Housing Technology*. Retrieved from https://www.housing-technology.com/20000-flagship-properties-in-switchee-iot-deal/

[23] 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*, 1–13. https://doi.org/10/gf7bw8

[24] HACT. 2020. *Do The Smart Thing: The future of the social smart home*. Retrieved September 12, 2022 from https://hact.org.uk/nextinnovations/smart-homes/

[25] Rory V. Jones, Alba Fuertes, Christine Boomsma, and Sabine Pahl. 2016. Space heating preferences in UK social housing: A socio-technical household survey combined with building audits. *Energy and Buildings* 127: 382–398. https://doi.org/10.1016/j.enbuild.2016.06.006

[26] Awais Hameed Khan, Neelam Ejaz, Sarah Matthews, Stephen Snow, and Ben Matthews. 2021. Speculative Design for Education: Using Participatory Methods to Map Design Challenges and Opportunities in Pakistan. In *Designing Interactive Systems Conference 2021*, 1748–1764. https://doi.org/10.1145/3461778.3462117

[27] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, and Christopher A. Le Dantec. 2019. Spaces and Traces: Implications of Smart Technology in Public Housing. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10/gjt7fn

[28] 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: 1–31. https://doi.org/10.1145/3274371

[29] Levelling Up, Housing and Communities Committee. 2022. *The Regulation of Social Housing*. Retrieved November 26, 2022 from https://publications.parliament.uk/pa/cm5803/cmselect/cmcomloc/18/report.html,

[30] Lizzie Coles-Kemp. 2020. Inclusive Security: Digital Security Meets Web Science. *Foundations and Trends® in Web Science* 7, 2: 88–241. https://doi.org/10.1561/1800000030

[31] Lynne Coventry, Pam Briggs, John Blythe, and Minh Tran. 2014. *Using behavioural insights to improve the public's use of cyber security best practices*. Government Office for Science. Retrieved February 8, 2023 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

[32] 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* 2020, 2: 436–458. https://doi.org/10.2478/popets-2020-0035

[33] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, 2189–2201. https://doi.org/10.1145/3025453.3025875

[34] National Housing Federation. 2022. Decarbonisation: a guide for housing associations. Retrieved from https://www.housing.org.uk/resources/decarbonisation-guide-for-housing-associations/

[35] Office for National Statistics. 2022. Energy prices and their effect on households. Retrieved from https://www.ons.gov.uk/economy/inflationandpriceindices/articles/energypricesandtheireffectonhouseholds/2022-02-01

[36] Ed Potton and Hinson, Suzanna. 2020. Housing and Net Zero. Retrieved August 15, 2022 from https://researchbriefings.files.parliament.uk/documents/CBP-8830/CBP-8830.pdf

[37] Alex Sciuto, Arnita Saini, Jodi Forlizzi, and Jason I. Hong. 2018. "Hey Alexa, What's Up?": A Mixed-Methods Studies of In-Home Conversational Agent Usage. In *Proceedings of the 2018 Designing Interactive Systems Conference* (DIS '18), 857–868. https://doi.org/10/gh3mz5

[38] William Seymour. 2020. A Design Philosophy for Agents in the Smart Home. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–9. https://doi.org/10/gh2qt2

[39] Julia Słupska, Ruba Abu-Salma, Selina Cho, and Nayanatara Prakash. 2022. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *31st USENIX Security Symposium*, 323–340.

[40] Yolande A.A. Strengers. 2011. Designing eco-feedback systems for everyday life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2135–2144. https://doi.org/10.1145/1978942.1979252

[41] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3290605.3300875

[42] Switchee. 2022. Heating Your Home For Less. Retrieved December 9, 2022 from https://www.switchee.com/residents/

[43] Neilly H Tan, Richmond Y Wong, Audrey Desjardins, Sean A Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–25. https://doi.org/10.1145/3491102.3517617

[44] Tim Coughlan, Kerstin Leder Mackley, Michael Brown, Sarah Martindale, Stephan Schlögl, Becky Mallaband, John Arnott, Jettie Hoonhout, Dalila Szostak, Erika Poole, Antti Pirhonen, Val Mitchell, Sarah Pink, and Nicholas Hine. 2013. Current Issues and Future Directions in Methods for Studying Technology in the Home. *PsychNology Journal* 11, 2: 159 – 184.

[45] Sarah Turner, Jason Nurse, and Shujun Li. 2021. When Googling It Doesn't Work: The Challenge of Finding Security Advice for Smart Home Devices. In *Human Aspects of Information Security and Assurance*, 115–126.

[46] Sarah Turner, Nandita Pattnaik, Jason R. C. Nurse, and Shujun Li. 2022. "You Just Assume It Is In There, I Guess": UK Families' Application And Knowledge Of Smart Home Cyber Security. In *Proceedings of the ACM on Human-Computer Interaction*, 1–34. https://doi.org/10.1145/3555159

[47] Ron Wakkary, William Odom, Sabrina Hauser, Garnet Hertz, and Henry Lin. 2015. Material Speculation: Actual Artifacts for Critical Inquiry. In *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives*, 97–108. https://doi.org/10/gjx3bf

[48] Alma Whitten and J D Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, 169–183.

[49] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2: 463–476. https://doi.org/10/f6zmp5

[50] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. In *Proceedings of the ACM on Human-Computer Interaction*, 1–21. https://doi.org/10.1145/3546719

[51] 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: 1–24. https://doi.org/10.1145/3359161

[52] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Thirteenth Symposium on Usable Privacy and Security*, 65–80.

[53] 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 *USENIX Security Symposium*, 159–176.

[54] 1994. The Secure Tenants of Local Housing Authorities (Right to Repair) Regulations.

A A APPENDICES

A.1 List of available core features for each smart device probe

Core Feature Category	Camera	Motion Sensor	Voice Assistant
Set Up	**(C1-CSU)** Can know who lives in your house	**(M1-CSU)** Assign different temperature preferences for individual rooms	**(V1-CSU)** "Your home is currently 20 degrees, is this too warm for you?" Can ask about temperature preferences
	(C2-CSU) Can assign different temperature preferences for individual household members	**(M2-CSU)** Can know which rooms you have in your house	**(V2-CSU)** "How much do you earn?" What do you regularly spend your money on?" Can ask about monthly income/outgoings
	(C3-CSU) Can know what typical facial expressions and/or body postures show that you (or your household members) are feeling too warm)	**(M3-CSU)** Allow all activity in the house to be monitored	**(V3-CSU)** "Are you worried about the cost of Christmas this year?" Can ask about particular financial concerns over the year
Monitors	**(C4-CM)** Can track what activities you are doing in the house e.g. cooking, watching tv, sleeping	**(M4-CM)** Can track which room(s) there has been movement and when	**(V4-CM)** "I think I might be overdrawn" Can listen out for money concerns and check your current bank balance to make sure you have enough funds for your heating bill
	(C5-CM) Can monitor individual facial expressions and body postures to look for signs of feeling too warm	**(M5-CM)** Can track daily/weekly patterns of movement in the house	**(V5-CM)** "I'm thinking about buying a new mobile phone" Can listen and track what other item/services you are spending money on
	(C6-CM) Can use facial recognition to know who is currently in the house	**(M6-CM)** Monitors the speed/intensity of movement e.g. high intensity during online exercise class or when vacuuming the house	**(V6-CM)** "I think you're wasting your money on that monthly gym membership" Can listen and record opinions about household spending habits from other family and friends
			(V7-CM) "I think you're wasting your money on that monthly gym membership" Can listen and record opinions about household spending habits from other family and friends
Acts	**(C7-CA)** Can automatically turn down heating if you are doing certain activities e.g. cooking (i.e. generating extra heat) or sleeping (i.e. house should be cooler)	**(M7-CM)** Can recommend changes you can make to your heating schedule based on regular activity in house/	**(V8-CA)** "Try turning your heating down by 1 degree" Can advise you about how to manually adjust your heating setting to keep bills affordable
	(C8-CA) Can automatically adjust heating settings to lowest comfortable temperature based on who is home	**(M8-CM)** Turns off heating automatically if no movement is detected in the house or specific room	**(V9-CA)** Can automatically adjust your heating settings to keep bills affordable
	(C9-CA) Can automatically turn down heating if anyone appears to be feeling too warm	**(M9-CM)** Adjusts heating automatically based on daily/weekly routine e.g. when you are typically out, high intensity movement	**(V10-CA)** Can advise you about how to change other spending habits to help you save for your heating bills
		(M10-CM) If your boiler breaks down can recommend repair appointment within times that movement is normally detected in the house	

A.2 List of available technical security features for each smart device probe

Security Feature Category	Camera	Motion Sensor	Voice Assistant
Monitors	**(C1-SM)** The green light on top of your smart camera lens is on when the camera is in use **(C2-SM)** Automatically enable camera cover when device is not in use	**(M1-SM)** The green light on top of your smart motion sensor flashes to show when it is tracking your movement	**(V1-SM)** The red light on top of your smart voice assistant flashes to show when it is recording your conversation **(V2-SM)** The green light on top of your smart voice assistant flashes to show when it is listening to your conversation
Limits	**(C3-SL)** Stop any video recordings being shared with others e.g. for the technology company to use the recordings to help them improve their own services	**(M2-SL)** Smart motion sensor will regularly auto-delete the usage history e.g. what rooms there has been movement in and what time	**(V3-SL)** Keep the storage of personal data to the minimum needed for the chosen smart camera features e.g. will not store information about your bank if the voice assistant does not need to check your account
	(C4-SL) Keep the storage of personal data to the minimum needed for the chosen smart camera features e.g. will not store information about who lives in your house if you do not include facial recognition	**(M3-SL)** Stop risky names being given to the motion sensor during the setup e.g. Flat 22 Motion Sensor, which reveals information about where the device is located	**(V4-SL)** Stop any voice recordings being shared with others e.g. for the technology company to use the recordings to help them improve their own services
	(C5-SL) Smart camera will regularly auto-delete any video recording	**(M4-SL)** Keep the storage of personal data to the minimum needed for the chosen smart camera features e.g. will not store information about when you are home if the device is not trying work out your daily/weekly routine	**(V5-SL)** Smart voice assistant will regularly auto-delete any audio recordings
	(C6-SL) Stop risky names being given to the smart camera during the setup e.g. Flat 22 Smart Camera, which reveals information about where the device is located	**(M5-SL)** Only allow the motion sensor to monitor to your movements during a specific part of the day e.g. only between 5pm-10pm	**(V6-SL)** Stop risky names being given to the smart voice assistant during the setup e.g. Flat 22 Voice Assistant, which reveals information about where the device is located
	(C7-SL) Smart camera will regularly auto-delete the usage history e.g. what behaviours it has identified, who has been in the house		**(V7-SL)** Lock the smart voice assistant so it can only list to your voice
	(C8-SL) Lock the smart camera so it can only identify your face		**(V8-SL)** Only allow the voice assistant to listen to your conversations during a specific part of the day e.g. only between 5pm-10pm **(V9-SL)** Smart voice assistant will regularly auto-delete the usage history e.g. what adjustments it has made, what advice it has given

Protects	**(C9-SP)** Smart camera can automatically install any security updates	**(M6-SP)** The motion sensor can automatically install any security updates	**(V10-SP)** Smart voice assistant can automatically install any security updates
	(C10-SP) Smart camera requires multi-factor authentication to allow access user account settings e.g. sending a code to your phone	**(M7-SP)** The motion sensor requires multi-factor authentication to allow access user account settings e.g. sending a code to your phone	**(V11-SP)** Smart voice assistant requires multi-factor authentication to allow access user account settings e.g. sending a code to your phone
	(C11-SP) Smart camera will ask for the user account password to be updated every 90 days	**(M8-SP)** The motion sensor will ask for the user account password to be updated every 90 days	**(V12-SP)** Smart voice assistant will ask for the user account password to be updated every 90 days